```
**********************************************************
    5271 Mon Mar 24 15:31:28 2008
new/deleted_files/usr/src/common/crypto/arcfour/amd64/arcfour_crypt_amd64.s
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
#if !defined(lint) && !defined(__lint)
/  ARCFOUR implementation optimized for AMD64.
/
/  Author: Marc Bevand <bevand_m (at) epita.fr>
/  Licence: I hereby disclaim the copyright on this code and place it
/  in the public domain.
/
/  The code has been designed to be easily integrated into openssl:
/  the exported RC4() function can replace the actual implementations
/  openssl already contains. Please note that when linking with openssl,
/  it requires that sizeof(RC4_INT) == 8. So openssl must be compiled
/  with -DRC4_INT='unsigned long'.
/
/  The throughput achieved by this code is about 320 MBytes/sec, on
/  a 1.8 GHz AMD Opteron (rev C0) processor.


/ ***** BEGIN LICENSE BLOCK *****
/ Version: MPL 1.1/GPL 2.0/LGPL 2.1
/
/ The contents of this file are subject to the Mozilla Public License Version
/ 1.1 (the "License"); you may not use this file except in compliance with
/ the License. You may obtain a copy of the License at
/ http://www.mozilla.org/MPL/
/
/ Software distributed under the License is distributed on an "AS IS" basis,
/ WITHOUT WARRANTY OF ANY KIND, either express or implied. See the License
/ for the specific language governing rights and limitations under the
/ License.
/
/ The Original Code is "Marc Bevand's fast AMD64 ARCFOUR source"
/
/ The Initial Developer of the Original Code is
/ Marc Bevand <bevand_m@epita.fr> .
/ Portions created by the Initial Developer are
/ Copyright (C) 2004 the Initial Developer. All Rights Reserved.
/
/ Contributor(s):
/
/ Alternatively, the contents of this file may be used under the terms of
/ either the GNU General Public License Version 2 or later (the "GPL"), or
/ the GNU Lesser General Public License Version 2.1 or later (the "LGPL"),
/ in which case the provisions of the GPL or the LGPL are applicable instead
/ of those above. If you wish to allow use of your version of this file only
/ under the terms of either the GPL or the LGPL, and not to allow others to
/ use your version of this file under the terms of the MPL, indicate your
/ decision by deleting the provisions above and replace them with the notice
/ and other provisions required by the GPL or the LGPL. If you do not delete
/ the provisions above, a recipient may use your version of this file under
/ the terms of any one of the MPL, the GPL or the LGPL.
/
/ ***** END LICENSE BLOCK *****

        .ident  "@(#)arcfour_crypt_amd64.s      1.1     08/01/02 SMI"

/
/ void arcfour_crypt(ARCFour_key *key, uchar_t *in,
/               uchar_t *out, size_t len);
/
/ The following is Marc Bevand's RC4 implementation optimized for
/ AMD64.  It has been lifted intact, except for minor interface
```



```
/ changes to get along with Solaris crypto common code (the parameter
/ order and the key struct element order are both different).
/ This function works for both aligned and unaligned data ('in' and 'out').
/ The key and key elements must be aligned.
/
/ Register Usage
/ rax           data[x]
/ rbx           ARG(len)
/ rcx           key->i (aka x)
/ rdx           key->j (aka y)
/ rsi           ARG(in)
/ rdi           ARG(out)
/ rbp           key->arr (aka data or d)
/ rsp           stack
/ r8            8 bytes of rc4 stream
/ r9            temp
/ r10-r15       unused
/

#include <sys/asm_linkage.h>


        ENTRY_NP(arcfour_crypt)
        /* EXPORT DELETE START */
                                        / load parameters
        push    %rbp
        push    %rbx
        mov     %rdi,           %rbp    / rbp = ARG(key)
                                        / rsi = ARG(in)
        mov     %rdx,           %rdi    / rdi = ARG(out)
        mov     %rcx,           %rbx    / rbx = ARG(len)

                                        / load key indices and key
        mov     2048(%rbp),     %rcx    / rcx x = key->i
        mov     2056(%rbp),     %rdx    / rdx y = key->j
                                        / rbp d = key->arr
        inc     %rcx                    / x++
        and     $255,           %rcx    / x &= 0xff
        lea     -8(%rbx,%rsi),  %rbx    / rbx = in+len-8
        mov     %rbx,           %r9     / tmp = in+len-8
        mov     (%rbp,%rcx,8),  %rax    / tx = d[x]
        cmp     %rsi,           %rbx    / cmp in with in+len-8
        jl      .Lend                   / jump if (in+len-8 < in)

.Lstart:
        add     $8,             %rsi            / increment in
        add     $8,             %rdi            / increment out

        / generate the next 8 bytes of the rc4 stream into %r8
        mov     $8,             %r11            / byte counter
1:      add     %al,            %dl             / y += tx
        mov     (%rbp,%rdx,8),  %ebx            / ty = d[y]
        mov     %ebx,           (%rbp,%rcx,8)   / d[x] = ty
        add     %al,            %bl             / val = ty + tx
        mov     %eax,           (%rbp,%rdx,8)   / d[y] = tx
        inc     %cl                             / x++           (NEXT ROUND)
        mov     (%rbp,%rcx,8),  %eax            / tx = d[x]     (NEXT ROUND)
        movb    (%rbp,%rbx,8),  %r8b            / val = d[val]
        dec     %r11b
        ror     $8,             %r8             / (ror does not change ZF)
        jnz     1b

        / xor 8 bytes
        xor     -8(%rsi),       %r8
        cmp     %r9,            %rsi            / cmp in+len-8 with in
        mov     %r8,            -8(%rdi)
```

```
128         jle     .Lstart                         / jump if (in <= in+len-8)

130 .Lend:
131         add     $8,             %r9             / tmp = in+len

133         / handle the last bytes, one by one
134 1:      cmp     %rsi,           %r9             / cmp in with in+len
135         jle     .Lfinished                      / jump if (in+len <= in)
136         add     %al,            %dl             / y += tx
137         mov     (%rbp,%rdx,8),  %ebx            / ty = d[y]
138         mov     %ebx,           (%rbp,%rcx,8)   / d[x] = ty
139         add     %al,            %bl             / val = ty + tx
140         mov     %eax,           (%rbp,%rdx,8)   / d[y] = tx
141         inc     %cl                             / x++           (NEXT ROUND)
142         mov     (%rbp,%rcx,8),  %eax            / tx = d[x]     (NEXT ROUND)
143         movb    (%rbp,%rbx,8),  %r8b            / val = d[val]
144         xor     (%rsi),         %r8b            / xor 1 byte
145         movb    %r8b,           (%rdi)
146         inc     %rsi                            / in++
147         inc     %rdi                            / out++
148         jmp     1b

150 .Lfinished:                                     / save key indices i & j
151         dec     %rcx                            / x--
152         movb    %dl,            2056(%rbp)      / key->j = y
153         movb    %cl,            2048(%rbp)      / key->i = x
154         pop     %rbx
155         pop     %rbp

157         /* EXPORT DELETE END */

159         ret
160         SET_SIZE(arcfour_crypt)

162 #else
163         /* LINTED */
164         /* Nothing to be linted in this file--it's pure assembly source. */
165 #endif /* !lint && !__lint */
```

```
**********************************************************
    1582 Mon Mar 24 15:31:30 2008
new/usr/src/cmd/cmd-crypto/digest/Makefile
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile   1.6     08/03/20 SMI"
# ident "@(#)Makefile   1.5     07/02/02 SMI"
#

PROG= digest
ROOTLINK= $(ROOTBIN)/mac
DCFILE= $(PROG).dc
PROG = digest

OBJS = digest.o

SRCS = $(OBJS:.o=.c)

include ../../Makefile.cmd

SUBDIRS= $(MACH)
$(BUILD64)SUBDIRS += $(MACH64)
CFLAGS += $(CCVERBOSE) -D_FILE_OFFSET_BITS=64

all     :=      TARGET = all
install :=      TARGET = install
clean   :=      TARGET = clean
clobber :=      TARGET = clobber
lint    :=      TARGET = lint
LDLIBS += -lkmf -lpkcs11 -lcryptoutil

.KEEP_STATE:

all clean clobber lint:    $(SUBDIRS)
all:    $(PROG)

install:        $(SUBDIRS)
        -$(RM) $(ROOTPROG) $(ROOTLINK)
        -$(LN) $(ISAEXEC) $(ROOTPROG)
        -$(LN) $(ISAEXEC) $(ROOTLINK)
$(PROG): $(OBJS)
```



```
        $(LINK.c) $(OBJS) -o $@ $(LDLIBS) $(DYNFLAGS)
        $(POST_PROCESS)

$(SUBDIRS):     FRC
        @cd $@; pwd; $(MAKE) $(TARGET)
install: all $(ROOTPROG)
        $(RM) $(ROOTBIN)/mac
        $(LN) $(ROOTPROG) $(ROOTBIN)/mac

$(DCFILE):
        $(RM) messages.po
        $(XGETTEXT) $(XGETFLAGS) -t $(PROG).c
        $(SED) -e '/^domain/d' messages.po > $@
        $(RM) messages.po
clean:
        $(RM) -f $(OBJS) $(PROG)

FRC:
lint:   lint_SRCS

include ../../Makefile.targ
```

```
**********************************************************
    1566 Mon Mar 24 15:31:35 2008
new/usr/src/cmd/cmd-crypto/digest/Makefile.com
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile.com       1.1     08/03/20 SMI"
#

PROG = digest

ROOTLINK32= $(ROOTBIN32)/mac
ROOTLINK64= $(ROOTBIN64)/mac

OBJS = digest.o

SRCS = $(OBJS:%.o=../%.c)

include ../../../Makefile.cmd

CFLAGS += $(CCVERBOSE)
CFLAGS64 += $(CCVERBOSE)
CPPFLAGS +=-D_FILE_OFFSET_BITS=64

LDLIBS += -lkmf -lpkcs11 -lcryptoutil

.KEEP_STATE:

all:    $(PROG)

lint: lint_SRCS

include ../../../Makefile.targ

%.o:    ../%.c
        $(COMPILE.c) $<

$(PROG): $(OBJS)
        $(LINK.c) $(OBJS) -o $@ $(LDLIBS) $(DYNFLAGS)
        $(POST_PROCESS)

$(ROOTLINK32): $(ROOTPROG32)
        $(RM) $@
```



```
        $(LN) $(ROOTPROG32) $@

$(ROOTLINK64): $(ROOTPROG64)
        $(RM) $@
        $(LN) $(ROOTPROG64) $@

clean:
        $(RM) $(PROG) $(OBJS)
```

```
**********************************************************
    1042 Mon Mar 24 15:31:36 2008
new/usr/src/cmd/cmd-crypto/digest/amd64/Makefile
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)Makefile   1.1     08/03/20 SMI"
  26 #

  28 include ../Makefile.com
  29 include ../../../Makefile.cmd.64

  31 install: all $(ROOTPROG64) $(ROOTLINK64)
```

```
**********************************************************
   23467 Mon Mar 24 15:31:38 2008
new/usr/src/cmd/cmd-crypto/digest/digest.c
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License (the "License").
 * You may not use this file except in compliance with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#pragma ident   "@(#)digest.c   1.12    08/03/20 SMI"
#pragma ident   "@(#)digest.c   1.11    07/10/04 SMI"

/*
 * digest.c
 *
 * Implements digest(1) and mac(1) commands
 * If command name is mac, performs mac operation
 * else perform digest operation
 *
 * See the man pages for digest and mac for details on
 * how these commands work.
 */

#include <stdio.h>
#include <stdlib.h>
#include <unistd.h>
#include <fcntl.h>
#include <ctype.h>
#include <strings.h>
#include <libintl.h>
#include <libgen.h>
#include <locale.h>
#include <errno.h>
#include <sys/types.h>
#include <sys/stat.h>
#include <security/cryptoki.h>
#include <limits.h>
#include <cryptoutil.h>
#include <kmfapi.h>

#define BUFFERSIZE      (4096)          /* Buffer size for reading file */

/*
 * RESULTLEN - large enough size in bytes to hold result for
```



```
 * digest and mac results for all mechanisms
 */
#define RESULTLEN       (512)

/*
 * Exit Status codes
 */
#ifndef EXIT_SUCCESS
#define EXIT_SUCCESS    0       /* No errors */
#define EXIT_FAILURE    1       /* All errors except usage */
#endif /* EXIT_SUCCESS */

#define EXIT_USAGE      2       /* usage/syntax error */

#define MAC_NAME        "mac"           /* name of mac command */
#define MAC_OPTIONS     "lva:k:T:K:"            /* for getopt */
#define DIGEST_NAME     "digest"        /* name of mac command */
#define DIGEST_OPTIONS  "lva:"          /* for getopt */

static boolean_t vflag = B_FALSE;       /* -v (verbose) flag, optional */
static boolean_t aflag = B_FALSE;       /* -a <algorithm> flag, required */
static boolean_t lflag = B_FALSE;       /* -l flag, for mac and digest */
static boolean_t kflag = B_FALSE;
static boolean_t Tflag = B_FALSE;
static boolean_t Kflag = B_FALSE;

static char *keyfile = NULL;    /* name of keyfile */
static char *token_label = NULL;
static char *key_label = NULL;

static CK_BYTE buf[BUFFERSIZE];

struct mech_alias {
        CK_MECHANISM_TYPE type;
        char *alias;
        CK_ULONG keysize_min;
        CK_ULONG keysize_max;
        int keysize_unit;
        boolean_t available;
};
```

*unchanged_portion_omitted_*

```
/*
 * Execute the command.
 *   algo_str - name of algorithm
 *   filecount - no. of files to process, if 0, use stdin
 *   filelist - list of files
 *   mac_cmd - if true do mac else do digest
 */
static int
execute_cmd(char *algo_str, int filecount, char **filelist, boolean_t mac_cmd)
{
        int fd;
        char *filename = NULL;
        CK_RV rv;
        CK_ULONG slotcount;
        CK_SLOT_ID slotID;
        CK_SLOT_ID_PTR pSlotList = NULL;
        CK_MECHANISM_TYPE mech_type;
        CK_MECHANISM_INFO info;
        CK_MECHANISM mech;
        CK_SESSION_HANDLE hSession = CK_INVALID_HANDLE;
        CK_BYTE_PTR resultbuf = NULL;
        CK_ULONG resultlen;
        CK_BYTE_PTR     pkeydata = NULL;
```

```
373         CK_OBJECT_HANDLE key = (CK_OBJECT_HANDLE) 0;
374         size_t keylen = 0;              /* key length */
374         int keylen = 0;         /* key length */
375         char *resultstr = NULL; /* result in hex string */
376         int resultstrlen;       /* result string length */
377         int i;
378         int exitcode = EXIT_SUCCESS;            /* return code */
379         int slot, mek;                  /* index variables */
380         int mech_match = 0;
381         CK_BYTE         salt[CK_PKCS5_PBKD2_SALT_SIZE];
382         CK_ULONG        keysize;
383         CK_ULONG        iterations = CK_PKCS5_PBKD2_ITERATIONS;
384         CK_KEY_TYPE keytype;
385         KMF_RETURN kmfrv;
386         CK_SLOT_ID token_slot_id;

388         if (aflag) {
389                 /*
390                  * Determine if algorithm/mechanism is valid
391                  */
392                 for (mech_match = 0; mech_match < MECH_ALIASES_COUNT;
393                     mech_match++) {
394                         if (strcmp(algo_str,
395                             mech_aliases[mech_match].alias) == 0) {
396                                 mech_type = mech_aliases[mech_match].type;
397                                 break;
398                         }

400                 }

402                 if (mech_match == MECH_ALIASES_COUNT) {
403                         cryptoerror(LOG_STDERR,
404                             gettext("unknown algorithm -- %s"), algo_str);
405                         return (EXIT_FAILURE);
406                 }

408                 /* Get key to do a MAC operation */
409                 if (mac_cmd) {
410                         int status;

412                         if (Kflag) {
413                                 /* get the pin of the token */
414                                 if (token_label == NULL ||
415                                     !strlen(token_label)) {
416                                         token_label = pkcs11_default_token();
417                                 }

419                                 status = pkcs11_get_pass(token_label,
420                                     (char **)&pkeydata, &keylen,
420                                     (char **)&pkeydata, (size_t *)&keylen,
421                                     0, B_FALSE);
422                         } else if (keyfile != NULL) {
423                                 /* get the key file */
424                                 status = pkcs11_read_data(keyfile,
425                                     (void **)&pkeydata, &keylen);
425                                     (void **)&pkeydata, (size_t *)&keylen);
426                         } else {
427                                 /* get the key from input */
428                                 status = pkcs11_get_pass(NULL,
429                                     (char **)&pkeydata, &keylen,
429                                     (char **)&pkeydata, (size_t *)&keylen,
430                                     0, B_FALSE);
431                         }

433                         if (status == -1 || keylen == 0 || pkeydata == NULL) {
434                                 cryptoerror(LOG_STDERR,
```



```
435                                     Kflag ? gettext("invalid passphrase.") :
436                                     gettext("invalid key."));
437                                 return (EXIT_FAILURE);
438                         }
439                 }
440         }

442         /* Initialize, and get list of slots */
443         rv = C_Initialize(NULL);
444         if (rv != CKR_OK && rv != CKR_CRYPTOKI_ALREADY_INITIALIZED) {
445                 cryptoerror(LOG_STDERR,
446                     gettext("failed to initialize PKCS #11 framework: %s"),
447                     pkcs11_strerror(rv));
448                 return (EXIT_FAILURE);
449         }

451         /* Get slot count */
452         rv = C_GetSlotList(0, NULL_PTR, &slotcount);
453         if (rv != CKR_OK || slotcount == 0) {
454                 cryptoerror(LOG_STDERR, gettext(
455                     "failed to find any cryptographic provider,"
456                     "please check with your system administrator: %s"),
457                     pkcs11_strerror(rv));
458                 exitcode = EXIT_FAILURE;
459                 goto cleanup;
460         }

462         /* Found at least one slot, allocate memory for slot list */
463         pSlotList = malloc(slotcount * sizeof (CK_SLOT_ID));
464         if (pSlotList == NULL_PTR) {
465                 int err = errno;
466                 cryptoerror(LOG_STDERR, gettext("malloc: %s\n"),
467                     strerror(err));
468                 exitcode = EXIT_FAILURE;
469                 goto cleanup;
470         }

472         /* Get the list of slots */
473         if ((rv = C_GetSlotList(0, pSlotList, &slotcount)) != CKR_OK) {
474                 cryptoerror(LOG_STDERR, gettext(
475                     "failed to find any cryptographic provider,"
476                     "please check with your system administrator: %s"),
477                     pkcs11_strerror(rv));
478                 exitcode = EXIT_FAILURE;
479                 goto cleanup;
480         }

482         /*
483          * Obtain list of algorithms if -l option was given
484          */
485         if (lflag) {

487                 for (slot = 0; slot < slotcount; slot++) {

489                         /* Iterate through each mechanism */
490                         for (mek = 0; mek < MECH_ALIASES_COUNT; mek++) {
491                                 rv = C_GetMechanismInfo(pSlotList[slot],
492                                     mech_aliases[mek].type, &info);

494                                 /* Only check algorithms that can be used */
495                                 if ((rv != CKR_OK) ||
496                                     (!mac_cmd && (info.flags & CKF_SIGN)) ||
497                                     (mac_cmd && (info.flags & CKF_DIGEST)))
498                                         continue;

500                                 /*
```

```
501                                 * Set to minimum/maximum key sizes assuming
502                                 * the values available are not 0.
503                                 */
504                                if (info.ulMinKeySize && (info.ulMinKeySize <
505                                    mech_aliases[mek].keysize_min))
506                                        mech_aliases[mek].keysize_min =
507                                            info.ulMinKeySize;

509                                if (info.ulMaxKeySize && (info.ulMaxKeySize >
510                                    mech_aliases[mek].keysize_max))
511                                        mech_aliases[mek].keysize_max =
512                                            info.ulMaxKeySize;

514                                mech_aliases[mek].available = B_TRUE;
515                        }

517                }

519                algorithm_list(mac_cmd);

521                goto cleanup;
522        }

524        /*
525         * Find a slot with matching mechanism
526         *
527         * If -K is specified, we find the slot id for the token first, then
528         * check if the slot supports the algorithm.
529         */
530        i = 0;
531        if (Kflag) {
532                kmfrv = kmf_pk11_token_lookup(NULL, token_label,
533                    &token_slot_id);
534                if (kmfrv != KMF_OK) {
535                        cryptoerror(LOG_STDERR,
536                            gettext("no matching PKCS#11 token"));
537                        exitcode = EXIT_FAILURE;
538                        goto cleanup;
539                }
540                rv = C_GetMechanismInfo(token_slot_id, mech_type, &info);
541                if (rv == CKR_OK && (info.flags & CKF_SIGN))
542                        slotID = token_slot_id;
543                else
544                        i = slotcount;

546        } else {
547                for (i = 0; i < slotcount; i++) {
548                        slotID = pSlotList[i];
549                        rv = C_GetMechanismInfo(slotID, mech_type, &info);
550                        if (rv != CKR_OK) {
551                                continue; /* to the next slot */
552                        } else {
553                                if (mac_cmd) {
554                                        /*
555                                         * Make sure the slot supports
556                                         * PKCS5 key generation if we
557                                         * will be using it later.
558                                         * We use it whenever the key
559                                         * is entered at command line.
560                                         */
561                                        if ((info.flags & CKF_SIGN) &&
562                                            (keyfile == NULL)) {
563                                                CK_MECHANISM_INFO kg_info;
564                                                rv = C_GetMechanismInfo(slotID,
565                                                    CKM_PKCS5_PBKD2, &kg_info);
566                                                if (rv == CKR_OK)
```



```
567                                                        break;
568                                        } else if (info.flags & CKF_SIGN) {
569                                                break;
570                                        }
571                                } else {
572                                        if (info.flags & CKF_DIGEST)
573                                                break;
574                                }
575                        }
576                }
577        }

579        /* Show error if no matching mechanism found */
580        if (i == slotcount) {
581                cryptoerror(LOG_STDERR,
582                    gettext("no cryptographic provider was "
583                    "found for this algorithm -- %s"), algo_str);
584                exitcode = EXIT_FAILURE;
585                goto cleanup;
586        }

588        /* Mechanism is supported. Go ahead & open a session */
589        rv = C_OpenSession(slotID, CKF_SERIAL_SESSION,
590            NULL_PTR, NULL, &hSession);

592        if (rv != CKR_OK) {
593                cryptoerror(LOG_STDERR,
594                    gettext("can not open PKCS#11 session: %s"),
595                    pkcs11_strerror(rv));
596                exitcode = EXIT_FAILURE;
597                goto cleanup;
598        }

600        /* Create a key object for mac operation */
601        if (mac_cmd) {
602                /*
603                 * If we read keybytes from a file,
604                 * do NOT process them with C_GenerateKey,
605                 * treat them as raw keydata bytes and
606                 * create a key object for them.
607                 */
608                if (keyfile) {
609                        /* XXX : why wasn't SUNW_C_KeyToObject used here? */
610                        CK_OBJECT_CLASS class = CKO_SECRET_KEY;
611                        CK_KEY_TYPE tmpl_keytype = CKK_GENERIC_SECRET;
612                        CK_BBOOL false = FALSE;
613                        int nattr = 0;
614                        CK_ATTRIBUTE template[5];

616                        if (mech_type == CKM_DES_MAC) {
617                                tmpl_keytype = CKK_DES;
618                        }
619                        template[nattr].type = CKA_CLASS;
620                        template[nattr].pValue = &class;
621                        template[nattr].ulValueLen = sizeof (class);
622                        nattr++;

624                        template[nattr].type = CKA_KEY_TYPE;
625                        template[nattr].pValue = &tmpl_keytype;
626                        template[nattr].ulValueLen = sizeof (tmpl_keytype);
627                        nattr++;

629                        template[nattr].type = CKA_SIGN;
630                        template[nattr].pValue = &true;
631                        template[nattr].ulValueLen = sizeof (true);
632                        nattr++;
```

```
634                         template[nattr].type = CKA_TOKEN;
635                         template[nattr].pValue = &false;
636                         template[nattr].ulValueLen = sizeof (false);
637                         nattr++;

639                         template[nattr].type = CKA_VALUE;
640                         template[nattr].pValue = pkeydata;
641                         template[nattr].ulValueLen = keylen;
642                         nattr++;

644                         rv = C_CreateObject(hSession, template, nattr, &key);

646                 } else if (Kflag) {

648                         if (mech_type == CKM_DES_MAC) {
649                                 keytype = CKK_DES;
650                         } else {
651                                 keytype = CKK_GENERIC_SECRET;
652                         }

654                         rv = get_token_key(hSession, keytype, key_label,
655                             pkeydata, keylen, &key);
656                         if (rv != CKR_OK) {
657                                 exitcode = EXIT_FAILURE;
658                                 goto cleanup;
659                         }
660                 } else {
661                         CK_KEY_TYPE keytype;
662                         if (mech_type == CKM_DES_MAC) {
663                                 keytype = CKK_DES;
664                                 keysize = 0;
665                         } else {
666                                 keytype = CKK_GENERIC_SECRET;
667                                 keysize = 16; /* 128 bits */
668                         }
669                         /*
670                          * We use a fixed salt (0x0a, 0x0a, 0x0a ...)
671                          * for creating the key so that the end user
672                          * will be able to generate the same 'mac'
673                          * using the same passphrase.
674                          */
675                         (void) memset(salt, 0x0a, sizeof (salt));
676                         rv = pkcs11_PasswdToPBKD2Object(hSession,
677                             (char *)pkeydata, (size_t)keylen, (void *)salt,
678                             sizeof (salt), iterations, keytype, keysize,
679                             CKF_SIGN, &key);
680                 }

682                 if (rv != CKR_OK) {
683                         cryptoerror(LOG_STDERR,
684                             gettext("unable to create key for crypto "
685                             "operation: %s"), pkcs11_strerror(rv));
686                         exitcode = EXIT_FAILURE;
687                         goto cleanup;
688                 }
689         }

691         /* Allocate a buffer to store result. */
692         resultlen = RESULTLEN;
693         if ((resultbuf = malloc(resultlen)) == NULL) {
694                 int err = errno;
695                 cryptoerror(LOG_STDERR, gettext("malloc: %s\n"),
696                     strerror(err));
697                 exitcode = EXIT_FAILURE;
698                 goto cleanup;
```



```
699         }

701         /* Allocate a buffer to store result string */
702         resultstrlen = RESULTLEN;
703         if ((resultstr = malloc(resultstrlen)) == NULL) {
704                 int err = errno;
705                 cryptoerror(LOG_STDERR, gettext("malloc: %s\n"),
706                     strerror(err));
707                 exitcode = EXIT_FAILURE;
708                 goto cleanup;
709         }

711         mech.mechanism = mech_type;
712         mech.pParameter = NULL_PTR;
713         mech.ulParameterLen = 0;
714         exitcode = EXIT_SUCCESS;
715         i = 0;

717         do {
718                 if (filecount > 0 && filelist != NULL) {
719                         filename = filelist[i];
720                         if ((fd = open(filename, O_RDONLY | O_NONBLOCK)) ==
721                             -1) {
722                                 cryptoerror(LOG_STDERR, gettext(
723                                     "can not open input file %s\n"), filename);
724                                 exitcode = EXIT_USAGE;
725                                 continue;
726                         }
727                 } else {
728                         fd = 0; /* use stdin */
729                 }

731                 /*
732                  * Perform the operation
733                  */
734                 if (mac_cmd) {
735                         rv = do_mac(hSession, &mech, fd, key, &resultbuf,
736                             &resultlen);
737                 } else {
738                         rv = do_digest(hSession, &mech, fd, &resultbuf,
739                             &resultlen);
740                 }

742                 if (rv != CKR_OK) {
743                         cryptoerror(LOG_STDERR,
744                             gettext("crypto operation failed for "
745                             "file %s: %s\n"),
746                             filename ? filename : "STDIN",
747                             pkcs11_strerror(rv));
748                         exitcode = EXIT_FAILURE;
749                         continue;
750                 }

752                 /* if result size has changed, allocate a bigger resulstr buf */
753                 if (resultlen != RESULTLEN) {
754                         resultstrlen = 2 * resultlen + 1;
755                         resultstr = realloc(resultstr, resultstrlen);

757                         if (resultstr == NULL) {
758                                 int err = errno;
759                                 cryptoerror(LOG_STDERR,
760                                     gettext("realloc: %s\n"), strerror(err));
761                                 exitcode =  EXIT_FAILURE;
762                                 goto cleanup;
763                         }
764                 }
```

```
766                 /* Output the result */
767                 tohexstr(resultbuf, resultlen, resultstr, resultstrlen);

769                 /* Include mechanism name for verbose */
770                 if (vflag)
771                         (void) fprintf(stdout, "%s ", algo_str);

773                 /* Include file name for multiple files, or if verbose */
774                 if (filecount > 1 || (vflag && filecount > 0)) {
775                         (void) fprintf(stdout, "(%s) = ", filename);
776                 }

778                 (void) fprintf(stdout, "%s\n", resultstr);
779                 (void) close(fd);


782         } while (++i < filecount);


785         /* clear and free the key */
786         if (mac_cmd) {
787                 (void) memset(pkeydata, 0, keylen);
788                 free(pkeydata);
789                 pkeydata = NULL;
790         }

792 cleanup:
793         if (resultbuf != NULL) {
794                 free(resultbuf);
795         }

797         if (resultstr != NULL) {
798                 free(resultstr);
799         }

801         if (pSlotList != NULL) {
802                 free(pSlotList);
803         }

805         if (!Kflag && key != (CK_OBJECT_HANDLE) 0) {
806                 (void) C_DestroyObject(hSession, key);
807         }

809         if (hSession != CK_INVALID_HANDLE)
810                 (void) C_CloseSession(hSession);

812         (void) C_Finalize(NULL_PTR);

814         return (exitcode);
815 }
```

_____***unchanged_portion_omitted_***

```
**********************************************************
    1009 Mon Mar 24 15:31:42 2008
new/usr/src/cmd/cmd-crypto/digest/i386/Makefile
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile   1.1     08/03/20 SMI"
#

include ../Makefile.com

install: all $(ROOTPROG32) $(ROOTLINK32)
```

```
**********************************************************
    1009 Mon Mar 24 15:31:44 2008
new/usr/src/cmd/cmd-crypto/digest/sparc/Makefile
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)Makefile   1.1     08/03/20 SMI"
  26 #

  28 include ../Makefile.com

  30 install: all $(ROOTPROG32) $(ROOTLINK32)
```

```
**********************************************************
    1042 Mon Mar 24 15:31:46 2008
new/usr/src/cmd/cmd-crypto/digest/sparcv9/Makefile
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)Makefile   1.1     08/03/20 SMI"
  26 #

  28 include ../Makefile.com
  29 include ../../../Makefile.cmd.64

  31 install: all $(ROOTPROG64) $(ROOTLINK64)
```

```
**********************************************************
    1758 Mon Mar 24 15:31:48 2008
new/usr/src/common/crypto/arcfour/amd64/THIRDPARTYLICENSE
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
Copyright (c) 2006, CRYPTOGAMS by <appro@openssl.org>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

      * Redistributions of source code must retain copyright notices,
        this list of conditions and the following disclaimer.

      * Redistributions in binary form must reproduce the above
        copyright notice, this list of conditions and the following
        disclaimer in the documentation and/or other materials
        provided with the distribution.

      * Neither the name of the CRYPTOGAMS nor the names of its
        copyright holder and contributors may be used to endorse or
        promote products derived from this software without specific
        prior written permission.

ALTERNATIVELY, provided that this notice is retained in full, this
product may be distributed under the terms of the GNU General Public
License (GPL), in which case the provisions of the GPL apply INSTEAD OF
those given above.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
**********************************************************
      34 Mon Mar 24 15:31:50 2008
new/usr/src/common/crypto/arcfour/amd64/THIRDPARTYLICENSE.descrip
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
   1 PORTIONS OF ARCFOUR FUNCTIONALITY
```

```
**********************************************************
   10756 Mon Mar 24 15:31:51 2008
new/usr/src/common/crypto/arcfour/amd64/arcfour-x86_64.pl
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
```

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@fy.chalmers.se> for the OpenSSL
# project. The module is, however, dual licensed under OpenSSL and
# CRYPTOGAMS licenses depending on where you obtain it. For further
# details see http://www.openssl.org/~appro/cryptogams/.
# ====================================================================
#
# 2.22x RC4 tune-up:-) It should be noted though that my hand [as in
# "hand-coded assembler"] doesn't stand for the whole improvement
# coefficient. It turned out that eliminating RC4_CHAR from config
# line results in ~40% improvement (yes, even for C implementation).
# Presumably it has everything to do with AMD cache architecture and
# RAW or whatever penalties. Once again! The module *requires* config
# line *without* RC4_CHAR! As for coding "secret," I bet on partial
# register arithmetics. For example instead of 'inc %r8; and $255,%r8'
# I simply 'inc %r8b'. Even though optimization manual discourages
# to operate on partial registers, it turned out to be the best bet.
# At least for AMD... How IA32E would perform remains to be seen...

# As was shown by Marc Bevand reordering of couple of load operations
# results in even higher performance gain of 3.3x:-) At least on
# Opteron... For reference, 1x in this case is RC4_CHAR C-code
# compiled with gcc 3.3.2, which performs at ~54MBps per 1GHz clock.
# Latter means that if you want to *estimate* what to expect from
# *your* Opteron, then multiply 54 by 3.3 and clock frequency in GHz.

# Intel P4 EM64T core was found to run the AMD64 code really slow...
# The only way to achieve comparable performance on P4 was to keep
# RC4_CHAR. Kind of ironic, huh? As it's apparently impossible to
# compose blended code, which would perform even within 30% marginal
# on either AMD and Intel platforms, I implement both cases. See
# rc4_skey.c for further details...

# P4 EM64T core appears to be "allergic" to 64-bit inc/dec. Replacing
# those with add/sub results in 50% performance improvement of folded
# loop...

# As was shown by Zou Nanhai loop unrolling can improve Intel EM64T
# performance by >30% [unlike P4 32-bit case that is]. But this is
# provided that loads are reordered even more aggressively! Both code
# pathes, AMD64 and EM64T, reorder loads in essentially same manner
# as my IA-64 implementation. On Opteron this resulted in modest 5%
# improvement [I had to test it], while final Intel P4 performance
# achieves respectful 432MBps on 2.8GHz processor now. For reference.
# If executed on Xeon, current RC4_CHAR code-path is 2.7x faster than
# RC4_INT code-path. While if executed on Opteron, it's only 25%
# slower than the RC4_INT one [meaning that if CPU µ-arch detection
# is not implemented, then this final RC4_CHAR code-path should be
# preferred, as it provides better *all-round* performance].

# Intel Core2 was observed to perform poorly on both code paths:-( It
# apparently suffers from some kind of partial register stall, which
# occurs in 64-bit mode only [as virtually identical 32-bit loop was
# observed to outperform 64-bit one by almost 50%]. Adding two movzb to
# cloop1 boosts its performance by 80%! This loop appears to be optimal
# fit for Core2 and therefore the code was modified to skip cloop8 on
# this CPU.

#
```



```
# OpenSolaris OS modifications
#
# Sun elects to use this software under the BSD license.
#
# This source originates from OpenSSL file rc4-x86_64.pl at
# ftp://ftp.openssl.org/snapshot/openssl-0.9.8-stable-SNAP-20080131.tar.gz
# (presumably for future OpenSSL release 0.9.8h), with these changes:
#
# 1. Added some comments, "use strict", and declared all variables.
#
# 2. Added OpenSolaris ENTRY_NP/SET_SIZE macros from
# /usr/include/sys/asm_linkage.h, .ident keywords, and lint(1B) guards.
#
# 3. Changed function name from RC4() to arcfour_crypt() and RC4_set_key()
# to arcfour_key_init(), and changed the parameter order for both to that
# used by OpenSolaris.
#
# 4. The current method of using cpuid feature bits 20 (NX) or 28 (HTT) from
# function OPENSSL_ia32_cpuid() to distinguish Intel/AMD does not work for
# some newer AMD64 processors, as these bits are set on both Intel EM64T
# processors and newer AMD64 processors.  I replaced this with code to use CPUID
# instruction subfunction EAX=0 to determine if we're running on "GenuineIntel"
# or not. The result decides whether to use a
#       * 1-byte key array (label .LRC4_CHAR, optimal on Intel EM64T) or a
#       * 4-byte key array (Labels .Lloop1 and .Lloop8, optimal on AMD64).
#
# 5. Removed x86_64-xlate.pl script (not needed for as(1) or gas(1) assemblers).
#
# 6. Removed Lcloop8 code (slower than Lcloop1 on EM64T and not used on AMD64).
#

use strict;
my ($code, $dat, $inp, $out, $len, $idx, $ido, $i, @XX, @TX, $YY, $TY);
my $output = shift;
open STDOUT,">$output";

#
# Parameters
#

# OpenSSL:
# void RC4(RC4_KEY *key, unsigned long len, const unsigned char *indata,
#       unsigned char *outdata);
#$dat="%rdi";       # arg1
#$len="%rsi";       # arg2
#$inp="%rdx";       # arg3
#$out="%rcx";       # arg4

# OpenSolaris:
# void arcfour_crypt(ARCFour_key *key, uchar_t *in, uchar_t *out, size_t len);
$dat="%rdi";        # arg1
$inp="%rsi";        # arg2
$out="%rdx";        # arg3
$len="%rcx";        # arg4

#
# Register variables
#
# $XX[0] is key->i (aka key->x), $XX[1] is a temporary.
# $TX[0] and $TX[1] are temporaries.
# $YY is key->j (aka key->y).
# $TY is a temporary.
#
@XX=("%r8","%r10");
@TX=("%r9","%r11");
$YY="%r12";
```

```
128 $TY="%r13";
129
130 $code=<<___;
131 #if !defined(lint) && !defined(__lint)
132
133         .ident  "@(#)arcfour-x86_64.pl  1.1     08/03/20 SMI"
134
135 #include <sys/asm_linkage.h>
136
137
138 ENTRY_NP(arcfour_crypt)
139         /* EXPORT DELETE START */
140
141         or      $len,$len # If (len == 0) return
142         jne     .Lentry
143         ret
144 .Lentry:
145         push    %r12
146         push    %r13
147
148         / Set $dat to beginning of array, key->arr[0]
149         add     \$8,$dat
150         / Get key->j
151         movl    -8($dat),$XX[0]#d
152         / Get key->i
153         movl    -4($dat),$YY#d
154
155         /
156         / Use a 1-byte data array, on Intel P4 EM64T,
157         / which is more efficient there,
158         / or a 4-byte data array (for AMD AMD64).
159         /
160
161         / If RC4_CHAR flag set (Intel EM64T), then use 1-byte array
162         cmpl    \$-1,256($dat)
163         je      .LRC4_CHAR
164         / otherwise use 4-byte integer array (AMD64)
165         inc     $XX[0]#b
166         movl    ($dat,$XX[0],4),$TX[0]#d
167         test    \$-8,$len
168         jz      .Lloop1
169         jmp     .Lloop8
170
171 .align  16
172 .Lloop8:
173         /
174         / This code is for use with a 4-byte integer data array, which is
175         / more efficient on AMD64 Athlon and Opteron-class processors.
176         /
177 ___
178 for ($i=0;$i<8;$i++) {
179 $code.=<<___;
180         add     $TX[0]#b,$YY#b
181         mov     $XX[0],$XX[1]
182         movl    ($dat,$YY,4),$TY#d
183         ror     \$8,%rax                        # ror is redundant when $i=0
184         inc     $XX[1]#b
185         movl    ($dat,$XX[1],4),$TX[1]#d
186         cmp     $XX[1],$YY
187         movl    $TX[0]#d,($dat,$YY,4)
188         cmove   $TX[0],$TX[1]
189         movl    $TY#d,($dat,$XX[0],4)
190         add     $TX[0]#b,$TY#b
191         movb    ($dat,$TY,4),%al
192 ___
193 push(@TX,shift(@TX)); push(@XX,shift(@XX));     # "rotate" registers
```



```
194 }
195 $code.=<<___;
196         ror     \$8,%rax
197         sub     \$8,$len
198
199         xor     ($inp),%rax
200         add     \$8,$inp
201         mov     %rax,($out)
202         add     \$8,$out
203
204         test    \$-8,$len
205         jnz     .Lloop8
206         cmp     \$0,$len
207         jne     .Lloop1
208 ___
209 $code.=<<___;
210 .Lexit:
211         /
212         / Cleanup and exit code
213         /
214         / --i to undo ++i done at entry
215         sub     \$1,$XX[0]#b
216         / set key->i
217         movl    $XX[0]#d,-8($dat)
218         / set key->j
219         movl    $YY#d,-4($dat)
220
221         pop     %r13
222         pop     %r12
223         ret
224 .align  16
225 .Lloop1:
226         add     $TX[0]#b,$YY#b
227         movl    ($dat,$YY,4),$TY#d
228         movl    $TX[0]#d,($dat,$YY,4)
229         movl    $TY#d,($dat,$XX[0],4)
230         add     $TY#b,$TX[0]#b
231         inc     $XX[0]#b
232         movl    ($dat,$TX[0],4),$TY#d
233         movl    ($dat,$XX[0],4),$TX[0]#d
234         xorb    ($inp),$TY#b
235         inc     $inp
236         movb    $TY#b,($out)
237         inc     $out
238         dec     $len
239         jnz     .Lloop1
240         jmp     .Lexit
241
242
243 .align  16
244 .LRC4_CHAR:
245         /
246         / This code is for use with a 1-byte integer data array, which is
247         / more efficient on Intel P4 EM64T-class processors.
248         /
249         add     \$1,$XX[0]#b
250         movzb   ($dat,$XX[0]),$TX[0]#d
251         jmp     .Lcloop1
252
253 .align  16
254 .Lcloop1:
255         add     $TX[0]#b,$YY#b
256         movzb   ($dat,$YY),$TY#d
257         movb    $TX[0]#b,($dat,$YY)
258         movb    $TY#b,($dat,$XX[0])
259         add     $TX[0]#b,$TY#b
```

```
260         add     \$1,$XX[0]#b
261         / Intel Optimization (preload $TY and $XX[0]):
262         movzb   $TY#b,$TY#d
263         movzb   $XX[0]#b,$XX[0]#d
264         movzb   ($dat,$TY),$TY#d
265         movzb   ($dat,$XX[0]),$TX[0]#d
266         xorb    ($inp),$TY#b
267         lea     1($inp),$inp
268         movb    $TY#b,($out)
269         lea     1($out),$out
270         sub     \$1,$len
271         jnz     .Lcloop1
272         jmp     .Lexit

274         /* EXPORT DELETE END */
275         ret
276 SET_SIZE(arcfour_crypt)
277 ___


280 #
281 # Parameters
282 #

284 # OpenSSL:
285 # void RC4_set_key(RC4_KEY *key, int len, const unsigned char *data);
286 #$dat="%rdi";       # arg1
287 #$len="%rsi";       # arg2
288 #$inp="%rdx";       # arg3

290 # OpenSolaris:
291 # void arcfour_key_init(ARCFour_key *key, uchar_t *keyval, int keyvallen);
292 $dat="%rdi";        # arg1
293 $inp="%rsi";        # arg2
294 $len="%rdx";        # arg3

296 # Temporaries
297 $idx="%r8";
298 $ido="%r9";

300 $code.=<<___;
301         / int arcfour_crypt_on_intel(void);
302 .extern arcfour_crypt_on_intel

304 ENTRY_NP(arcfour_key_init)
305         /* EXPORT DELETE START */

307         / Find out if we're running on Intel or something else (e.g., AMD64).
308         / This sets %eax to 1 for Intel, otherwise 0.
309         push    %rdi            / Save arg1
310         push    %rsi            / Save arg2
311         push    %rdx            / Save arg3
312         call    arcfour_crypt_on_intel
313         pop     %rdx            / Restore arg3
314         pop     %rsi            / Restore arg2
315         pop     %rdi            / Restore arg1

317         / Set $dat to beginning of array, key->arr[0]
318         lea     8($dat),$dat
319         lea     ($inp,$len),$inp
320         neg     $len
321         mov     $len,%rcx
322         / Zeroed below, as %eax contains a flag from arcfour_crypt_on_intel():
323         /xor    %eax,%eax
324         xor     $ido,$ido
325         xor     %r10,%r10
```



```
326         xor     %r11,%r11

328         /
329         / Use a 1-byte data array, on Intel P4 EM64T,
330         / which is more efficient there,
331         / or a 4-byte data array (for AMD AMD64).
332         /
333         cmp     \$1,%eax        / Test if Intel
334         mov     \$0,%eax        / Zero eax without modifying flags
335         je      .Lc1stloop      / If Intel then use a 1-byte array,
336         jmp     .Lw1stloop      / otherwise use a 4-byte array.

338 .align  16
339 .Lw1stloop:
340         / AMD64 (4-byte array)
341         mov     %eax,($dat,%rax,4)
342         add     \$1,%al
343         jnc     .Lw1stloop

345         xor     $ido,$ido
346         xor     $idx,$idx
347 .align  16
348 .Lw2ndloop:
349         mov     ($dat,$ido,4),%r10d
350         add     ($inp,$len,1),$idx#b
351         add     %r10b,$idx#b
352         add     \$1,$len
353         mov     ($dat,$idx,4),%r11d
354         cmovz   %rcx,$len
355         mov     %r10d,($dat,$idx,4)
356         mov     %r11d,($dat,$ido,4)
357         add     \$1,$ido#b
358         jnc     .Lw2ndloop
359         jmp     .Lexit_key

361 .align  16
362 .Lc1stloop:
363         / Intel EM64T (1-byte array)
364         mov     %al,($dat,%rax)
365         add     \$1,%al
366         jnc     .Lc1stloop

368         xor     $ido,$ido
369         xor     $idx,$idx
370 .align  16
371 .Lc2ndloop:
372         mov     ($dat,$ido),%r10b
373         add     ($inp,$len),$idx#b
374         add     %r10b,$idx#b
375         add     \$1,$len
376         mov     ($dat,$idx),%r11b
377         jnz     .Lcnowrap
378         mov     %rcx,$len
379 .Lcnowrap:
380         mov     %r10b,($dat,$idx)
381         mov     %r11b,($dat,$ido)
382         add     \$1,$ido#b
383         jnc     .Lc2ndloop
384         movl    \$-1,256($dat)

386 .align  16
387 .Lexit_key:
388         xor     %eax,%eax
389         mov     %eax,-8($dat)
390         mov     %eax,-4($dat)
```

```
392         /* EXPORT DELETE END */
393         ret
394 SET_SIZE(arcfour_key_init)
395 .asciz  "RC4 for x86_64, CRYPTOGAMS by <appro\@openssl.org>"

397 #else
398         /* LINTED */
399         /* Nothing to be linted in this file--it's pure assembly source. */
400 #endif /* !lint && !__lint */
401 ___

403 $code =~ s/#([bwd])/$1/gm;

405 print $code;

407 close STDOUT;
```

```
**********************************************************
    1726 Mon Mar 24 15:31:53 2008
new/usr/src/common/crypto/arcfour/arcfour.h
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License (the "License").
 * You may not use this file except in compliance with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#ifndef _ARCFOUR_H
#define _ARCFOUR_H

#pragma ident   "@(#)arcfour.h  1.7     08/03/20 SMI"
#pragma ident   "@(#)arcfour.h  1.6     07/03/29 SMI"

#ifdef __cplusplus
extern "C" {
#endif

#include <sys/types.h>
#include <sys/crypto/common.h>

#define ARCFOUR_MIN_KEY_BYTES   1

#define ARCFOUR_MAX_KEY_BYTES   256

#define ARCFOUR_MIN_KEY_BITS    (ARCFOUR_MIN_KEY_BYTES << 3)
#define ARCFOUR_MAX_KEY_BITS    (ARCFOUR_MAX_KEY_BYTES << 3)

typedef arcfour_state_t ARCFour_key;

void arcfour_key_init(ARCFour_key *key, uchar_t *keyval, int keyvallen);
void arcfour_crypt(ARCFour_key *key, uchar_t *in, uchar_t *out, size_t len);
#ifdef  sun4u
void arcfour_crypt_aligned(ARCFour_key *key, size_t len, uchar_t *in,
    uchar_t *out);
#endif  /* sun4u */
#ifdef  __amd64
int arcfour_crypt_on_intel(void);
#endif  /* _amd64 */

#ifdef  __cplusplus
}
_____unchanged_portion_omitted_
```

```
**********************************************************
    3539 Mon Mar 24 15:31:57 2008
new/usr/src/common/crypto/arcfour/arcfour_crypt.c
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
```

```
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License (the "License").
 * You may not use this file except in compliance with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#pragma ident   "@(#)arcfour_crypt.c    1.7     08/03/20 SMI"
#pragma ident   "@(#)arcfour_crypt.c    1.6     08/01/02 SMI"

#include "arcfour.h"

#if defined(__amd64)
#ifdef _KERNEL
#include <sys/x86_archext.h>
#include <sys/cpuvar.h>

#else
#include <sys/auxv.h>
#endif  /* _KERNEL */
/*
 * Use hand-tuned, processor-specific assembly version of arcfour_crypt()
 * for 64-bit x86:
 */
#define USE_PSR_VERSION_OF_ARCFOUR_CRYPT
#endif  /* __amd64 */

#if !defined(__amd64)
/* Initialize the key stream 'key' using the key value */
void
arcfour_key_init(ARCFour_key *key, uchar_t *keyval, int keyvallen)
{
/* EXPORT DELETE START */

        uchar_t ext_keyval[256];
        uchar_t tmp;
        int i, j;

        /* Normalize key length to 256 */
        for (i = j = 0; i < 256; i++, j++) {
                if (j == keyvallen)
                        j = 0;
```



```
                ext_keyval[i] = keyval[j];
        }

        for (i = 0; i < 256; i++)
                key->arr[i] = (uchar_t)i;

        j = 0;
        for (i = 0; i < 256; i++) {
                j = (j + key->arr[i] + ext_keyval[i]) % 256;
                tmp = key->arr[i];
                key->arr[i] = key->arr[j];
                key->arr[j] = tmp;
        }
        key->i = 0;
        key->j = 0;

/* EXPORT DELETE END */
}


#if !defined(USE_PSR_VERSION_OF_ARCFOUR_CRYPT)
/*
 * Encipher 'in' using 'key'.
 * in and out can point to the same location
 */
void
arcfour_crypt(ARCFour_key *key, uchar_t *in, uchar_t *out, size_t len)
{
        size_t ii;
        uchar_t tmp, i, j;

/* EXPORT DELETE START */

        /*
         * The sun4u has a version of arcfour_crypt_aligned() hand-tuned for
         * the cases where the input and output  buffers are aligned on
         * a multiple of 8-byte boundary.
         */
#ifdef  sun4u
        int index;

        index = (((uint64_t)(uintptr_t)in) & 0x7);

        /* Get the 'in' on an 8-byte alignment */
        if (index > 0) {
                i = key->i;
                j = key->j;
                for (index = 8 - (uint64_t)(uintptr_t)in & 0x7;
                    (index-- > 0) && len > 0;
                    len--, in++, out++) {
                        i = i + 1;
                        j = j + key->arr[i];
                        tmp = key->arr[i];
                        key->arr[i] = key->arr[j];
                        key->arr[j] = tmp;
                        tmp = key->arr[i] + key->arr[j];
                        *out = *in ^ key->arr[tmp];
                }
                key->i = i;
                key->j = j;

        }
        if (len == 0)
                return;

        /* See if we're fortunate and 'out' got aligned as well */
```

```
121         if ((((uint64_t)(uintptr_t)out) & 7) != 0) {
122 #endif  /* sun4u */
123                 i = key->i;
124                 j = key->j;
125                 for (ii = 0; ii < len; ii++) {
126                         i = i + 1;
127                         j = j + key->arr[i];
128                         tmp = key->arr[i];
129                         key->arr[i] = key->arr[j];
130                         key->arr[j] = tmp;
131                         tmp = key->arr[i] + key->arr[j];
132                         out[ii] = in[ii] ^ key->arr[tmp];
133                 }
134                 key->i = i;
135                 key->j = j;
136 #ifdef  sun4u
137         } else {
138                 arcfour_crypt_aligned(key, len, in, out);
139         }
140 #endif  /* sun4u */

142 /* EXPORT DELETE END */
143 }
145 #else

147 /*
148  * Return 1 if executing on Intel, otherwise 0 (e.g., AMD64).
149  */
150 int
151 arcfour_crypt_on_intel(void)
152 {
153 #ifdef _KERNEL
154         return (cpuid_getvendor(CPU) == X86_VENDOR_Intel);
155 #else
156         uint_t  ui;
157         (void) getisax(&ui, 1);
158         return ((ui & AV_386_AMD_MMX) == 0);
159 #endif  /* _KERNEL */
160 }
161 #endif  /* !__amd64 */
141 #endif  /* !USE_PSR_VERSION_OF_ARCFOUR_CRYPT */
```

****
9157 Mon Mar 24 15:32:02 2008
new/usr/src/common/crypto/sha1/amd64/sha1-x86_64.pl
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
****
_____unchanged_portion_omitted_

```
 146 #
 147 # void sha1_block_data_order(SHA1_CTX *ctx, const void *inpp, size_t blocks);
 148 #

 150 # Arguments:
 151 $ctx="%rdi";    # 1st arg
 152 $inp="%rsi";    # 2nd arg
 153 $num="%rdx";    # 3rd arg

 155 # reassign arguments in order to produce more compact code
 156 $ctx="%r8";
 157 $inp="%r9";
 158 $num="%r10";

 160 # Temporaries:
 161 $xi="%eax";
 162 $t0="%ebx";
 163 $t1="%ecx";
 164 # State information from SHA-1 context:
 165 $A="%edx";
 166 $B="%esi";
 167 $C="%edi";
 168 $D="%ebp";
 169 $E="%r11d";
 170 # Temporary:
 171 $T="%r12d";

 173 @V=($A,$B,$C,$D,$E,$T);

 175 sub PROLOGUE {
 176 my $func=shift;
 177 $code.=<<___;
 178 ENTRY_NP($func)
 179         /* EXPORT DELETE START */
 179         push    %rbx
 180         push    %rbp
 181         push    %r12
 182         mov     %rsp,%rax
 183         mov     %rdi,$ctx       # reassigned argument
 184         sub     \$'8+16*4',%rsp
 185         mov     %rsi,$inp       # reassigned argument
 186         and     \$-64,%rsp
 187         mov     %rdx,$num       # reassigned argument
 188         mov     %rax,'16*4'(%rsp)

 190         mov     0($ctx),$A
 191         mov     4($ctx),$B
 192         mov     8($ctx),$C
 193         mov     12($ctx),$D
 194         mov     16($ctx),$E
 195 ___
 196 }

 198 sub EPILOGUE {
 199 my $func=shift;
 200 $code.=<<___;
 201         mov     '16*4'(%rsp),%rsp
 202         pop     %r12
 203         pop     %rbp
 204         pop     %rbx
 206         /* EXPORT DELETE END */
 205         ret
 206 SET_SIZE($func)
```

_____unchanged_portion_omitted_


```
 319 $code=<<___;
 320 #if !defined(lint) && !defined(__lint)
 321         .ident  "@(#)sha1-x86_64.pl     1.2     08/03/20 SMI"
 323         .ident  "@(#)sha1-x86_64.pl     1.1     08/03/02 SMI"
 322 #include <sys/asm_linkage.h>
 323 ___


 326 &PROLOGUE("sha1_block_data_order");
 327 $code.=".align  4\n.Lloop:\n";
 328 for($i=0;$i<20;$i++)    { &BODY_00_19($i,@V); unshift(@V,pop(@V)); }
 329 for(;$i<40;$i++)        { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
 330 for(;$i<60;$i++)        { &BODY_40_59($i,@V); unshift(@V,pop(@V)); }
 331 for(;$i<80;$i++)        { &BODY_20_39($i,@V); unshift(@V,pop(@V)); }
 332 $code.=<<___;
 333         / Update and save state information in SHA-1 context
 334         add     0($ctx),$E
 335         add     4($ctx),$T
 336         add     8($ctx),$A
 337         add     12($ctx),$B
 338         add     16($ctx),$C
 339         mov     $E,0($ctx)
 340         mov     $T,4($ctx)
 341         mov     $A,8($ctx)
 342         mov     $B,12($ctx)
 343         mov     $C,16($ctx)

 345         xchg    $E,$A   # mov   $E,$A
 346         xchg    $T,$B   # mov   $T,$B
 347         xchg    $E,$C   # mov   $A,$C
 348         xchg    $T,$D   # mov   $B,$D
 349                         # mov   $C,$E
 350         lea     '16*4'($inp),$inp
 351         sub     \$1,$num
 352         jnz     .Lloop
 353 ___
 354 &EPILOGUE("sha1_block_data_order");
 355 $code.=<<___;
 356 .asciz  "SHA1 block transform for x86_64, CRYPTOGAMS by <appro\@openssl.org>"

 358 #else
 359         /* LINTED */
 360         /* Nothing to be linted in this file--it's pure assembly source. */
 361 #endif /* !lint && !__lint */
 362 ___

 364 ################################################################

 366 $code =~ s/\'([^\']*)\'/eval $1/gem;
 367 print $code;
 368 close STDOUT;
```

****
1758 Mon Mar 24 15:32:06 2008
new/usr/src/common/crypto/sha2/amd64/THIRDPARTYLICENSE
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
****

```
Copyright (c) 2006, CRYPTOGAMS by <appro@openssl.org>
All rights reserved.

Redistribution and use in source and binary forms, with or without
modification, are permitted provided that the following conditions
are met:

      * Redistributions of source code must retain copyright notices,
        this list of conditions and the following disclaimer.

      * Redistributions in binary form must reproduce the above
        copyright notice, this list of conditions and the following
        disclaimer in the documentation and/or other materials
        provided with the distribution.

      * Neither the name of the CRYPTOGAMS nor the names of its
        copyright holder and contributors may be used to endorse or
        promote products derived from this software without specific
        prior written permission.

ALTERNATIVELY, provided that this notice is retained in full, this
product may be distributed under the terms of the GNU General Public
License (GPL), in which case the provisions of the GPL apply INSTEAD OF
those given above.

THIS SOFTWARE IS PROVIDED BY THE COPYRIGHT HOLDER AND CONTRIBUTORS
"AS IS" AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT
LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR
A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE COPYRIGHT
OWNER OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL,
SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT
LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE,
DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY
THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT
(INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE
OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.
```

```
**********************************************************
      31 Mon Mar 24 15:32:08 2008
new/usr/src/common/crypto/sha2/amd64/THIRDPARTYLICENSE.descrip
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
   1 PORTIONS OF SHA2 FUNCTIONALITY
```

```
**********************************************************
   11076 Mon Mar 24 15:32:09 2008
new/usr/src/common/crypto/sha2/amd64/sha512-x86_64.pl
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
```

```
#!/usr/bin/env perl
#
# ====================================================================
# Written by Andy Polyakov <appro@fy.chalmers.se> for the OpenSSL
# project. Rights for redistribution and usage in source and binary
# forms are granted according to the OpenSSL license.
# ====================================================================
#
# sha256/512_block procedure for x86_64.
#
# 40% improvement over compiler-generated code on Opteron. On EM64T
# sha256 was observed to run >80% faster and sha512 - >40%. No magical
# tricks, just straight implementation... I really wonder why gcc
# [being armed with inline assembler] fails to generate as fast code.
# The only thing which is cool about this module is that it's very
# same instruction sequence used for both SHA-256 and SHA-512. In
# former case the instructions operate on 32-bit operands, while in
# latter - on 64-bit ones. All I had to do is to get one flavor right,
# the other one passed the test right away:-)
#
# sha256_block runs in ~1005 cycles on Opteron, which gives you
# asymptotic performance of 64*1000/1005=63.7MBps times CPU clock
# frequency in GHz. sha512_block runs in ~1275 cycles, which results
# in 128*1000/1275=100MBps per GHz. Is there room for improvement?
# Well, if you compare it to IA-64 implementation, which maintains
# X[16] in register bank[!], tends to 4 instructions per CPU clock
# cycle and runs in 1003 cycles, 1275 is very good result for 3-way
# issue Opteron pipeline and X[16] maintained in memory. So that *if*
# there is a way to improve it, *then* the only way would be to try to
# offload X[16] updates to SSE unit, but that would require "deeper"
# loop unroll, which in turn would naturally cause size blow-up, not
# to mention increased complexity! And once again, only *if* it's
# actually possible to noticeably improve overall ILP, instruction
# level parallelism, on a given CPU implementation in this case.
#
# Special note on Intel EM64T. While Opteron CPU exhibits perfect
# perfromance ratio of 1.5 between 64- and 32-bit flavors [see above],
# [currently available] EM64T CPUs apparently are far from it. On the
# contrary, 64-bit version, sha512_block, is ~30% *slower* than 32-bit
# sha256_block:-( This is presumably because 64-bit shifts/rotates
# apparently are not atomic instructions, but implemented in microcode.

#
# OpenSolaris OS modifications
#
# Sun elects to use this software under the BSD license.
#
# This source originates from OpenSSL file sha512-x86_64.pl at
# ftp://ftp.openssl.org/snapshot/openssl-0.9.8-stable-SNAP-20080131.tar.gz
# (presumably for future OpenSSL release 0.9.8h), with these changes:
#
# 1. Added perl "use strict" and declared variables.
#
# 2. Added OpenSolaris ENTRY_NP/SET_SIZE macros from
# /usr/include/sys/asm_linkage.h, .ident keywords, and lint(1B) guards.
#
# 3. Removed x86_64-xlate.pl script (not needed for as(1) or gas(1)
# assemblers).  Replaced the .picmeup macro with assembler code.
#
# 4. Added 8 to $ctx, as OpenSolaris OS has an extra 4-byte field, "algotype",
# at the beginning of SHA2_CTX (the next field is 8-byte aligned).
```



```
#

use strict;
my ($code, $func, $TABLE, $SZ, @Sigma0, @Sigma1, @sigma0, @sigma1, $rounds,
        @ROT, $A, $B, $C, $D, $E, $F, $G, $H, $T1, $a0, $a1, $a2, $i,
        $ctx, $round, $inp, $Tbl, $_ctx, $_inp, $_end, $_rsp, $framesz);
my $output = shift;
open STDOUT,">$output";

#
# OpenSSL library:
# void sha512_block_data_order(SHA512_CTX *ctx, const void *in, size_t num);
# void sha256_block_data_order(SHA256_CTX *ctx, const void *in, size_t num);
#
# OpenSolaris OS:
# void SHA512TransformBlocks(SHA2_CTX *ctx, const void *in, size_t num);
# void SHA256TransformBlocks(SHA2_CTX *ctx, const void *in, size_t num);
# Note: the OpenSolaris SHA2 structure has an extra 8 byte field at the
# beginning (over OpenSSL's SHA512 or SHA256 structure).
#

if ($output =~ /512/) {
        $func="SHA512TransformBlocks";
        $TABLE="K512";
        $SZ=8;
        @ROT=($A,$B,$C,$D,$E,$F,$G,$H)=("%rax","%rbx","%rcx","%rdx",
                                        "%r8", "%r9", "%r10","%r11");
        ($T1,$a0,$a1,$a2)=("%r12","%r13","%r14","%r15");
        @Sigma0=(28,34,39);
        @Sigma1=(14,18,41);
        @sigma0=(1,  8, 7);
        @sigma1=(19,61, 6);
        $rounds=80;
} else {
        $func="SHA256TransformBlocks";
        $TABLE="K256";
        $SZ=4;
        @ROT=($A,$B,$C,$D,$E,$F,$G,$H)=("%eax","%ebx","%ecx","%edx",
                                        "%r8d","%r9d","%r10d","%r11d");
        ($T1,$a0,$a1,$a2)=("%r12d","%r13d","%r14d","%r15d");
        @Sigma0=( 2,13,22);
        @Sigma1=( 6,11,25);
        @sigma0=( 7,18, 3);
        @sigma1=(17,19,10);
        $rounds=64;
}

$ctx="%rdi";    # 1st arg
$round="%rdi";  # zaps $ctx
$inp="%rsi";    # 2nd arg
$Tbl="%rbp";

$_ctx="16*$SZ+0*8(%rsp)";
$_inp="16*$SZ+1*8(%rsp)";
$_end="16*$SZ+2*8(%rsp)";
$_rsp="16*$SZ+3*8(%rsp)";
$framesz="16*$SZ+4*8";


sub ROUND_00_15()
{ my ($i,$a,$b,$c,$d,$e,$f,$g,$h) = @_;

$code.=<<___;
        mov     $e,$a0
        mov     $e,$a1
        mov     $f,$a2
```

```
129         ror     \$$Sigma1[0],$a0
130         ror     \$$Sigma1[1],$a1
131         xor     $g,$a2                  # f^g

133         xor     $a1,$a0
134         ror     \$'$Sigma1[2]-$Sigma1[1]',$a1
135         and     $e,$a2                  # (f^g)&e
136         mov     $T1,'$SZ*($i&0xf)'(%rsp)

138         xor     $a1,$a0                 # Sigma1(e)
139         xor     $g,$a2                  # Ch(e,f,g)=((f^g)&e)^g
140         add     $h,$T1                  # T1+=h

142         mov     $a,$h
143         add     $a0,$T1                 # T1+=Sigma1(e)

145         add     $a2,$T1                 # T1+=Ch(e,f,g)
146         mov     $a,$a0
147         mov     $a,$a1

149         ror     \$$Sigma0[0],$h
150         ror     \$$Sigma0[1],$a0
151         mov     $a,$a2
152         add     ($Tbl,$round,$SZ),$T1   # T1+=K[round]

154         xor     $a0,$h
155         ror     \$'$Sigma0[2]-$Sigma0[1]',$a0
156         or      $c,$a1                  # a|c

158         xor     $a0,$h                  # h=Sigma0(a)
159         and     $c,$a2                  # a&c
160         add     $T1,$d                  # d+=T1

162         and     $b,$a1                  # (a|c)&b
163         add     $T1,$h                  # h+=T1

165         or      $a2,$a1                 # Maj(a,b,c)=((a|c)&b)|(a&c)
166         lea     1($round),$round        # round++

168         add     $a1,$h                  # h+=Maj(a,b,c)
169 ___
170 }

172 sub ROUND_16_XX()
173 { my ($i,$a,$b,$c,$d,$e,$f,$g,$h) = @_;

175 $code.=<<___;
176         mov     '$SZ*(($i+1)&0xf)'(%rsp),$a0
177         mov     '$SZ*(($i+14)&0xf)'(%rsp),$T1

179         mov     $a0,$a2

181         shr     \$$sigma0[2],$a0
182         ror     \$$sigma0[0],$a2

184         xor     $a2,$a0
185         ror     \$'$sigma0[1]-$sigma0[0]',$a2

187         xor     $a2,$a0                 # sigma0(X[(i+1)&0xf])
188         mov     $T1,$a1

190         shr     \$$sigma1[2],$T1
191         ror     \$$sigma1[0],$a1

193         xor     $a1,$T1
```



```
194         ror     \$'$sigma1[1]-$sigma1[0]',$a1

196         xor     $a1,$T1                 # sigma1(X[(i+14)&0xf])

198         add     $a0,$T1

200         add     '$SZ*(($i+9)&0xf)'(%rsp),$T1

202         add     '$SZ*($i&0xf)'(%rsp),$T1
203 ___
204         &ROUND_00_15(@_);
205 }

207 #
208 # Execution begins here
209 #

211 $code=<<___;
212 #if !defined(lint) && !defined(__lint)
213         .ident  "@(#)sha512-x86_64.pl   1.1     08/03/20 SMI"
214 #include <sys/asm_linkage.h>

216 ENTRY_NP($func)
217         push    %rbx
218         push    %rbp
219         push    %r12
220         push    %r13
221         push    %r14
222         push    %r15
223         mov     %rsp,%rbp               # copy %rsp
224         shl     \$4,%rdx                # num*16
225         sub     \$$framesz,%rsp
226         lea     ($inp,%rdx,$SZ),%rdx    # inp+num*16*$SZ
227         and     \$-64,%rsp              # align stack frame
228         add     \$8,$ctx                # Skip OpenSolaris field, "algotype"
229         mov     $ctx,$_ctx              # save ctx, 1st arg
230         mov     $inp,$_inp              # save inp, 2nd arg
231         mov     %rdx,$_end              # save end pointer, "3rd" arg
232         mov     %rbp,$_rsp              # save copy of %rsp

234         /.picmeup $Tbl
235         / The .picmeup pseudo-directive, from perlasm/x86_64_xlate.pl, puts
236         / the address of the "next" instruction into the target register
237         / ($Tbl).  This generates these 2 instructions:
238         lea     .Llea(%rip),$Tbl
239         /nop    / .picmeup generates a nop for mod 8 alignment--not needed here

241 .Llea:
242         lea     $TABLE-.($Tbl),$Tbl

244         mov     $SZ*0($ctx),$A
245         mov     $SZ*1($ctx),$B
246         mov     $SZ*2($ctx),$C
247         mov     $SZ*3($ctx),$D
248         mov     $SZ*4($ctx),$E
249         mov     $SZ*5($ctx),$F
250         mov     $SZ*6($ctx),$G
251         mov     $SZ*7($ctx),$H
252         jmp     .Lloop

254 .align  16
255 .Lloop:
256         xor     $round,$round
257 ___
258         for($i=0;$i<16;$i++) {
259                 $code.="        mov     $SZ*$i($inp),$T1\n";
```

```
260                 $code.="        bswap   $T1\n";
261                 &ROUND_00_15($i,@ROT);
262                 unshift(@ROT,pop(@ROT));
263         }
264 $code.=<<___;
265         jmp     .Lrounds_16_xx
266 .align  16
267 .Lrounds_16_xx:
268 ___
269         for(;$i<32;$i++) {
270                 &ROUND_16_XX($i,@ROT);
271                 unshift(@ROT,pop(@ROT));
272         }

274 $code.=<<___;
275         cmp     \$$rounds,$round
276         jb      .Lrounds_16_xx

278         mov     $_ctx,$ctx
279         lea     16*$SZ($inp),$inp

281         add     $SZ*0($ctx),$A
282         add     $SZ*1($ctx),$B
283         add     $SZ*2($ctx),$C
284         add     $SZ*3($ctx),$D
285         add     $SZ*4($ctx),$E
286         add     $SZ*5($ctx),$F
287         add     $SZ*6($ctx),$G
288         add     $SZ*7($ctx),$H

290         cmp     $_end,$inp

292         mov     $A,$SZ*0($ctx)
293         mov     $B,$SZ*1($ctx)
294         mov     $C,$SZ*2($ctx)
295         mov     $D,$SZ*3($ctx)
296         mov     $E,$SZ*4($ctx)
297         mov     $F,$SZ*5($ctx)
298         mov     $G,$SZ*6($ctx)
299         mov     $H,$SZ*7($ctx)
300         jb      .Lloop

302         mov     $_rsp,%rsp
303         pop     %r15
304         pop     %r14
305         pop     %r13
306         pop     %r12
307         pop     %rbp
308         pop     %rbx

310         ret
311 SET_SIZE($func)

313 ___

315 if ($SZ==4) {
316 # SHA256
317 $code.=<<___;
318 .align  64
319 .type   $TABLE,\@object
320 $TABLE:
321         .long   0x428a2f98,0x71374491,0xb5c0fbcf,0xe9b5dba5
322         .long   0x3956c25b,0x59f111f1,0x923f82a4,0xab1c5ed5
323         .long   0xd807aa98,0x12835b01,0x243185be,0x550c7dc3
324         .long   0x72be5d74,0x80deb1fe,0x9bdc06a7,0xc19bf174
325         .long   0xe49b69c1,0xefbe4786,0x0fc19dc6,0x240ca1cc
```



```
326         .long   0x2de92c6f,0x4a7484aa,0x5cb0a9dc,0x76f988da
327         .long   0x983e5152,0xa831c66d,0xb00327c8,0xbf597fc7
328         .long   0xc6e00bf3,0xd5a79147,0x06ca6351,0x14292967
329         .long   0x27b70a85,0x2e1b2138,0x4d2c6dfc,0x53380d13
330         .long   0x650a7354,0x766a0abb,0x81c2c92e,0x92722c85
331         .long   0xa2bfe8a1,0xa81a664b,0xc24b8b70,0xc76c51a3
332         .long   0xd192e819,0xd6990624,0xf40e3585,0x106aa070
333         .long   0x19a4c116,0x1e376c08,0x2748774c,0x34b0bcb5
334         .long   0x391c0cb3,0x4ed8aa4a,0x5b9cca4f,0x682e6ff3
335         .long   0x748f82ee,0x78a5636f,0x84c87814,0x8cc70208
336         .long   0x90befffa,0xa4506ceb,0xbef9a3f7,0xc67178f2
337 ___
338 } else {
339 # SHA512
340 $code.=<<___;
341 .align  64
342 .type   $TABLE,\@object
343 $TABLE:
344         .quad   0x428a2f98d728ae22,0x7137449123ef65cd
345         .quad   0xb5c0fbcfec4d3b2f,0xe9b5dba58189dbbc
346         .quad   0x3956c25bf348b538,0x59f111f1b605d019
347         .quad   0x923f82a4af194f9b,0xab1c5ed5da6d8118
348         .quad   0xd807aa98a3030242,0x12835b0145706fbe
349         .quad   0x243185be4ee4b28c,0x550c7dc3d5ffb4e2
350         .quad   0x72be5d74f27b896f,0x80deb1fe3b1696b1
351         .quad   0x9bdc06a725c71235,0xc19bf174cf692694
352         .quad   0xe49b69c19ef14ad2,0xefbe4786384f25e3
353         .quad   0x0fc19dc68b8cd5b5,0x240ca1cc77ac9c65
354         .quad   0x2de92c6f592b0275,0x4a7484aa6ea6e483
355         .quad   0x5cb0a9dcbd41fbd4,0x76f988da831153b5
356         .quad   0x983e5152ee66dfab,0xa831c66d2db43210
357         .quad   0xb00327c898fb213f,0xbf597fc7beef0ee4
358         .quad   0xc6e00bf33da88fc2,0xd5a79147930aa725
359         .quad   0x06ca6351e003826f,0x142929670a0e6e70
360         .quad   0x27b70a8546d22ffc,0x2e1b21385c26c926
361         .quad   0x4d2c6dfc5ac42aed,0x53380d139d95b3df
362         .quad   0x650a73548baf63de,0x766a0abb3c77b2a8
363         .quad   0x81c2c92e47edaee6,0x92722c851482353b
364         .quad   0xa2bfe8a14cf10364,0xa81a664bbc423001
365         .quad   0xc24b8b70d0f89791,0xc76c51a30654be30
366         .quad   0xd192e819d6ef5218,0xd69906245565a910
367         .quad   0xf40e35855771202a,0x106aa07032bbd1b8
368         .quad   0x19a4c116b8d2d0c8,0x1e376c085141ab53
369         .quad   0x2748774cdf8eeb99,0x34b0bcb5e19b48a8
370         .quad   0x391c0cb3c5c95a63,0x4ed8aa4ae3418acb
371         .quad   0x5b9cca4f7763e373,0x682e6ff3d6b2b8a3
372         .quad   0x748f82ee5defb2fc,0x78a5636f43172f60
373         .quad   0x84c87814a1f0ab72,0x8cc702081a6439ec
374         .quad   0x90befffa23631e28,0xa4506cebde82bde9
375         .quad   0xbef9a3f7b2c67915,0xc67178f2e372532b
376         .quad   0xca273eceea26619c,0xd186b8c721c0c207
377         .quad   0xeada7dd6cde0eb1e,0xf57d4f7fee6ed178
378         .quad   0x06f067aa72176fba,0x0a637dc5a2c898a6
379         .quad   0x113f9804bef90dae,0x1b710b35131c471b
380         .quad   0x28db77f523047d84,0x32caab7b40c72493
381         .quad   0x3c9ebe0a15c9bebc,0x431d67c49c100d4c
382         .quad   0x4cc5d4becb3e42b6,0x597f299cfc657e2a
383         .quad   0x5fcb6fab3ad6faec,0x6c44198c4a475817
384 ___
385 }
386 $code.=<<___;

388 #else
389         /* LINTED */
390         /* Nothing to be linted in this file--it's pure assembly source. */
391 #endif /* !lint && !__lint */
```

```
392 ___

394 $code =~ s/\`([^\`]*)\`/eval $1/gem;
395 print $code;
396 close STDOUT;
```

```
**********************************************************
   31347 Mon Mar 24 15:32:11 2008
new/usr/src/common/crypto/sha2/sha2.c
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
```

```
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#pragma ident   "@(#)sha2.c     1.8     08/03/20 SMI"
#pragma ident   "@(#)sha2.c     1.7     07/04/10 SMI"


/*
 * The basic framework for this code came from the reference
 * implementation for MD5.  That implementation is Copyright (C)
 * 1991-2, RSA Data Security, Inc. Created 1991. All rights reserved.
 *
 * License to copy and use this software is granted provided that it
 * is identified as the "RSA Data Security, Inc. MD5 Message-Digest
 * Algorithm" in all material mentioning or referencing this software
 * or this function.
 *
 * License is also granted to make and use derivative works provided
 * that such works are identified as "derived from the RSA Data
 * Security, Inc. MD5 Message-Digest Algorithm" in all material
 * mentioning or referencing the derived work.
 *
 * RSA Data Security, Inc. makes no representations concerning either
 * the merchantability of this software or the suitability of this
 * software for any particular purpose. It is provided "as is"
 * without express or implied warranty of any kind.
 *
 * These notices must be retained in any copies of any part of this
 * documentation and/or software.
 *
 * NOTE: Cleaned-up and optimized, version of SHA2, based on the FIPS 180-2
 * standard, available at http://www.itl.nist.gov/div897/pubs/fip180-2.htm
 * Not as fast as one would like -- further optimizations are encouraged
 * and appreciated.
 */

#include <sys/types.h>
#include <sys/param.h>
#include <sys/systm.h>
#include <sys/sysmacros.h>
#define _SHA2_IMPL
#include <sys/sha2.h>
#include <sys/sha2_consts.h>

#ifdef _KERNEL
#include <sys/cmn_err.h>
#ifndef _KERNEL

#else
#include <strings.h>
#include <stdlib.h>
#include <errno.h>

#pragma weak SHA256Update = SHA2Update
#pragma weak SHA384Update = SHA2Update
#pragma weak SHA512Update = SHA2Update

#pragma weak SHA256Final = SHA2Final
```



```
#pragma weak SHA384Final = SHA2Final
#pragma weak SHA512Final = SHA2Final

#endif  /* !_KERNEL */

#ifdef _KERNEL
#include <sys/cmn_err.h>
#endif  /* _KERNEL */

static void Encode(uint8_t *, uint32_t *, size_t);
static void Encode64(uint8_t *, uint64_t *, size_t);

#if     defined(__amd64)
#define SHA512Transform(ctx, in) SHA512TransformBlocks((ctx), (in), 1)
#define SHA256Transform(ctx, in) SHA256TransformBlocks((ctx), (in), 1)

void SHA512TransformBlocks(SHA2_CTX *ctx, const void *in, size_t num);
void SHA256TransformBlocks(SHA2_CTX *ctx, const void *in, size_t num);

#else
static void SHA256Transform(SHA2_CTX *, const uint8_t *);
static void SHA512Transform(SHA2_CTX *, const uint8_t *);
#endif  /* __amd64 */

static uint8_t PADDING[128] = { 0x80, /* all zeros */ };

/* Ch and Maj are the basic SHA2 functions. */
#define Ch(b, c, d)     (((b) & (c)) ^ ((~b) & (d)))
#define Maj(b, c, d)    (((b) & (c)) ^ ((b) & (d)) ^ ((c) & (d)))

/* Rotates x right n bits. */
#define ROTR(x, n)      \
        (((x) >> (n)) | ((x) << ((sizeof (x) * NBBY)-(n))))

/* Shift x right n bits */
#define SHR(x, n)       ((x) >> (n))

/* SHA256 Functions */
#define BIGSIGMA0_256(x)        (ROTR((x), 2) ^ ROTR((x), 13) ^ ROTR((x), 22))
#define BIGSIGMA1_256(x)        (ROTR((x), 6) ^ ROTR((x), 11) ^ ROTR((x), 25))
#define SIGMA0_256(x)           (ROTR((x), 7) ^ ROTR((x), 18) ^ SHR((x), 3))
#define SIGMA1_256(x)           (ROTR((x), 17) ^ ROTR((x), 19) ^ SHR((x), 10))

#define SHA256ROUND(a, b, c, d, e, f, g, h, i, w)                       \
        T1 = h + BIGSIGMA1_256(e) + Ch(e, f, g) + SHA256_CONST(i) + w;  \
        d += T1;                                                        \
        T2 = BIGSIGMA0_256(a) + Maj(a, b, c);                           \
        h = T1 + T2

/* SHA384/512 Functions */
#define BIGSIGMA0(x)    (ROTR((x), 28) ^ ROTR((x), 34) ^ ROTR((x), 39))
#define BIGSIGMA1(x)    (ROTR((x), 14) ^ ROTR((x), 18) ^ ROTR((x), 41))
#define SIGMA0(x)       (ROTR((x), 1) ^ ROTR((x), 8) ^ SHR((x), 7))
#define SIGMA1(x)       (ROTR((x), 19) ^ ROTR((x), 61) ^ SHR((x), 6))
#define SHA512ROUND(a, b, c, d, e, f, g, h, i, w)                       \
        T1 = h + BIGSIGMA1(e) + Ch(e, f, g) + SHA512_CONST(i) + w;      \
        d += T1;                                                        \
        T2 = BIGSIGMA0(a) + Maj(a, b, c);                               \
        h = T1 + T2

/*
 * sparc optimization:
 *
 * on the sparc, we can load big endian 32-bit data easily.  note that
 * special care must be taken to ensure the address is 32-bit aligned.
 * in the interest of speed, we don't check to make sure, since
```

```
 * careful programming can guarantee this for us.
 */

#if     defined(_BIG_ENDIAN)

#define LOAD_BIG_32(addr)       (*(uint32_t *)(addr))

#else   /* little endian -- will work on big endian, but slowly */

#define LOAD_BIG_32(addr)       \
        (((addr)[0] << 24) | ((addr)[1] << 16) | ((addr)[2] << 8) | (addr)[3])
#endif


#if     defined(_BIG_ENDIAN)

#define LOAD_BIG_64(addr)       (*(uint64_t *)(addr))

#else   /* little endian -- will work on big endian, but slowly */

#define LOAD_BIG_64(addr)       \
        (((uint64_t)(addr)[0] << 56) | ((uint64_t)(addr)[1] << 48) |    \
            ((uint64_t)(addr)[2] << 40) | ((uint64_t)(addr)[3] << 32) | \
            ((uint64_t)(addr)[4] << 24) | ((uint64_t)(addr)[5] << 16) | \
            ((uint64_t)(addr)[6] << 8) | (uint64_t)(addr)[7])

#endif


#if     !defined(__amd64)
/* SHA256 Transform */

static void
SHA256Transform(SHA2_CTX *ctx, const uint8_t *blk)
{

        uint32_t a = ctx->state.s32[0];
        uint32_t b = ctx->state.s32[1];
        uint32_t c = ctx->state.s32[2];
        uint32_t d = ctx->state.s32[3];
        uint32_t e = ctx->state.s32[4];
        uint32_t f = ctx->state.s32[5];
        uint32_t g = ctx->state.s32[6];
        uint32_t h = ctx->state.s32[7];

        uint32_t w0, w1, w2, w3, w4, w5, w6, w7;
        uint32_t w8, w9, w10, w11, w12, w13, w14, w15;
        uint32_t T1, T2;

#if     defined(__sparc)
        static const uint32_t sha256_consts[] = {
                SHA256_CONST_0, SHA256_CONST_1, SHA256_CONST_2,
                SHA256_CONST_3, SHA256_CONST_4, SHA256_CONST_5,
                SHA256_CONST_6, SHA256_CONST_7, SHA256_CONST_8,
                SHA256_CONST_9, SHA256_CONST_10, SHA256_CONST_11,
                SHA256_CONST_12, SHA256_CONST_13, SHA256_CONST_14,
                SHA256_CONST_15, SHA256_CONST_16, SHA256_CONST_17,
                SHA256_CONST_18, SHA256_CONST_19, SHA256_CONST_20,
                SHA256_CONST_21, SHA256_CONST_22, SHA256_CONST_23,
                SHA256_CONST_24, SHA256_CONST_25, SHA256_CONST_26,
                SHA256_CONST_27, SHA256_CONST_28, SHA256_CONST_29,
                SHA256_CONST_30, SHA256_CONST_31, SHA256_CONST_32,
                SHA256_CONST_33, SHA256_CONST_34, SHA256_CONST_35,
                SHA256_CONST_36, SHA256_CONST_37, SHA256_CONST_38,
                SHA256_CONST_39, SHA256_CONST_40, SHA256_CONST_41,
                SHA256_CONST_42, SHA256_CONST_43, SHA256_CONST_44,
```



```
                SHA256_CONST_45, SHA256_CONST_46, SHA256_CONST_47,
                SHA256_CONST_48, SHA256_CONST_49, SHA256_CONST_50,
                SHA256_CONST_51, SHA256_CONST_52, SHA256_CONST_53,
                SHA256_CONST_54, SHA256_CONST_55, SHA256_CONST_56,
                SHA256_CONST_57, SHA256_CONST_58, SHA256_CONST_59,
                SHA256_CONST_60, SHA256_CONST_61, SHA256_CONST_62,
                SHA256_CONST_63
        };
#endif  /* __sparc */
#endif

        if ((uintptr_t)blk & 0x3) {             /* not 4-byte aligned? */
                bcopy(blk, ctx->buf_un.buf32,  sizeof (ctx->buf_un.buf32));
                blk = (uint8_t *)ctx->buf_un.buf32;
        }

        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w0 =  LOAD_BIG_32(blk + 4 * 0);
        SHA256ROUND(a, b, c, d, e, f, g, h, 0, w0);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w1 =  LOAD_BIG_32(blk + 4 * 1);
        SHA256ROUND(h, a, b, c, d, e, f, g, 1, w1);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w2 =  LOAD_BIG_32(blk + 4 * 2);
        SHA256ROUND(g, h, a, b, c, d, e, f, 2, w2);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w3 =  LOAD_BIG_32(blk + 4 * 3);
        SHA256ROUND(f, g, h, a, b, c, d, e, 3, w3);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w4 =  LOAD_BIG_32(blk + 4 * 4);
        SHA256ROUND(e, f, g, h, a, b, c, d, 4, w4);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w5 =  LOAD_BIG_32(blk + 4 * 5);
        SHA256ROUND(d, e, f, g, h, a, b, c, 5, w5);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w6 =  LOAD_BIG_32(blk + 4 * 6);
        SHA256ROUND(c, d, e, f, g, h, a, b, 6, w6);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w7 =  LOAD_BIG_32(blk + 4 * 7);
        SHA256ROUND(b, c, d, e, f, g, h, a, 7, w7);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w8 =  LOAD_BIG_32(blk + 4 * 8);
        SHA256ROUND(a, b, c, d, e, f, g, h, 8, w8);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w9 =  LOAD_BIG_32(blk + 4 * 9);
        SHA256ROUND(h, a, b, c, d, e, f, g, 9, w9);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w10 =  LOAD_BIG_32(blk + 4 * 10);
        SHA256ROUND(g, h, a, b, c, d, e, f, 10, w10);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w11 =  LOAD_BIG_32(blk + 4 * 11);
        SHA256ROUND(f, g, h, a, b, c, d, e, 11, w11);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w12 =  LOAD_BIG_32(blk + 4 * 12);
        SHA256ROUND(e, f, g, h, a, b, c, d, 12, w12);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w13 =  LOAD_BIG_32(blk + 4 * 13);
        SHA256ROUND(d, e, f, g, h, a, b, c, 13, w13);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w14 =  LOAD_BIG_32(blk + 4 * 14);
        SHA256ROUND(c, d, e, f, g, h, a, b, 14, w14);
        /* LINTED E_BAD_PTR_CAST_ALIGN */
        w15 =  LOAD_BIG_32(blk + 4 * 15);
        SHA256ROUND(b, c, d, e, f, g, h, a, 15, w15);

        w0 = SIGMA1_256(w14) + w9 + SIGMA0_256(w1) + w0;
```

```
249         SHA256ROUND(a, b, c, d, e, f, g, h, 16, w0);
250         w1 = SIGMA1_256(w15) + w10 + SIGMA0_256(w2) + w1;
251         SHA256ROUND(h, a, b, c, d, e, f, g, 17, w1);
252         w2 = SIGMA1_256(w0) + w11 + SIGMA0_256(w3) + w2;
253         SHA256ROUND(g, h, a, b, c, d, e, f, 18, w2);
254         w3 = SIGMA1_256(w1) + w12 + SIGMA0_256(w4) + w3;
255         SHA256ROUND(f, g, h, a, b, c, d, e, 19, w3);
256         w4 = SIGMA1_256(w2) + w13 + SIGMA0_256(w5) + w4;
257         SHA256ROUND(e, f, g, h, a, b, c, d, 20, w4);
258         w5 = SIGMA1_256(w3) + w14 + SIGMA0_256(w6) + w5;
259         SHA256ROUND(d, e, f, g, h, a, b, c, 21, w5);
260         w6 = SIGMA1_256(w4) + w15 + SIGMA0_256(w7) + w6;
261         SHA256ROUND(c, d, e, f, g, h, a, b, 22, w6);
262         w7 = SIGMA1_256(w5) + w0 + SIGMA0_256(w8) + w7;
263         SHA256ROUND(b, c, d, e, f, g, h, a, 23, w7);
264         w8 = SIGMA1_256(w6) + w1 + SIGMA0_256(w9) + w8;
265         SHA256ROUND(a, b, c, d, e, f, g, h, 24, w8);
266         w9 = SIGMA1_256(w7) + w2 + SIGMA0_256(w10) + w9;
267         SHA256ROUND(h, a, b, c, d, e, f, g, 25, w9);
268         w10 = SIGMA1_256(w8) + w3 + SIGMA0_256(w11) + w10;
269         SHA256ROUND(g, h, a, b, c, d, e, f, 26, w10);
270         w11 = SIGMA1_256(w9) + w4 + SIGMA0_256(w12) + w11;
271         SHA256ROUND(f, g, h, a, b, c, d, e, 27, w11);
272         w12 = SIGMA1_256(w10) + w5 + SIGMA0_256(w13) + w12;
273         SHA256ROUND(e, f, g, h, a, b, c, d, 28, w12);
274         w13 = SIGMA1_256(w11) + w6 + SIGMA0_256(w14) + w13;
275         SHA256ROUND(d, e, f, g, h, a, b, c, 29, w13);
276         w14 = SIGMA1_256(w12) + w7 + SIGMA0_256(w15) + w14;
277         SHA256ROUND(c, d, e, f, g, h, a, b, 30, w14);
278         w15 = SIGMA1_256(w13) + w8 + SIGMA0_256(w0) + w15;
279         SHA256ROUND(b, c, d, e, f, g, h, a, 31, w15);

281         w0 = SIGMA1_256(w14) + w9 + SIGMA0_256(w1) + w0;
282         SHA256ROUND(a, b, c, d, e, f, g, h, 32, w0);
283         w1 = SIGMA1_256(w15) + w10 + SIGMA0_256(w2) + w1;
284         SHA256ROUND(h, a, b, c, d, e, f, g, 33, w1);
285         w2 = SIGMA1_256(w0) + w11 + SIGMA0_256(w3) + w2;
286         SHA256ROUND(g, h, a, b, c, d, e, f, 34, w2);
287         w3 = SIGMA1_256(w1) + w12 + SIGMA0_256(w4) + w3;
288         SHA256ROUND(f, g, h, a, b, c, d, e, 35, w3);
289         w4 = SIGMA1_256(w2) + w13 + SIGMA0_256(w5) + w4;
290         SHA256ROUND(e, f, g, h, a, b, c, d, 36, w4);
291         w5 = SIGMA1_256(w3) + w14 + SIGMA0_256(w6) + w5;
292         SHA256ROUND(d, e, f, g, h, a, b, c, 37, w5);
293         w6 = SIGMA1_256(w4) + w15 + SIGMA0_256(w7) + w6;
294         SHA256ROUND(c, d, e, f, g, h, a, b, 38, w6);
295         w7 = SIGMA1_256(w5) + w0 + SIGMA0_256(w8) + w7;
296         SHA256ROUND(b, c, d, e, f, g, h, a, 39, w7);
297         w8 = SIGMA1_256(w6) + w1 + SIGMA0_256(w9) + w8;
298         SHA256ROUND(a, b, c, d, e, f, g, h, 40, w8);
299         w9 = SIGMA1_256(w7) + w2 + SIGMA0_256(w10) + w9;
300         SHA256ROUND(h, a, b, c, d, e, f, g, 41, w9);
301         w10 = SIGMA1_256(w8) + w3 + SIGMA0_256(w11) + w10;
302         SHA256ROUND(g, h, a, b, c, d, e, f, 42, w10);
303         w11 = SIGMA1_256(w9) + w4 + SIGMA0_256(w12) + w11;
304         SHA256ROUND(f, g, h, a, b, c, d, e, 43, w11);
305         w12 = SIGMA1_256(w10) + w5 + SIGMA0_256(w13) + w12;
306         SHA256ROUND(e, f, g, h, a, b, c, d, 44, w12);
307         w13 = SIGMA1_256(w11) + w6 + SIGMA0_256(w14) + w13;
308         SHA256ROUND(d, e, f, g, h, a, b, c, 45, w13);
309         w14 = SIGMA1_256(w12) + w7 + SIGMA0_256(w15) + w14;
310         SHA256ROUND(c, d, e, f, g, h, a, b, 46, w14);
311         w15 = SIGMA1_256(w13) + w8 + SIGMA0_256(w0) + w15;
312         SHA256ROUND(b, c, d, e, f, g, h, a, 47, w15);

314         w0 = SIGMA1_256(w14) + w9 + SIGMA0_256(w1) + w0;
```



```
315         SHA256ROUND(a, b, c, d, e, f, g, h, 48, w0);
316         w1 = SIGMA1_256(w15) + w10 + SIGMA0_256(w2) + w1;
317         SHA256ROUND(h, a, b, c, d, e, f, g, 49, w1);
318         w2 = SIGMA1_256(w0) + w11 + SIGMA0_256(w3) + w2;
319         SHA256ROUND(g, h, a, b, c, d, e, f, 50, w2);
320         w3 = SIGMA1_256(w1) + w12 + SIGMA0_256(w4) + w3;
321         SHA256ROUND(f, g, h, a, b, c, d, e, 51, w3);
322         w4 = SIGMA1_256(w2) + w13 + SIGMA0_256(w5) + w4;
323         SHA256ROUND(e, f, g, h, a, b, c, d, 52, w4);
324         w5 = SIGMA1_256(w3) + w14 + SIGMA0_256(w6) + w5;
325         SHA256ROUND(d, e, f, g, h, a, b, c, 53, w5);
326         w6 = SIGMA1_256(w4) + w15 + SIGMA0_256(w7) + w6;
327         SHA256ROUND(c, d, e, f, g, h, a, b, 54, w6);
328         w7 = SIGMA1_256(w5) + w0 + SIGMA0_256(w8) + w7;
329         SHA256ROUND(b, c, d, e, f, g, h, a, 55, w7);
330         w8 = SIGMA1_256(w6) + w1 + SIGMA0_256(w9) + w8;
331         SHA256ROUND(a, b, c, d, e, f, g, h, 56, w8);
332         w9 = SIGMA1_256(w7) + w2 + SIGMA0_256(w10) + w9;
333         SHA256ROUND(h, a, b, c, d, e, f, g, 57, w9);
334         w10 = SIGMA1_256(w8) + w3 + SIGMA0_256(w11) + w10;
335         SHA256ROUND(g, h, a, b, c, d, e, f, 58, w10);
336         w11 = SIGMA1_256(w9) + w4 + SIGMA0_256(w12) + w11;
337         SHA256ROUND(f, g, h, a, b, c, d, e, 59, w11);
338         w12 = SIGMA1_256(w10) + w5 + SIGMA0_256(w13) + w12;
339         SHA256ROUND(e, f, g, h, a, b, c, d, 60, w12);
340         w13 = SIGMA1_256(w11) + w6 + SIGMA0_256(w14) + w13;
341         SHA256ROUND(d, e, f, g, h, a, b, c, 61, w13);
342         w14 = SIGMA1_256(w12) + w7 + SIGMA0_256(w15) + w14;
343         SHA256ROUND(c, d, e, f, g, h, a, b, 62, w14);
344         w15 = SIGMA1_256(w13) + w8 + SIGMA0_256(w0) + w15;
345         SHA256ROUND(b, c, d, e, f, g, h, a, 63, w15);

347         ctx->state.s32[0] += a;
348         ctx->state.s32[1] += b;
349         ctx->state.s32[2] += c;
350         ctx->state.s32[3] += d;
351         ctx->state.s32[4] += e;
352         ctx->state.s32[5] += f;
353         ctx->state.s32[6] += g;
354         ctx->state.s32[7] += h;
355 }


358 /* SHA384 and SHA512 Transform */

360 static void
361 SHA512Transform(SHA2_CTX *ctx, const uint8_t *blk)
362 {

364         uint64_t a = ctx->state.s64[0];
365         uint64_t b = ctx->state.s64[1];
366         uint64_t c = ctx->state.s64[2];
367         uint64_t d = ctx->state.s64[3];
368         uint64_t e = ctx->state.s64[4];
369         uint64_t f = ctx->state.s64[5];
370         uint64_t g = ctx->state.s64[6];
371         uint64_t h = ctx->state.s64[7];

373         uint64_t w0, w1, w2, w3, w4, w5, w6, w7;
374         uint64_t w8, w9, w10, w11, w12, w13, w14, w15;
375         uint64_t T1, T2;

377 #if     defined(__sparc)
378         static const uint64_t sha512_consts[] = {
379                 SHA512_CONST_0, SHA512_CONST_1, SHA512_CONST_2,
380                 SHA512_CONST_3, SHA512_CONST_4, SHA512_CONST_5,
```

```
381                 SHA512_CONST_6, SHA512_CONST_7, SHA512_CONST_8,
382                 SHA512_CONST_9, SHA512_CONST_10, SHA512_CONST_11,
383                 SHA512_CONST_12, SHA512_CONST_13, SHA512_CONST_14,
384                 SHA512_CONST_15, SHA512_CONST_16, SHA512_CONST_17,
385                 SHA512_CONST_18, SHA512_CONST_19, SHA512_CONST_20,
386                 SHA512_CONST_21, SHA512_CONST_22, SHA512_CONST_23,
387                 SHA512_CONST_24, SHA512_CONST_25, SHA512_CONST_26,
388                 SHA512_CONST_27, SHA512_CONST_28, SHA512_CONST_29,
389                 SHA512_CONST_30, SHA512_CONST_31, SHA512_CONST_32,
390                 SHA512_CONST_33, SHA512_CONST_34, SHA512_CONST_35,
391                 SHA512_CONST_36, SHA512_CONST_37, SHA512_CONST_38,
392                 SHA512_CONST_39, SHA512_CONST_40, SHA512_CONST_41,
393                 SHA512_CONST_42, SHA512_CONST_43, SHA512_CONST_44,
394                 SHA512_CONST_45, SHA512_CONST_46, SHA512_CONST_47,
395                 SHA512_CONST_48, SHA512_CONST_49, SHA512_CONST_50,
396                 SHA512_CONST_51, SHA512_CONST_52, SHA512_CONST_53,
397                 SHA512_CONST_54, SHA512_CONST_55, SHA512_CONST_56,
398                 SHA512_CONST_57, SHA512_CONST_58, SHA512_CONST_59,
399                 SHA512_CONST_60, SHA512_CONST_61, SHA512_CONST_62,
400                 SHA512_CONST_63, SHA512_CONST_64, SHA512_CONST_65,
401                 SHA512_CONST_66, SHA512_CONST_67, SHA512_CONST_68,
402                 SHA512_CONST_69, SHA512_CONST_70, SHA512_CONST_71,
403                 SHA512_CONST_72, SHA512_CONST_73, SHA512_CONST_74,
404                 SHA512_CONST_75, SHA512_CONST_76, SHA512_CONST_77,
405                 SHA512_CONST_78, SHA512_CONST_79
406         };
407 #endif  /* __sparc */
401 #endif


410         if ((uintptr_t)blk & 0x7) {             /* not 8-byte aligned? */
411                 bcopy(blk, ctx->buf_un.buf64,  sizeof (ctx->buf_un.buf64));
412                 blk = (uint8_t *)ctx->buf_un.buf64;
413         }

415         /* LINTED E_BAD_PTR_CAST_ALIGN */
416         w0 =  LOAD_BIG_64(blk + 8 * 0);
417         SHA512ROUND(a, b, c, d, e, f, g, h, 0, w0);
418         /* LINTED E_BAD_PTR_CAST_ALIGN */
419         w1 =  LOAD_BIG_64(blk + 8 * 1);
420         SHA512ROUND(h, a, b, c, d, e, f, g, 1, w1);
421         /* LINTED E_BAD_PTR_CAST_ALIGN */
422         w2 =  LOAD_BIG_64(blk + 8 * 2);
423         SHA512ROUND(g, h, a, b, c, d, e, f, 2, w2);
424         /* LINTED E_BAD_PTR_CAST_ALIGN */
425         w3 =  LOAD_BIG_64(blk + 8 * 3);
426         SHA512ROUND(f, g, h, a, b, c, d, e, 3, w3);
427         /* LINTED E_BAD_PTR_CAST_ALIGN */
428         w4 =  LOAD_BIG_64(blk + 8 * 4);
429         SHA512ROUND(e, f, g, h, a, b, c, d, 4, w4);
430         /* LINTED E_BAD_PTR_CAST_ALIGN */
431         w5 =  LOAD_BIG_64(blk + 8 * 5);
432         SHA512ROUND(d, e, f, g, h, a, b, c, 5, w5);
433         /* LINTED E_BAD_PTR_CAST_ALIGN */
434         w6 =  LOAD_BIG_64(blk + 8 * 6);
435         SHA512ROUND(c, d, e, f, g, h, a, b, 6, w6);
436         /* LINTED E_BAD_PTR_CAST_ALIGN */
437         w7 =  LOAD_BIG_64(blk + 8 * 7);
438         SHA512ROUND(b, c, d, e, f, g, h, a, 7, w7);
439         /* LINTED E_BAD_PTR_CAST_ALIGN */
440         w8 =  LOAD_BIG_64(blk + 8 * 8);
441         SHA512ROUND(a, b, c, d, e, f, g, h, 8, w8);
442         /* LINTED E_BAD_PTR_CAST_ALIGN */
443         w9 =  LOAD_BIG_64(blk + 8 * 9);
444         SHA512ROUND(h, a, b, c, d, e, f, g, 9, w9);
445         /* LINTED E_BAD_PTR_CAST_ALIGN */
```



```
446         w10 =  LOAD_BIG_64(blk + 8 * 10);
447         SHA512ROUND(g, h, a, b, c, d, e, f, 10, w10);
448         /* LINTED E_BAD_PTR_CAST_ALIGN */
449         w11 =  LOAD_BIG_64(blk + 8 * 11);
450         SHA512ROUND(f, g, h, a, b, c, d, e, 11, w11);
451         /* LINTED E_BAD_PTR_CAST_ALIGN */
452         w12 =  LOAD_BIG_64(blk + 8 * 12);
453         SHA512ROUND(e, f, g, h, a, b, c, d, 12, w12);
454         /* LINTED E_BAD_PTR_CAST_ALIGN */
455         w13 =  LOAD_BIG_64(blk + 8 * 13);
456         SHA512ROUND(d, e, f, g, h, a, b, c, 13, w13);
457         /* LINTED E_BAD_PTR_CAST_ALIGN */
458         w14 =  LOAD_BIG_64(blk + 8 * 14);
459         SHA512ROUND(c, d, e, f, g, h, a, b, 14, w14);
460         /* LINTED E_BAD_PTR_CAST_ALIGN */
461         w15 =  LOAD_BIG_64(blk + 8 * 15);
462         SHA512ROUND(b, c, d, e, f, g, h, a, 15, w15);

464         w0 = SIGMA1(w14) + w9 + SIGMA0(w1) + w0;
465         SHA512ROUND(a, b, c, d, e, f, g, h, 16, w0);
466         w1 = SIGMA1(w15) + w10 + SIGMA0(w2) + w1;
467         SHA512ROUND(h, a, b, c, d, e, f, g, 17, w1);
468         w2 = SIGMA1(w0) + w11 + SIGMA0(w3) + w2;
469         SHA512ROUND(g, h, a, b, c, d, e, f, 18, w2);
470         w3 = SIGMA1(w1) + w12 + SIGMA0(w4) + w3;
471         SHA512ROUND(f, g, h, a, b, c, d, e, 19, w3);
472         w4 = SIGMA1(w2) + w13 + SIGMA0(w5) + w4;
473         SHA512ROUND(e, f, g, h, a, b, c, d, 20, w4);
474         w5 = SIGMA1(w3) + w14 + SIGMA0(w6) + w5;
475         SHA512ROUND(d, e, f, g, h, a, b, c, 21, w5);
476         w6 = SIGMA1(w4) + w15 + SIGMA0(w7) + w6;
477         SHA512ROUND(c, d, e, f, g, h, a, b, 22, w6);
478         w7 = SIGMA1(w5) + w0 + SIGMA0(w8) + w7;
479         SHA512ROUND(b, c, d, e, f, g, h, a, 23, w7);
480         w8 = SIGMA1(w6) + w1 + SIGMA0(w9) + w8;
481         SHA512ROUND(a, b, c, d, e, f, g, h, 24, w8);
482         w9 = SIGMA1(w7) + w2 + SIGMA0(w10) + w9;
483         SHA512ROUND(h, a, b, c, d, e, f, g, 25, w9);
484         w10 = SIGMA1(w8) + w3 + SIGMA0(w11) + w10;
485         SHA512ROUND(g, h, a, b, c, d, e, f, 26, w10);
486         w11 = SIGMA1(w9) + w4 + SIGMA0(w12) + w11;
487         SHA512ROUND(f, g, h, a, b, c, d, e, 27, w11);
488         w12 = SIGMA1(w10) + w5 + SIGMA0(w13) + w12;
489         SHA512ROUND(e, f, g, h, a, b, c, d, 28, w12);
490         w13 = SIGMA1(w11) + w6 + SIGMA0(w14) + w13;
491         SHA512ROUND(d, e, f, g, h, a, b, c, 29, w13);
492         w14 = SIGMA1(w12) + w7 + SIGMA0(w15) + w14;
493         SHA512ROUND(c, d, e, f, g, h, a, b, 30, w14);
494         w15 = SIGMA1(w13) + w8 + SIGMA0(w0) + w15;
495         SHA512ROUND(b, c, d, e, f, g, h, a, 31, w15);

497         w0 = SIGMA1(w14) + w9 + SIGMA0(w1) + w0;
498         SHA512ROUND(a, b, c, d, e, f, g, h, 32, w0);
499         w1 = SIGMA1(w15) + w10 + SIGMA0(w2) + w1;
500         SHA512ROUND(h, a, b, c, d, e, f, g, 33, w1);
501         w2 = SIGMA1(w0) + w11 + SIGMA0(w3) + w2;
502         SHA512ROUND(g, h, a, b, c, d, e, f, 34, w2);
503         w3 = SIGMA1(w1) + w12 + SIGMA0(w4) + w3;
504         SHA512ROUND(f, g, h, a, b, c, d, e, 35, w3);
505         w4 = SIGMA1(w2) + w13 + SIGMA0(w5) + w4;
506         SHA512ROUND(e, f, g, h, a, b, c, d, 36, w4);
507         w5 = SIGMA1(w3) + w14 + SIGMA0(w6) + w5;
508         SHA512ROUND(d, e, f, g, h, a, b, c, 37, w5);
509         w6 = SIGMA1(w4) + w15 + SIGMA0(w7) + w6;
510         SHA512ROUND(c, d, e, f, g, h, a, b, 38, w6);
511         w7 = SIGMA1(w5) + w0 + SIGMA0(w8) + w7;
```

```
        SHA512ROUND(b, c, d, e, f, g, h, a, 39, w7);
        w8 = SIGMA1(w6) + w1 + SIGMA0(w9) + w8;
        SHA512ROUND(a, b, c, d, e, f, g, h, 40, w8);
        w9 = SIGMA1(w7) + w2 + SIGMA0(w10) + w9;
        SHA512ROUND(h, a, b, c, d, e, f, g, 41, w9);
        w10 = SIGMA1(w8) + w3 + SIGMA0(w11) + w10;
        SHA512ROUND(g, h, a, b, c, d, e, f, 42, w10);
        w11 = SIGMA1(w9) + w4 + SIGMA0(w12) + w11;
        SHA512ROUND(f, g, h, a, b, c, d, e, 43, w11);
        w12 = SIGMA1(w10) + w5 + SIGMA0(w13) + w12;
        SHA512ROUND(e, f, g, h, a, b, c, d, 44, w12);
        w13 = SIGMA1(w11) + w6 + SIGMA0(w14) + w13;
        SHA512ROUND(d, e, f, g, h, a, b, c, 45, w13);
        w14 = SIGMA1(w12) + w7 + SIGMA0(w15) + w14;
        SHA512ROUND(c, d, e, f, g, h, a, b, 46, w14);
        w15 = SIGMA1(w13) + w8 + SIGMA0(w0) + w15;
        SHA512ROUND(b, c, d, e, f, g, h, a, 47, w15);

        w0 = SIGMA1(w14) + w9 + SIGMA0(w1) + w0;
        SHA512ROUND(a, b, c, d, e, f, g, h, 48, w0);
        w1 = SIGMA1(w15) + w10 + SIGMA0(w2) + w1;
        SHA512ROUND(h, a, b, c, d, e, f, g, 49, w1);
        w2 = SIGMA1(w0) + w11 + SIGMA0(w3) + w2;
        SHA512ROUND(g, h, a, b, c, d, e, f, 50, w2);
        w3 = SIGMA1(w1) + w12 + SIGMA0(w4) + w3;
        SHA512ROUND(f, g, h, a, b, c, d, e, 51, w3);
        w4 = SIGMA1(w2) + w13 + SIGMA0(w5) + w4;
        SHA512ROUND(e, f, g, h, a, b, c, d, 52, w4);
        w5 = SIGMA1(w3) + w14 + SIGMA0(w6) + w5;
        SHA512ROUND(d, e, f, g, h, a, b, c, 53, w5);
        w6 = SIGMA1(w4) + w15 + SIGMA0(w7) + w6;
        SHA512ROUND(c, d, e, f, g, h, a, b, 54, w6);
        w7 = SIGMA1(w5) + w0 + SIGMA0(w8) + w7;
        SHA512ROUND(b, c, d, e, f, g, h, a, 55, w7);
        w8 = SIGMA1(w6) + w1 + SIGMA0(w9) + w8;
        SHA512ROUND(a, b, c, d, e, f, g, h, 56, w8);
        w9 = SIGMA1(w7) + w2 + SIGMA0(w10) + w9;
        SHA512ROUND(h, a, b, c, d, e, f, g, 57, w9);
        w10 = SIGMA1(w8) + w3 + SIGMA0(w11) + w10;
        SHA512ROUND(g, h, a, b, c, d, e, f, 58, w10);
        w11 = SIGMA1(w9) + w4 + SIGMA0(w12) + w11;
        SHA512ROUND(f, g, h, a, b, c, d, e, 59, w11);
        w12 = SIGMA1(w10) + w5 + SIGMA0(w13) + w12;
        SHA512ROUND(e, f, g, h, a, b, c, d, 60, w12);
        w13 = SIGMA1(w11) + w6 + SIGMA0(w14) + w13;
        SHA512ROUND(d, e, f, g, h, a, b, c, 61, w13);
        w14 = SIGMA1(w12) + w7 + SIGMA0(w15) + w14;
        SHA512ROUND(c, d, e, f, g, h, a, b, 62, w14);
        w15 = SIGMA1(w13) + w8 + SIGMA0(w0) + w15;
        SHA512ROUND(b, c, d, e, f, g, h, a, 63, w15);

        w0 = SIGMA1(w14) + w9 + SIGMA0(w1) + w0;
        SHA512ROUND(a, b, c, d, e, f, g, h, 64, w0);
        w1 = SIGMA1(w15) + w10 + SIGMA0(w2) + w1;
        SHA512ROUND(h, a, b, c, d, e, f, g, 65, w1);
        w2 = SIGMA1(w0) + w11 + SIGMA0(w3) + w2;
        SHA512ROUND(g, h, a, b, c, d, e, f, 66, w2);
        w3 = SIGMA1(w1) + w12 + SIGMA0(w4) + w3;
        SHA512ROUND(f, g, h, a, b, c, d, e, 67, w3);
        w4 = SIGMA1(w2) + w13 + SIGMA0(w5) + w4;
        SHA512ROUND(e, f, g, h, a, b, c, d, 68, w4);
        w5 = SIGMA1(w3) + w14 + SIGMA0(w6) + w5;
        SHA512ROUND(d, e, f, g, h, a, b, c, 69, w5);
        w6 = SIGMA1(w4) + w15 + SIGMA0(w7) + w6;
        SHA512ROUND(c, d, e, f, g, h, a, b, 70, w6);
        w7 = SIGMA1(w5) + w0 + SIGMA0(w8) + w7;
```



```
        SHA512ROUND(b, c, d, e, f, g, h, a, 71, w7);
        w8 = SIGMA1(w6) + w1 + SIGMA0(w9) + w8;
        SHA512ROUND(a, b, c, d, e, f, g, h, 72, w8);
        w9 = SIGMA1(w7) + w2 + SIGMA0(w10) + w9;
        SHA512ROUND(h, a, b, c, d, e, f, g, 73, w9);
        w10 = SIGMA1(w8) + w3 + SIGMA0(w11) + w10;
        SHA512ROUND(g, h, a, b, c, d, e, f, 74, w10);
        w11 = SIGMA1(w9) + w4 + SIGMA0(w12) + w11;
        SHA512ROUND(f, g, h, a, b, c, d, e, 75, w11);
        w12 = SIGMA1(w10) + w5 + SIGMA0(w13) + w12;
        SHA512ROUND(e, f, g, h, a, b, c, d, 76, w12);
        w13 = SIGMA1(w11) + w6 + SIGMA0(w14) + w13;
        SHA512ROUND(d, e, f, g, h, a, b, c, 77, w13);
        w14 = SIGMA1(w12) + w7 + SIGMA0(w15) + w14;
        SHA512ROUND(c, d, e, f, g, h, a, b, 78, w14);
        w15 = SIGMA1(w13) + w8 + SIGMA0(w0) + w15;
        SHA512ROUND(b, c, d, e, f, g, h, a, 79, w15);

        ctx->state.s64[0] += a;
        ctx->state.s64[1] += b;
        ctx->state.s64[2] += c;
        ctx->state.s64[3] += d;
        ctx->state.s64[4] += e;
        ctx->state.s64[5] += f;
        ctx->state.s64[6] += g;
        ctx->state.s64[7] += h;

}
#endif  /* !__amd64 */


/*
 * Encode()
 *
 * purpose: to convert a list of numbers from little endian to big endian
 *   input: uint8_t *   : place to store the converted big endian numbers
 *          uint32_t *  : place to get numbers to convert from
 *          size_t      : the length of the input in bytes
 *  output: void
 */

static void
Encode(uint8_t *_RESTRICT_KYWD output, uint32_t *_RESTRICT_KYWD input,
    size_t len)
{
        size_t          i, j;

#if     defined(__sparc)
        if (IS_P2ALIGNED(output, sizeof (uint32_t))) {
                for (i = 0, j = 0; j < len; i++, j += 4) {
                        /* LINTED: pointer alignment */
                        *((uint32_t *)(output + j)) = input[i];
                }
        } else {
#endif  /* little endian -- will work on big endian, but slowly */
                for (i = 0, j = 0; j < len; i++, j += 4) {
                        output[j]       = (input[i] >> 24) & 0xff;
                        output[j + 1]   = (input[i] >> 16) & 0xff;
                        output[j + 2]   = (input[i] >>  8) & 0xff;
                        output[j + 3]   = input[i] & 0xff;
                }
#if     defined(__sparc)
        }
#endif
}
```

unchanged_portion_omitted_

```
#endif /* _KERNEL */

/*
 * SHA2Update()
 *
 * purpose: continues an sha2 digest operation, using the message block
 *          to update the context.
 *   input: SHA2_CTX *  : the context to update
 *          void *      : the message block
 *          size_t      : the length of the message block, in bytes
 *          size_t    : the length of the message block in bytes
 *  output: void
 */

void
SHA2Update(SHA2_CTX *ctx, const void *inptr, size_t input_len)
{
        uint32_t        i, buf_index, buf_len, buf_limit;
        const uint8_t   *input = inptr;
        uint32_t        algotype = ctx->algotype;
#if defined(__amd64)
        uint32_t        block_count;
#endif  /* !__amd64 */


        /* check for noop */
        if (input_len == 0)
                return;

        if (algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {
        if (ctx->algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {
                buf_limit = 64;

                /* compute number of bytes mod 64 */
                buf_index = (ctx->count.c32[1] >> 3) & 0x3F;

                /* update number of bits */
                if ((ctx->count.c32[1] += (input_len << 3)) < (input_len << 3))
                        ctx->count.c32[0]++;

                ctx->count.c32[0] += (input_len >> 29);

        } else {
                buf_limit = 128;

                /* compute number of bytes mod 128 */
                buf_index = (ctx->count.c64[1] >> 3) & 0x7F;

                /* update number of bits */
                if ((ctx->count.c64[1] += (input_len << 3)) < (input_len << 3))
                        ctx->count.c64[0]++;

                ctx->count.c64[0] += (input_len >> 29);
        }

        buf_len = buf_limit - buf_index;

        /* transform as many times as possible */
        i = 0;
        if (input_len >= buf_len) {

                /*
                 * general optimization:
                 *
                 * only do initial bcopy() and SHA2Transform() if
```



```
                 * buf_index != 0.  if buf_index == 0, we're just
                 * wasting our time doing the bcopy() since there
                 * wasn't any data left over from a previous call to
                 * SHA2Update().
                 */
                if (buf_index) {
                        bcopy(input, &ctx->buf_un.buf8[buf_index], buf_len);
                        if (algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE)
                        if (ctx->algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE)
                                SHA256Transform(ctx, ctx->buf_un.buf8);
                        else
                                SHA512Transform(ctx, ctx->buf_un.buf8);

                        i = buf_len;
                }

#if !defined(__amd64)
                if (algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {

                        for (; i + buf_limit - 1 < input_len; i += buf_limit) {
                        if (ctx->algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE)
                                SHA256Transform(ctx, &input[i]);
                        }
                } else {
                        for (; i + buf_limit - 1 < input_len; i += buf_limit) {
                        else
                                SHA512Transform(ctx, &input[i]);
                        }
                }

#else
                if (algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {
                        block_count = (input_len - i) >> 6;
                        if (block_count > 0) {
                                SHA256TransformBlocks(ctx, &input[i],
                                    block_count);
                                i += block_count << 6;
                        }
                } else {
                        block_count = (input_len - i) >> 7;
                        if (block_count > 0) {
                                SHA512TransformBlocks(ctx, &input[i],
                                    block_count);
                                i += block_count << 7;
                        }
                }
#endif  /* !__amd64 */

                /*
                 * general optimization:
                 *
                 * if i and input_len are the same, return now instead
                 * of calling bcopy(), since the bcopy() in this case
                 * will be an expensive noop.
                 * will be an expensive nop.
                 */

                if (input_len == i)
                        return;

                buf_index = 0;
        }

        /* buffer remaining input */
        bcopy(&input[i], &ctx->buf_un.buf8[buf_index], input_len - i);
}
```

```
 876 /*
 877  * SHA2Final()
 878  *
 879  * purpose: ends an sha2 digest operation, finalizing the message digest and
 880  *          zeroing the context.
 881  *   input: uchar_t *   : a buffer to store the digest
 848  *   input: uchar_t *   : a buffer to store the digest in
 882  *                      : The function actually uses void* because many
 883  *                      : callers pass things other than uchar_t here.
 884  *          SHA2_CTX *  : the context to finalize, save, and zero
 885  *  output: void
 886  */

 888 void
 889 SHA2Final(void *digest, SHA2_CTX *ctx)
 890 {
 891         uint8_t         bitcount_be[sizeof (ctx->count.c32)];
 892         uint8_t         bitcount_be64[sizeof (ctx->count.c64)];
 893         uint32_t        index;
 894         uint32_t        algotype = ctx->algotype;

 896         if (algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {

 863         if (ctx->algotype <= SHA256_HMAC_GEN_MECH_INFO_TYPE) {
 897                 index  = (ctx->count.c32[1] >> 3) & 0x3f;
 898                 Encode(bitcount_be, ctx->count.c32, sizeof (bitcount_be));
 899                 SHA2Update(ctx, PADDING, ((index < 56) ? 56 : 120) - index);
 900                 SHA2Update(ctx, bitcount_be, sizeof (bitcount_be));
 901                 Encode(digest, ctx->state.s32, sizeof (ctx->state.s32));

 903         } else {
 904                 index  = (ctx->count.c64[1] >> 3) & 0x7f;
 905                 Encode64(bitcount_be64, ctx->count.c64,
 906                     sizeof (bitcount_be64));
 907                 SHA2Update(ctx, PADDING, ((index < 112) ? 112 : 240) - index);
 908                 SHA2Update(ctx, bitcount_be64, sizeof (bitcount_be64));
 909                 if (algotype <= SHA384_HMAC_GEN_MECH_INFO_TYPE) {
 876                 if (ctx->algotype <= SHA384_HMAC_GEN_MECH_INFO_TYPE) {
 910                         ctx->state.s64[6] = ctx->state.s64[7] = 0;
 911                         Encode64(digest, ctx->state.s64,
 912                             sizeof (uint64_t) * 6);
 913                 } else
 914                         Encode64(digest, ctx->state.s64,
 915                             sizeof (ctx->state.s64));
 916         }

 918         /* zeroize sensitive information */
 919         bzero(ctx, sizeof (*ctx));
 920 }
```

*unchanged_portion_omitted_*

```
**********
    3404 Mon Mar 24 15:32:16 2008
new/usr/src/lib/libmd/Makefile.com
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile.com       1.5     08/03/20 SMI"
# ident "@(#)Makefile.com       1.4     08/03/02 SMI"
#

# $LIBRARY is set in lower makefiles so we can have platform and
# processor optimised versions of this library via libmd_psr and libmd_hwcapN

#LIBRARY= libmd.a
VERS= .1

OBJECTS= md4.o md5.o $(MD5_PSR_OBJECTS) sha1.o $(SHA1_PSR_OBJECTS) \
                sha2.o $(SHA2_PSR_OBJECTS)
OBJECTS= md4.o md5.o $(MD5_PSR_OBJECTS) sha1.o $(SHA1_PSR_OBJECTS) sha2.o

# Use $(SRC) to include makefiles rather than ../../ because the
# platform subdirs are one level deeper so it would be ../../../ for them
include $(SRC)/lib/Makefile.lib
include $(SRC)/lib/Makefile.rootfs

LIBS =          $(DYNLIB) $(LINTLIB)
SRCS = \
        $(COMDIR)/md4/md4.c \
        $(COMDIR)/md5/md5.c \
        $(COMDIR)/sha1/sha1.c \
        $(COMDIR)/sha2/sha2.c

COMDIR= $(SRC)/common/crypto

$(LINTLIB) :=   SRCS = $(SRCDIR)/$(LINTSRC)
LDLIBS +=       -lc

SRCDIR =        ../common
COMDIR =        $(SRC)/common/crypto

CFLAGS += $(CCVERBOSE) $(C_BIGPICFLAGS)
CFLAGS64 += $(C_BIGPICFLAGS)
CPPFLAGS += -I$(SRCDIR)
```



```
# The md5 and sha1 code is very careful about data alignment
# but lint doesn't know that, so just shut lint up.
LINTFLAGS += -erroff=E_SUPPRESSION_DIRECTIVE_UNUSED
LINTFLAGS64 += -erroff=E_SUPPRESSION_DIRECTIVE_UNUSED


ROOTLINT= $(LINTSRC:%=$(ROOTLIBDIR)/%)

.KEEP_STATE:

all: $(LIBS) fnamecheck

lint: lintcheck

pics/%.o: $(COMDIR)/md4/%.c
        $(COMPILE.c) -I$(COMDIR)/md4 -o $@ $<
        $(POST_PROCESS_O)

pics/%.o: $(COMDIR)/md5/%.c
        $(COMPILE.c) -I$(COMDIR)/md5 $(INLINES) -o $@ $<
        $(POST_PROCESS_O)

pics/%.o: $(COMDIR)/sha1/%.c
        $(COMPILE.c) -I$(COMDIR)/sha1 -o $@ $<
        $(POST_PROCESS_O)

pics/%.o: $(COMDIR)/sha1/sparc/$(PLATFORM)/sha1_asm.s
        $(COMPILE.s) -P -DPIC -D_ASM -o $@ $<
        $(POST_PROCESS_O)

pics/%.o: $(COMDIR)/sha2/%.c
        $(COMPILE.c) -I$(COMDIR)/sha2 -o $@ $<
        $(POST_PROCESS_O)

#
# Used when building links in /platform/$(PLATFORM)/lib for libmd_psr.so.1
#

LIBMD_PSR_DIRS = $(LINKED_PLATFORMS:%=$(ROOT_PLAT_DIR)/%/lib)
LIBMD_PSR_LINKS = $(LINKED_PLATFORMS:%=$(ROOT_PLAT_DIR)/%/lib/$(MODULE))

LIBMD_PSR64_DIRS = $(LINKED_PLATFORMS:%=$(ROOT_PLAT_DIR)/%/lib/$(MACH64))
LIBMD_PSR64_LINKS = $(LINKED_PLATFORMS:%=$(ROOT_PLAT_DIR)/%/lib/$(MACH64)/$(MODU

INS.slink6 = $(RM) -r $@; $(SYMLINK) ../../$(PLATFORM)/lib/$(MODULE) $@ $(CHOWNL

INS.slink64 = $(RM) -r $@; $(SYMLINK) ../../../$(PLATFORM)/lib/$(MACH64)/$(MODUL

$(LIBMD_PSR_DIRS):
        -$(INS.dir.root.bin)

$(LIBMD_PSR_LINKS): $(LIBMD_PSR_DIRS)
        -$(INS.slink6)

$(LIBMD_PSR64_DIRS):
        -$(INS.dir.root.bin)

$(LIBMD_PSR64_LINKS): $(LIBMD_PSR64_DIRS)
        -$(INS.slink64)

include $(SRC)/lib/Makefile.targ
```

```
**********************************************************
    1686 Mon Mar 24 15:32:20 2008
new/usr/src/lib/libmd/amd64/Makefile
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile   1.4     08/03/20 SMI"
# ident "@(#)Makefile   1.3     08/03/02 SMI"
#

LIBRARY= libmd.a

MD5_PSR_OBJECTS = md5_amd64.o
SHA1_PSR_OBJECTS = sha1-x86_64.o
SHA2_PSR_OBJECTS = sha512-x86_64.o sha256-x86_64.o

include ../Makefile.com
include $(SRC)/lib/Makefile.lib.64

CLEANFILES += md5_amd64.s sha1-x86_64.s sha512-x86_64.s sha256-x86_64.s
CLEANFILES += md5_amd64.s sha1-x86_64.s

# This prevents <sys/asm_linkage.h> from including C source:
AS_CPPFLAGS += -D_ASM

install: all $(ROOTLIBS64) $(ROOTLINKS64) $(ROOTLINT64)

pics/%.o: %.s
pics/md5_amd64.o: md5_amd64.s
        $(COMPILE.s) -o $@ ${@F:.o=.s}
        $(POST_PROCESS_O)

pics/sha1-x86_64.o: sha1-x86_64.s
        $(COMPILE.s) -o $@ ${@F:.o=.s}
        $(POST_PROCESS_O)

md5_amd64.s: $(COMDIR)/md5/amd64/md5_amd64.pl
        $(PERL) $? $@

sha1-x86_64.s: $(COMDIR)/sha1/amd64/sha1-x86_64.pl
        $(PERL) $? $@

sha512-x86_64.s: $(COMDIR)/sha2/amd64/sha512-x86_64.pl
```



```
        $(PERL) $? $@

sha256-x86_64.s: $(COMDIR)/sha2/amd64/sha512-x86_64.pl
        $(PERL) $? $@
```

```
**********************************************************
    6448 Mon Mar 24 15:32:24 2008
new/usr/src/lib/pkcs11/pkcs11_softtoken/Makefile.com
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile.com       1.6     08/03/20 SMI"
# ident "@(#)Makefile.com       1.5     08/02/26 SMI"
#
# lib/pkcs11/pkcs11_softtoken/Makefile.com
#

LIBRARY = pkcs11_softtoken.a
VERS= .1

LCL_OBJECTS = \
        softGeneral.o           \
        softSlotToken.o         \
        softSession.o           \
        softObject.o            \
        softDigest.o            \
        softSign.o              \
        softVerify.o            \
        softDualCrypt.o         \
        softKeys.o              \
        softRand.o              \
        softSessionUtil.o       \
        softDigestUtil.o        \
        softAttributeUtil.o     \
        softObjectUtil.o        \
        softDESCrypt.o          \
        softEncrypt.o           \
        softDecrypt.o           \
        softEncryptUtil.o       \
        softDecryptUtil.o       \
        softSignUtil.o          \
        softVerifyUtil.o        \
        softMAC.o               \
        softRSA.o               \
        softRandUtil.o          \
        softKeysUtil.o          \
        softARCFourCrypt.o      \
        softDSA.o               \
```



```
        softDH.o                \
        softAESCrypt.o          \
        softCrypt.o             \
        softKeystore.o          \
        softKeystoreUtil.o      \
        softSSL.o               \
        softASN1.o              \
        softBlowfishCrypt.o     \
        softEC.o

ASFLAGS = $(AS_PICFLAGS) -P -D__STDC__ -D_ASM $(CPPFLAGS)

AES_COBJECTS = aes_cbc_crypt.o  aes_impl.o
BLOWFISH_COBJECTS = blowfish_cbc_crypt.o blowfish_impl.o
ARCFOUR_COBJECTS = arcfour_crypt.o
DES_COBJECTS = des_cbc_crypt.o des_impl.o des_ks.o

ECC_COBJECTS = \
        ec.o ec2_163.o ec2_mont.o ecdecode.o ecl_mult.o ecp_384.o \
        ecp_jac.o ec2_193.o ecl.o ecp_192.o ecp_521.o \
        ecp_jm.o ec2_233.o ecl_curve.o ecp_224.o ecp_aff.o ecp_mont.o \
        ec2_aff.o ec_naf.o ecl_gf.o ecp_256.o oid.o secitem.o \
        ec2_test.o ecp_test.o

MPI_COBJECTS = mp_gf2m.o mpi.o mplogic.o mpmontg.o mpprime.o

RSA_COBJECTS = rsa_impl.o
BIGNUM_COBJECTS = bignumimpl.o

AES_OBJECTS = $(AES_COBJECTS) $(AES_PSR_OBJECTS)
BLOWFISH_OBJECTS = $(BLOWFISH_COBJECTS) $(BLOWFISH_PSR_OBJECTS)
ARCFOUR_OBJECTS = $(ARCFOUR_COBJECTS) $(ARCFOUR_PSR_OBJECTS)
DES_OBJECTS = $(DES_COBJECTS) $(DES_PSR_OBJECTS)

ECC_OBJECTS = $(ECC_COBJECTS) $(ECC_PSR_OBJECTS)
MPI_OBJECTS = $(MPI_COBJECTS) $(MPI_PSR_OBJECTS)
RSA_OBJECTS = $(RSA_COBJECTS) $(RSA_PSR_OBJECTS)
SHA1_OBJECTS = $(SHA1_COBJECTS) $(SHA1_PSR_OBJECTS)
SHA2_OBJECTS = $(SHA2_COBJECTS) $(SHA2_PSR_OBJECTS)
BIGNUM_OBJECTS = $(BIGNUM_COBJECTS) $(BIGNUM_PSR_OBJECTS)

BER_OBJECTS = bprint.o decode.o encode.o io.o

# Sparc userland uses a floating-point implementation of
# Montgomery multiply.  So, USE_FLOATING_POINT is defined here
# for Sparc targets.
#
# x86 does not use floating-point for the kernel or userland.
#
# Sparc has only one integer implementation of big_mul_add_vec()
# and friends, so these functions are called directly.
# So, HWCAP (HardWare CAPabilities) is not defined for Sparc.
#
# x86 has multiple integer implementations to choose from.
# Hardware features are tested at run time, just once,
# on first use.  So, big_mul_add_vec() and friends must be
# called through a function pointer.
#
# AMD64 has a 64x64->128 bit multiply instruction, which makes
# things even faster than i386 SSE2 instructions.  Since there
# is no run-time testing of features, as there is for SSE2,
# there is no need to call big_mul_add_vec() and friends through
# functions pointers, and so HWCAP is not defined.
#
# For now i386 and amd64 use the C code version of mont_mulf
```

```
125 OBJECTS = \
126         $(LCL_OBJECTS)          \
127         $(AES_OBJECTS)          \
128         $(BLOWFISH_OBJECTS)     \
129         $(ARCFOUR_OBJECTS)      \
130         $(DES_OBJECTS)          \
131         $(MPI_OBJECTS)          \
132         $(RSA_OBJECTS)          \
135         $(SHA1_OBJECTS)         \
136         $(SHA2_OBJECTS)         \
133         $(BIGNUM_OBJECTS)       \
134         $(BER_OBJECTS)          \
135         $(ECC_OBJECTS)

137 AESDIR=         $(SRC)/common/crypto/aes
138 BLOWFISHDIR=    $(SRC)/common/crypto/blowfish
139 ARCFOURDIR=     $(SRC)/common/crypto/arcfour
140 DESDIR=         $(SRC)/common/crypto/des
141 ECCDIR=         $(SRC)/common/crypto/ecc
142 MPIDIR=         $(SRC)/common/mpi
143 RSADIR=         $(SRC)/common/crypto/rsa
144 BIGNUMDIR=      $(SRC)/common/bignum
145 BERDIR=         ../../../libldap5/sources/ldap/ber

147 include $(SRC)/lib/Makefile.lib

149 #       set signing mode
150 POST_PROCESS_SO +=      ; $(ELFSIGN_CRYPTO)

152 SRCDIR= ../common

154 SRCS =  \
155         $(LCL_OBJECTS:%.o=$(SRCDIR)/%.c) \
156         $(AES_COBJECTS:%.o=$(AESDIR)/%.c) \
157         $(BLOWFISH_COBJECTS:%.o=$(BLOWFISHDIR)/%.c) \
158         $(ARCFOUR_COBJECTS:%.o=$(ARCFOURDIR)/%.c) \
159         $(DES_COBJECTS:%.o=$(DESDIR)/%.c) \
160         $(MPI_COBJECTS:%.o=$(MPIDIR)/%.c) \
161         $(RSA_COBJECTS:%.o=$(RSADIR)/%.c) \
166         $(SHA1_COBJECTS:%.o=$(SHA1DIR)/%.c) \
167         $(SHA2_COBJECTS:%.o=$(SHA2DIR)/%.c) \
162         $(BIGNUM_COBJECTS:%.o=$(BIGNUMDIR)/%.c) \
163         $(BIGNUM_PSR_SRCS) \
164         $(ECC_COBJECTS:%.o=$(ECCDIR)/%.c)

166 # libelfsign needs a static pkcs11_softtoken
167 LIBS    =       $(DYNLIB)
168 LDLIBS  +=      -lc -lmd -lcryptoutil

170 CFLAGS  +=      $(CCVERBOSE)
171 CPPFLAGS += -I$(AESDIR) -I$(BLOWFISHDIR) -I$(ARCFOURDIR) -I$(DESDIR) \
172             -I$(ECCDIR) -I$(MPIDIR) -I$(RSADIR) -I$(SRCDIR) -I$(BIGNUMDIR) \
173             -D_POSIX_PTHREAD_SEMANTICS -DMP_API_COMPATIBLE \
174             -DNSS_ECC_MORE_THAN_SUITE_B

176 LINTFLAGS64 += -errchk=longptr64

178 ROOTLIBDIR=     $(ROOT)/usr/lib/security
179 ROOTLIBDIR64=   $(ROOT)/usr/lib/security/$(MACH64)

181 LINTSRC = \
182         $(LCL_OBJECTS:%.o=$(SRCDIR)/%.c) \
183         $(AES_COBJECTS:%.o=$(AESDIR)/%.c) \
184         $(BLOWFISH_COBJECTS:%.o=$(BLOWFISHDIR)/%.c) \
185         $(ARCFOUR_COBJECTS:%.o=$(ARCFOURDIR)/%.c) \
186         $(DES_COBJECTS:%.o=$(DESDIR)/%.c) \
```



```
187         $(RSA_COBJECTS:%.o=$(RSADIR)/%.c) \
194         $(SHA1_COBJECTS:%.o=$(SHA1DIR)/%.c) \
195         $(SHA2_COBJECTS:%.o=$(SHA2DIR)/%.c) \
188         $(BIGNUM_COBJECTS:%.o=$(BIGNUMDIR)/%.c) \
189         $(BIGNUM_PSR_SRCS)

191 .KEEP_STATE:

193 all:    $(LIBS)

195 lint:   $$(LINTSRC)
196         $(LINT.c) $(LINTCHECKFLAGS) $(LINTSRC) $(LDLIBS)

198 pics/%.o:       $(AESDIR)/%.c
199         $(COMPILE.c) -o $@ $<
200         $(POST_PROCESS_O)

202 pics/%.o:       $(BLOWFISHDIR)/%.c
203         $(COMPILE.c) -o $@ $<
204         $(POST_PROCESS_O)

206 pics/%.o:       $(ARCFOURDIR)/%.c
207         $(COMPILE.c) -o $@ $<
208         $(POST_PROCESS_O)

210 pics/%.o:       $(DESDIR)/%.c
211         $(COMPILE.c) -o $@ $<
212         $(POST_PROCESS_O)

214 pics/%.o:       $(ECCDIR)/%.c
215         $(COMPILE.c) -o $@ $<
216         $(POST_PROCESS_O)

218 pics/%.o:       $(MPIDIR)/%.c
219         $(COMPILE.c) -o $@ $<
220         $(POST_PROCESS_O)

222 pics/%.o:       $(RSADIR)/%.c
223         $(COMPILE.c) -o $@ $<
224         $(POST_PROCESS_O)

234 pics/%.o:       $(SHA1DIR)/%.c
235         $(COMPILE.c) -o $@ $<
236         $(POST_PROCESS_O)

238 pics/%.o:       $(SHA2DIR)/%.c
239         $(COMPILE.c) -o $@ $<
240         $(POST_PROCESS_O)

226 pics/%.o:       $(BIGNUMDIR)/%.c
227         $(COMPILE.c) -o $@ $(BIGNUM_CFG) $<
228         $(POST_PROCESS_O)

230 pics/%.o:       $(BERDIR)/%.c
231         $(COMPILE.c) -o $@ $< -D_SOLARIS_SDK -I$(BERDIR) \
232                 -I../../../libldap5/include/ldap
233         $(POST_PROCESS_O)

235 include $(SRC)/lib/Makefile.targ
```

```
**********************************************************
    1999 Mon Mar 24 15:32:28 2008
new/usr/src/lib/pkcs11/pkcs11_softtoken/amd64/Makefile
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile   1.5     08/03/20 SMI"
# ident "@(#)Makefile   1.4     08/02/26 SMI"
#
# lib/pkcs11/pkcs11_softtoken/amd64/Makefile

AES_PSR_OBJECTS =
ARCFOUR_PSR_OBJECTS =  arcfour-x86_64.o
ARCFOUR_PSR_OBJECTS =  arcfour_crypt_amd64.o
DES_PSR_OBJECTS =
RSA_PSR_OBJECTS =
SHA1_PSR_OBJECTS =
BIGNUM_PSR_OBJECTS = bignum_amd64.o bignum_amd64_asm.o
BIGNUM_PSR_PICS = $(BIGNUM_PSR_OBJECTS:%=pics/%)
BIGNUM_CFG = -DPSR_MUL
BIGNUM_PSR_SRCS = \
        $(BIGNUMDIR)/amd64/bignum_amd64.c \
        $(BIGNUMDIR)/amd64/bignum_amd64_asm.s

pics/bignum_amd64.o := amd64_COPTFLAG = -xO3

include ../Makefile.com
include ../../../Makefile.lib.64

#
# Overrides
#
CLEANFILES      += arcfour-x86_64.s

install: all $(ROOTLIBS64) $(ROOTLINKS64)

$(BIGNUM_PSR_PICS) := CFLAGS += $(C_BIGPICFLAGS) $(BIGNUM_CFG)

LINTFLAGS64 += $(BIGNUM_CFG)

pics/arcfour-x86_64.o: arcfour-x86_64.s
        $(COMPILE.s) -o $@ $(AS_BIGPICFLAGS) ${@F:.o=.s}
```



```
pics/arcfour_crypt_amd64.o: $(ARCFOURDIR)/amd64/arcfour_crypt_amd64.s
        $(COMPILE.s) -o $@ $(AS_BIGPICFLAGS) \
                $(ARCFOURDIR)/amd64/arcfour_crypt_amd64.s
        $(POST_PROCESS_O)

arcfour-x86_64.s: $(ARCFOURDIR)/amd64/arcfour-x86_64.pl
        $(PERL) $? $@

pics/%.o: $(BIGNUMDIR)/$(MACH64)/%.c
        $(COMPILE.c) -o $@ $(C_BIGPICFLAGS) $(BIGNUM_CFG) $<
        $(POST_PROCESS_O)

pics/%.o: $(BIGNUMDIR)/$(MACH64)/%.s
        $(COMPILE.s) -o $@ $(AS_BIGPICFLAGS) $(BIGNUM_CFG) $<
        $(POST_PROCESS_O)
```

```
**********************************************************
    1605 Mon Mar 24 15:32:33 2008
new/usr/src/lib/pkcs11/pkcs11_softtoken/i386/Makefile
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)Makefile   1.6     08/03/20 SMI"
  25 # ident "@(#)Makefile   1.5     08/02/26 SMI"
  26 #
  27 # lib/pkcs11/pkcs11_softtoken/i386/Makefile

  29 AES_PSR_OBJECTS =
  30 ARCFOUR_PSR_OBJECTS =
  31 DES_PSR_OBJECTS =
  32 RSA_PSR_OBJECTS =
  33 SHA1_PSR_OBJECTS =
  33 BIGNUM_PSR_OBJECTS = bignum_i386.o bignum_i386_asm.o
  34 BIGNUM_CFG = -DPSR_MUL -DHWCAP
  35 BIGNUM_PSR_SRCS = \
  36         $(BIGNUMDIR)/i386/bignum_i386.c \
  37         $(BIGNUMDIR)/i386/bignum_i386_asm.s

  39 include ../Makefile.com

  41 CPPFLAGS += -DMP_USE_UINT_DIGIT

  43 install: all $(ROOTLIBS) $(ROOTLINKS)

  45 DYNFLAGS += -M $(BIGNUMDIR)/i386/cap_mapfile

  47 pics/bignum_i386.o := COPTFLAG = -xO3

  49 pics/%.o:       $(BIGNUMDIR)/$(MACH)/%.c
  50         $(COMPILE.c) -o $@ $(BIGNUM_CFG) $<
  51         $(POST_PROCESS_O)

  53 pics/%.o:       $(BIGNUMDIR)/$(MACH)/%.s
  54         $(COMPILE.s) -o $@ $(BIGNUM_CFG) $<
  55         $(POST_PROCESS_O)
```

```
**********************************************************
   87373 Mon Mar 24 15:32:37 2008
new/usr/src/pkgdefs/SUNWcsu/prototype_com
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)prototype_com      1.569   08/03/20 SMI"
  25 # ident "@(#)prototype_com      1.568   08/02/21 SMI"
  26 #
  27 # This required package information file contains a list of package contents.
  28 # The 'pkgmk' command uses this file to identify the contents of a package
  29 # and their location on the development machine when building the package.
  30 # Can be created via a text editor or through use of the 'pkgproto' command.


  33 #!search <pathname pathname ...>        # where to find pkg objects
  34 #!include <filename>                    # include another 'prototype' file
  35 #!default <mode> <owner> <group>        # default used if not specified on entry
  36 #!<param>=<value>                       # puts parameter in pkg environment

  38 # packaging files
  39 i pkginfo
  40 i copyright
  41 i postinstall
  42 #
  43 # source locations relative to the prototype file
  44 #
  45 # SUNWcsu
  46 #
  47 d none usr 755 root sys
  48 s none usr/adm=../var/adm
  49 d none usr/bin 755 root bin
  50 f none usr/bin/alias 555 root bin
  51 f none usr/bin/amt 555 root bin
  52 f none usr/bin/arch 555 root bin
  53 f none usr/bin/at 4755 root sys
  54 f none usr/bin/atq 4755 root sys
  55 f none usr/bin/atrm 4755 root sys
  56 f none usr/bin/auths 555 root bin
  57 f none usr/bin/basename 555 root bin
  58 l none usr/bin/bg=../../usr/bin/alias
  59 f none usr/bin/busstat 555 root bin
  60 s none usr/bin/cachefspack=../lib/fs/cachefs/cachefspack
```



```
  61 s none usr/bin/cachefsstat=../lib/fs/cachefs/cachefsstat
  62 f none usr/bin/captoinfo 555 root bin
  63 f none usr/bin/cat 555 root bin
  64 l none usr/bin/cd=../../usr/bin/alias
  65 f none usr/bin/chgrp 555 root bin
  66 f none usr/bin/chmod 555 root bin
  67 f none usr/bin/chown 555 root bin
  68 f none usr/bin/ckdate 555 root bin
  69 f none usr/bin/ckgid 555 root bin
  70 f none usr/bin/ckint 555 root bin
  71 f none usr/bin/ckitem 555 root bin
  72 f none usr/bin/ckkeywd 555 root bin
  73 f none usr/bin/ckpath 555 root bin
  74 f none usr/bin/ckrange 555 root bin
  75 f none usr/bin/ckstr 555 root bin
  76 f none usr/bin/cksum 555 root bin
  77 f none usr/bin/cktime 555 root bin
  78 f none usr/bin/ckuid 555 root bin
  79 f none usr/bin/ckyorn 555 root bin
  80 f none usr/bin/clear 555 root bin
  81 f none usr/bin/cmp 555 root bin
  82 l none usr/bin/command=../../usr/bin/alias
  83 f none usr/bin/coreadm 555 root bin
  84 f none usr/bin/cp 555 root bin
  85 f none usr/bin/cpio 555 root bin
  86 f none usr/bin/crle 555 root bin
  87 f none usr/bin/crontab 4555 root bin
  88 f none usr/bin/crypt 555 root bin
  89 f none usr/bin/csh 555 root bin
  90 f none usr/bin/ctrun 555 root bin
  91 f none usr/bin/ctstat 555 root bin
  92 f none usr/bin/ctwatch 555 root bin
  93 f none usr/bin/cut 555 root bin
  94 f none usr/bin/date 555 root bin
  95 f none usr/bin/dd 555 root bin
  96 f none usr/bin/decrypt 555 root bin
  97 f none usr/bin/devattr 555 root bin
  98 f none usr/bin/devfree 555 root bin
  99 f none usr/bin/devreserv 555 root bin
 100 s none usr/bin/df=../sbin/df
 101 l none usr/bin/digest=../../usr/lib/isaexec
 101 f none usr/bin/digest 555 root bin
 102 f none usr/bin/dirname 555 root bin
 103 l none usr/bin/dispgid=../../usr/bin/ckgid
 104 l none usr/bin/dispuid=../../usr/bin/ckuid
 105 f none usr/bin/domainname 555 root bin
 106 f none usr/bin/du 555 root bin
 107 f none usr/bin/dumpcs 555 root bin
 108 f none usr/bin/dumpkeys 555 root bin
 109 f none usr/bin/echo 555 root bin
 110 f none usr/bin/ed 555 root bin
 111 f none usr/bin/edit 555 root bin
 112 f none usr/bin/egrep 555 root bin
 113 f none usr/bin/eject 555 root bin
 114 l none usr/bin/encrypt=../../usr/bin/decrypt
 115 f none usr/bin/env 555 root bin
 116 l none usr/bin/ex=../../usr/bin/edit
 117 f none usr/bin/expr 555 root bin
 118 f none usr/bin/false 555 root bin
 119 l none usr/bin/fc=../../usr/bin/alias
 120 f none usr/bin/fdetach 555 root bin
 121 f none usr/bin/fdformat 4555 root bin
 122 l none usr/bin/fg=../../usr/bin/alias
 123 f none usr/bin/fgrep 555 root bin
 124 f none usr/bin/file 555 root bin
 125 f none usr/bin/find 555 root bin
```

```
126 f none usr/bin/fmli 755 root bin
127 f none usr/bin/fmt 555 root bin
128 f none usr/bin/fmtmsg 555 root bin
129 f none usr/bin/fold 555 root bin
130 f none usr/bin/fsstat 555 root bin
131 f none usr/bin/geniconvtbl 555 root bin
132 f none usr/bin/getconf 555 root bin
133 f none usr/bin/getdev 555 root bin
134 f none usr/bin/getdgrp 555 root bin
135 f none usr/bin/getent 555 root bin
136 f none usr/bin/getfacl 555 root bin
137 f none usr/bin/getopt 555 root bin
138 l none usr/bin/getopts=../../usr/bin/alias
139 f none usr/bin/gettext 555 root bin
140 f none usr/bin/getvol 555 root bin
141 f none usr/bin/grep 555 root bin
142 f none usr/bin/groups 555 root bin
143 l none usr/bin/hash=../../usr/bin/alias
144 f none usr/bin/head 555 root bin
145 f none usr/bin/hostid 555 root bin
146 f none usr/bin/hostname 555 root bin
147 f none usr/bin/i286 555 root bin
148 l none usr/bin/i386=../../usr/bin/i286
149 l none usr/bin/i486=../../usr/bin/i286
150 l none usr/bin/i860=../../usr/bin/i286
151 l none usr/bin/i86pc=../../usr/bin/i286
152 l none usr/bin/iAPX286=../../usr/bin/i286
153 f none usr/bin/iconv 555 root bin
154 f none usr/bin/id 555 root bin
155 f none usr/bin/infocmp 555 root bin
156 f none usr/bin/iostat 555 root bin
157 f none usr/bin/isainfo 555 root bin
158 f none usr/bin/isalist 555 root bin
159 l none usr/bin/jobs=../../usr/bin/alias
160 f none usr/bin/join 555 root bin
161 s none usr/bin/jsh=../../sbin/sh
162 f none usr/bin/kbd 555 root bin
163 f none usr/bin/keylogin 555 root bin
164 f none usr/bin/keylogout 555 root bin
165 l none usr/bin/kill=../../usr/bin/alias
166 f none usr/bin/kmfcfg 555 root bin
167 f none usr/bin/ksh 555 root bin
168 l none usr/bin/ksh93=../../usr/lib/isaexec
169 f none usr/bin/line 555 root bin
170 f none usr/bin/listdgrp 555 root bin
171 f none usr/bin/listusers 555 root bin
172 l none usr/bin/ln=../../usr/bin/cp
173 f none usr/bin/loadkeys 555 root bin
174 f none usr/bin/localedef 555 root bin
175 f none usr/bin/logger 555 root bin
176 f none usr/bin/login 4555 root bin
177 f none usr/bin/logins 750 root bin
178 f none usr/bin/ls 555 root bin
179 l none usr/bin/m68k=../../usr/bin/i286
180 l none usr/bin/mac=../../usr/lib/isaexec
180 l none usr/bin/mac=../../usr/bin/digest
181 f none usr/bin/mach 555 root bin
182 f none usr/bin/mail 2511 root mail
183 f none usr/bin/mailx 2511 root mail
184 f none usr/bin/makedev 555 root bin
185 l none usr/bin/mc68000=../../usr/bin/i286
186 l none usr/bin/mc68010=../../usr/bin/i286
187 l none usr/bin/mc68020=../../usr/bin/i286
188 l none usr/bin/mc68030=../../usr/bin/i286
189 l none usr/bin/mc68040=../../usr/bin/i286
190 f none usr/bin/mesg 555 root bin
```



```
191 f none usr/bin/mkdir 555 root bin
192 f none usr/bin/mkpwdict 555 root bin
193 f none usr/bin/mktemp 555 root bin
194 f none usr/bin/moe 555 root bin
195 f none usr/bin/more 555 root bin
196 f none usr/bin/mpstat 555 root bin
197 f none usr/bin/mt 555 root bin
198 l none usr/bin/mv=../../usr/bin/cp
199 f none usr/bin/netstat 555 root bin
200 f none usr/bin/newgrp 4755 root sys
201 l none usr/bin/newtask=../../usr/lib/isaexec
202 f none usr/bin/nice 555 root bin
203 l none usr/bin/nohup=../../usr/lib/isaexec
204 f none usr/bin/optisa 555 root bin
205 l none usr/bin/page=../../usr/bin/more
206 f none usr/bin/pagesize 555 root bin
207 s none usr/bin/passmgmt=../sbin/passmgmt
208 f none usr/bin/passwd 6555 root sys
209 f none usr/bin/patch 555 root bin
210 f none usr/bin/pathchk 555 root bin
211 f none usr/bin/pax 555 root bin
212 l none usr/bin/pdp11=../../usr/bin/i286
213 l none usr/bin/pfcsh=../../usr/bin/csh
214 f none usr/bin/pfexec 4555 root bin
215 l none usr/bin/pfksh=../../usr/bin/ksh
216 s none usr/bin/pfsh=../../sbin/sh
217 f none usr/bin/pg 555 root bin
218 f none usr/bin/pgrep 555 root bin
219 l none usr/bin/pkill=../../usr/bin/pgrep
220 f none usr/bin/pktool 555 root bin
221 f none usr/bin/pr 555 root bin
222 l none usr/bin/prctl=../../usr/lib/isaexec
223 f none usr/bin/priocntl 555 root bin
224 f none usr/bin/profiles 555 root bin
225 f none usr/bin/projects 555 root bin
226 l none usr/bin/prstat=../../usr/lib/isaexec
227 l none usr/bin/ps=../../usr/lib/isaexec
228 f none usr/bin/putdev 555 root bin
229 f none usr/bin/putdgrp 555 root bin
230 s none usr/bin/pwconv=../sbin/pwconv
231 f none usr/bin/pwd 555 root bin
232 l none usr/bin/read=../../usr/bin/alias
233 l none usr/bin/red=../../usr/bin/ed
234 f none usr/bin/renice 555 root bin
235 l none usr/bin/rksh=../../usr/bin/ksh
236 l none usr/bin/rksh93=../../usr/lib/isaexec
237 f none usr/bin/rm 555 root bin
238 s none usr/bin/rmail=./mail
239 f none usr/bin/rmdir 555 root bin
240 f none usr/bin/roles 555 root bin
241 f none usr/bin/rpcinfo 555 root bin
242 f none usr/bin/runat 555 root bin
243 l none usr/bin/savecore=../../usr/lib/isaexec
244 f none usr/bin/script 555 root bin
245 f none usr/bin/sed 555 root bin
246 f none usr/bin/setfacl 555 root bin
247 f none usr/bin/setpgrp 555 root sys
248 f none usr/bin/settime 555 root bin
249 l none usr/bin/setuname=../../usr/lib/isaexec
250 s none usr/bin/sh=../../sbin/sh
251 f none usr/bin/sleep 555 root bin
252 l none usr/bin/sparc=../../usr/bin/i286
253 f none usr/bin/strchg 555 root root
254 s none usr/bin/strclean=../sbin/strclean
255 f none usr/bin/strconf 555 root root
256 s none usr/bin/strerr=../sbin/strerr
```

```
257 f none usr/bin/stty 555 root bin
258 f none usr/bin/su 4555 root sys
259 l none usr/bin/sun2=../../usr/bin/i286
260 l none usr/bin/sun3=../../usr/bin/i286
261 l none usr/bin/sun3x=../../usr/bin/i286
262 l none usr/bin/sun4=../../usr/bin/i286
263 l none usr/bin/sun4c=../../usr/bin/i286
264 l none usr/bin/sun4d=../../usr/bin/i286
265 l none usr/bin/sun4e=../../usr/bin/i286
266 l none usr/bin/sun4m=../../usr/bin/i286
267 l none usr/bin/sun=../../usr/bin/i286
268 f none usr/bin/svcprop 0555 root bin
269 f none usr/bin/svcs 0555 root bin
270 s none usr/bin/sync=../../sbin/sync
271 f none usr/bin/tabs 555 root bin
272 f none usr/bin/tail 555 root bin
273 s none usr/bin/tar=../sbin/tar
274 f none usr/bin/tee 555 root bin
275 l none usr/bin/test=../../usr/bin/alias
276 f none usr/bin/tic 555 root bin
277 f none usr/bin/time 555 root bin
278 f none usr/bin/tip 4511 uucp bin
279 l none usr/bin/touch=../../usr/bin/settime
280 f none usr/bin/tplot 555 root bin
281 f none usr/bin/tput 555 root bin
282 f none usr/bin/tr 555 root bin
283 f none usr/bin/true 555 root bin
284 f none usr/bin/tty 555 root bin
285 l none usr/bin/type=../../usr/bin/alias
286 f none usr/bin/tzselect 555 root bin
287 l none usr/bin/u370=../../usr/bin/i286
288 l none usr/bin/u3b15=../../usr/bin/i286
289 l none usr/bin/u3b2=../../usr/bin/i286
290 l none usr/bin/u3b5=../../usr/bin/i286
291 l none usr/bin/u3b=../../usr/bin/i286
292 l none usr/bin/ulimit=../../usr/bin/alias
293 l none usr/bin/umask=../../usr/bin/alias
294 l none usr/bin/unalias=../../usr/bin/alias
295 s none usr/bin/uname=../../sbin/uname
296 l none usr/bin/uptime=../../usr/lib/isaexec
297 l none usr/bin/vax=../../usr/bin/i286
298 l none usr/bin/vedit=../../usr/bin/edit
299 l none usr/bin/vi=../../usr/bin/edit
300 l none usr/bin/view=../../usr/bin/edit
301 f none usr/bin/vmstat 555 root bin
302 l none usr/bin/w=../../usr/lib/isaexec
303 l none usr/bin/wait=../../usr/bin/alias
304 f none usr/bin/wc 555 root bin
305 f none usr/bin/which 555 root bin
306 f none usr/bin/who 555 root bin
307 f none usr/bin/wracct 555 root bin
308 f none usr/bin/write 2555 root tty
309 f none usr/bin/xargs 555 root bin
310 f none usr/bin/xstr 555 root bin
311 d none usr/ccs 0755 root bin
312 d none usr/ccs/bin 0755 root bin
313 f none usr/bin/m4 0555 root bin
314 s none usr/ccs/bin/m4=../../bin/m4
315 d none usr/demo 755 root bin
316 d none usr/games 755 root bin
317 d none usr/kernel 755 root sys
318 d none usr/kernel/drv 755 root sys
319 f none usr/kernel/drv/dump.conf 644 root sys
320 f none usr/kernel/drv/fssnap.conf 644 root sys
321 f none usr/kernel/drv/kstat.conf 644 root sys
322 f none usr/kernel/drv/ksyms.conf 644 root sys
```



```
323 f none usr/kernel/drv/logindmux.conf 644 root sys
324 f none usr/kernel/drv/ptm.conf 644 root sys
325 f none usr/kernel/drv/pts.conf 644 root sys
326 d none usr/kernel/exec 755 root sys
327 d none usr/kernel/fs 755 root sys
328 d none usr/kernel/pcbe 755 root sys
329 d none usr/kernel/sched 755 root sys
330 d none usr/kernel/strmod 755 root sys
331 d none usr/kernel/sys 755 root sys
332 d none usr/kvm 755 root bin
333 f none usr/kvm/README 644 root sys
334 d none usr/lib 755 root bin
335 d none usr/lib/audit 0755 root bin
336 f none usr/lib/audit/audit_record_attr 444 root bin
337 f none usr/lib/calprog 555 root bin
338 d none usr/lib/class 755 root bin
339 d none usr/lib/class/FX 755 root bin
340 f none usr/lib/class/FX/FXdispadmin 555 root bin
341 f none usr/lib/class/FX/FXpriocntl 555 root bin
342 d none usr/lib/class/IA 755 root bin
343 f none usr/lib/class/IA/IAdispadmin 555 root bin
344 f none usr/lib/class/IA/IApriocntl 555 root bin
345 d none usr/lib/class/RT 755 root bin
346 f none usr/lib/class/RT/RTdispadmin 555 root bin
347 f none usr/lib/class/RT/RTpriocntl 555 root bin
348 d none usr/lib/class/TS 755 root bin
349 f none usr/lib/class/TS/TSdispadmin 555 root bin
350 f none usr/lib/class/TS/TSpriocntl 555 root bin
351 s none usr/lib/cron=../../etc/cron.d
352 d none usr/lib/crypto 755 root bin
353 f none usr/lib/crypto/kcfd 555 root bin
354 d none usr/lib/devfsadm 755 root sys
355 s none usr/lib/devfsadm/devfsadmd=../../sbin/devfsadm
356 d none usr/lib/devfsadm/linkmod 755 root sys
357 f none usr/lib/devfsadm/linkmod/SUNW_audio_link.so 755 root sys
358 f none usr/lib/devfsadm/linkmod/SUNW_cfg_link.so 755 root sys
359 f none usr/lib/devfsadm/linkmod/SUNW_disk_link.so 755 root sys
360 f none usr/lib/devfsadm/linkmod/SUNW_fssnap_link.so 755 root sys
361 f none usr/lib/devfsadm/linkmod/SUNW_lofi_link.so 755 root sys
362 f none usr/lib/devfsadm/linkmod/SUNW_md_link.so 755 root sys
363 f none usr/lib/devfsadm/linkmod/SUNW_misc_link.so 755 root sys
364 f none usr/lib/devfsadm/linkmod/SUNW_port_link.so 755 root sys
365 f none usr/lib/devfsadm/linkmod/SUNW_ramdisk_link.so 755 root sys
366 f none usr/lib/devfsadm/linkmod/SUNW_sgen_link.so 755 root sys
367 f none usr/lib/devfsadm/linkmod/SUNW_smp_link.so 755 root sys
368 f none usr/lib/devfsadm/linkmod/SUNW_tape_link.so 755 root sys
369 f none usr/lib/devfsadm/linkmod/SUNW_usb_link.so 755 root sys
370 f none usr/lib/diffh 555 root bin
371 s none usr/lib/embedded_su=../bin/su
372 f none usr/lib/expreserve 555 root bin
373 f none usr/lib/exrecover 555 root bin
374 d none usr/lib/fs 755 root sys
375 d none usr/lib/fs/cachefs 755 root sys
376 f none usr/lib/fs/cachefs/cachefsd 555 root bin
377 f none usr/lib/fs/cachefs/cachefslog 555 root bin
378 f none usr/lib/fs/cachefs/cachefspack 555 root bin
379 f none usr/lib/fs/cachefs/cachefsstat 555 root bin
380 f none usr/lib/fs/cachefs/cachefswssize 555 root bin
381 f none usr/lib/fs/cachefs/cfsadmin 555 root bin
382 f none usr/lib/fs/cachefs/cfsfstype 555 root bin
383 f none usr/lib/fs/cachefs/cfstagchk 555 root bin
384 f none usr/lib/fs/cachefs/dfshares 555 root bin
385 f none usr/lib/fs/cachefs/fsck 555 root bin
386 f none usr/lib/fs/cachefs/mount 555 root bin
387 f none usr/lib/fs/cachefs/share 555 root bin
388 f none usr/lib/fs/cachefs/umount 555 root bin
```

```
f none usr/lib/fs/cachefs/unshare 555 root bin
d none usr/lib/fs/ctfs 755 root sys
f none usr/lib/fs/ctfs/mount 555 root bin
d none usr/lib/fs/dev 755 root sys
s none usr/lib/fs/dev/mount=../../../../etc/fs/dev/mount
d none usr/lib/fs/fd 755 root sys
f none usr/lib/fs/fd/mount 555 root bin
d none usr/lib/fs/hsfs 755 root sys
f none usr/lib/fs/hsfs/fstyp.so.1 555 root bin
l none usr/lib/fs/hsfs/fstyp=../../../sbin/fstyp
f none usr/lib/fs/hsfs/labelit 555 root bin
s none usr/lib/fs/hsfs/mount=../../../../etc/fs/hsfs/mount
d none usr/lib/fs/lofs 755 root sys
f none usr/lib/fs/lofs/mount 555 root bin
d none usr/lib/fs/mntfs 755 root sys
f none usr/lib/fs/mntfs/mount 555 root bin
d none usr/lib/fs/objfs 755 root sys
f none usr/lib/fs/objfs/mount 555 root bin
d none usr/lib/fs/proc 755 root sys
f none usr/lib/fs/proc/mount 555 root bin
d none usr/lib/fs/sharefs 755 root sys
f none usr/lib/fs/sharefs/mount 555 root bin
d none usr/lib/fs/tmpfs 755 root sys
f none usr/lib/fs/tmpfs/mount 555 root bin
d none usr/lib/fs/ufs 755 root sys
f none usr/lib/fs/ufs/clri 555 root bin
l none usr/lib/fs/ufs/dcopy=../../../../usr/lib/fs/ufs/clri
f none usr/lib/fs/ufs/df 555 root bin
f none usr/lib/fs/ufs/edquota 555 root bin
f none usr/lib/fs/ufs/ff 555 root bin
f none usr/lib/fs/ufs/fsck 555 root bin
f none usr/lib/fs/ufs/fsckall 555 root bin
f none usr/lib/fs/ufs/fsdb 555 root bin
f none usr/lib/fs/ufs/fsirand 555 root bin
f none usr/lib/fs/ufs/fssnap 555 root bin
f none usr/lib/fs/ufs/fstyp.so.1 555 root bin
l none usr/lib/fs/ufs/fstyp=../../../sbin/fstyp
f none usr/lib/fs/ufs/labelit 555 root bin
f none usr/lib/fs/ufs/lockfs 555 root bin
f none usr/lib/fs/ufs/mkfs 555 root bin
s none usr/lib/fs/ufs/mount=../../../../etc/fs/ufs/mount
f none usr/lib/fs/ufs/ncheck 555 root bin
f none usr/lib/fs/ufs/newfs 555 root bin
f none usr/lib/fs/ufs/quot 555 root bin
f none usr/lib/fs/ufs/quota 4555 root bin
f none usr/lib/fs/ufs/quotacheck 555 root bin
f none usr/lib/fs/ufs/quotaoff 555 root bin
l none usr/lib/fs/ufs/quotaon=../../../../usr/lib/fs/ufs/quotaoff
f none usr/lib/fs/ufs/repquota 555 root bin
f none usr/lib/fs/ufs/tunefs 555 root bin
f none usr/lib/fs/ufs/ufsdump 4555 root bin
f none usr/lib/fs/ufs/ufsrestore 4555 root bin
f none usr/lib/fs/ufs/volcopy 555 root bin
f none usr/lib/getoptcvt 555 root bin
d none usr/lib/help 755 root bin
d none usr/lib/help/auths 755 root bin
d none usr/lib/help/auths/locale 755 root bin
d none usr/lib/help/auths/locale/C 755 root bin
f none usr/lib/help/auths/locale/C/AllSolAuthsHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/AuditConfig.html 444 root bin
f none usr/lib/help/auths/locale/C/AuditHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/AuditRead.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthJobsAdmin.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthJobsUser.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthProfmgrAssign.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthProfmgrDelegate.html 444 root bin
```



```
f none usr/lib/help/auths/locale/C/AuthProfmgrExecattrWrite.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthProfmgrRead.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthProfmgrWrite.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthRoleAssign.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthRoleDelegate.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthRoleWrite.html 444 root bin
f none usr/lib/help/auths/locale/C/BindStates.html 444 root bin
f none usr/lib/help/auths/locale/C/DevAllocHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/DevAllocate.html 444 root bin
f none usr/lib/help/auths/locale/C/DevConfig.html 444 root bin
f none usr/lib/help/auths/locale/C/DevGrant.html 444 root bin
f none usr/lib/help/auths/locale/C/DevRevoke.html 444 root bin
f none usr/lib/help/auths/locale/C/DhcpmgrHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/DhcpmgrWrite.html 444 root bin
f none usr/lib/help/auths/locale/C/JobHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/JobsGrant.html 444 root bin
f none usr/lib/help/auths/locale/C/LoginEnable.html 444 root bin
f none usr/lib/help/auths/locale/C/LoginHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/LoginRemote.html 444 root bin
f none usr/lib/help/auths/locale/C/NetworkHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/PriAdmin.html 444 root bin
f none usr/lib/help/auths/locale/C/ProfmgrHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/RoleHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfAutofsStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfCronStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfManageHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfMDNSStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfModifyAppl.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfModifyDepend.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfModifyFramework.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfModifyHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfModifyMethod.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfInetdStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfIPsecStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfNscdStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfNADDStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfNWAMStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfPowerStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfRoutingStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfSendmailStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfSMBFSStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfSMBStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfSshStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfSyslogStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueInetd.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueIPsec.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueIscsitgt.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueMDNS.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueNADD.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueNDMP.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfNDMPStates.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthReadNDMP.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueNWAM.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueRouting.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueSMB.html 444 root bin
f none usr/lib/help/auths/locale/C/AuthReadSMB.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfWpaStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SysDate.html 444 root bin
f none usr/lib/help/auths/locale/C/SysHeader.html 444 root bin
f none usr/lib/help/auths/locale/C/SysShutdown.html 444 root bin
f none usr/lib/help/auths/locale/C/WifiConfig.html 444 root bin
f none usr/lib/help/auths/locale/C/WifiWep.html 444 root bin
f none usr/lib/help/auths/locale/C/LinkSecurity.html 444 root bin
f none usr/lib/help/auths/locale/C/IdmapRules.html 444 root bin
```

```
f none usr/lib/help/auths/locale/C/SmfIdmapStates.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueIdmap.html 444 root bin
f none usr/lib/help/auths/locale/C/SmfValueVscan.html 0444 root bin
f none usr/lib/help/auths/locale/C/SmfVscanStates.html 0444 root bin
d none usr/lib/help/profiles 755 root bin
d none usr/lib/help/profiles/locale 755 root bin
d none usr/lib/help/profiles/locale/C 755 root bin
f none usr/lib/help/profiles/locale/C/RtAll.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtAuditCtrl.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtAuditReview.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtConsUser.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtContractObserver.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtCronMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtCryptoMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtDHCPMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtDatAdmin.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtDefault.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtDeviceMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtDeviceSecurity.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtFTPMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtFileSysMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtFileSysSecurity.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtInetdMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtIPFilterMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtKerberosClntMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtKerberosSrvrMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtLogMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtMailMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtMaintAndRepair.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNDMPMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtMediaBkup.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtMediaRestore.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNameServiceAdmin.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNameServiceSecure.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetIPsec.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetSecure.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetWifiMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetWifiSecure.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtNetLinkSecure.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtObAccessMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtPrntAdmin.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtProcManagement.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtRightsDelegate.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtSoftwareInstall.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtSMBFSMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtSMBMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtSysEvMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtUserMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtUserSecurity.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtZFSFileSysMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtZFSStorageMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtZoneMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtIdmapMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtIdmapNameRulesMngmnt.html 444 root bin
f none usr/lib/help/profiles/locale/C/RtVscanMngmnt.html 444 root bin
d none usr/lib/iconv 755 root bin
f none usr/lib/iconv/646da.8859.t 444 root bin
f none usr/lib/iconv/646de.8859.t 444 root bin
f none usr/lib/iconv/646en.8859.t 444 root bin
f none usr/lib/iconv/646es.8859.t 444 root bin
f none usr/lib/iconv/646fr.8859.t 444 root bin
f none usr/lib/iconv/646it.8859.t 444 root bin
f none usr/lib/iconv/646sv.8859.t 444 root bin
f none usr/lib/iconv/8859.646.t 444 root bin
f none usr/lib/iconv/8859.646da.t 444 root bin
```



```
f none usr/lib/iconv/8859.646de.t 444 root bin
f none usr/lib/iconv/8859.646en.t 444 root bin
f none usr/lib/iconv/8859.646es.t 444 root bin
f none usr/lib/iconv/8859.646fr.t 444 root bin
f none usr/lib/iconv/8859.646it.t 444 root bin
f none usr/lib/iconv/8859.646sv.t 444 root bin
f none usr/lib/iconv/iconv_data 444 root bin
f none usr/lib/idmapd 555 root bin
d none usr/lib/inet 755 root bin
f none usr/lib/inet/certdb 555 root bin
f none usr/lib/inet/certlocal 555 root bin
f none usr/lib/inet/certrldb 555 root bin
d none usr/lib/inet/dhcp 755 root bin
d none usr/lib/inet/dhcp/nsu 755 root bin
d none usr/lib/inet/dhcp/svc 755 root bin
f none usr/lib/inet/in.iked 555 root bin
f none usr/lib/inet/in.mpathd 555 root bin
f none usr/lib/inet/inetd 555 root bin
f none usr/lib/intrd 555 root bin
f none usr/lib/isaexec 555 root bin
f none usr/lib/kssladm 555 root bin
s none usr/lib/ld.so.1=../../lib/ld.so.1
d none usr/lib/locale 755 root bin
d none usr/lib/locale/C 755 root bin
d none usr/lib/locale/C/LC_COLLATE 755 root bin
d none usr/lib/locale/C/LC_CTYPE 755 root bin
d none usr/lib/locale/C/LC_MESSAGES 755 root bin
d none usr/lib/locale/C/LC_MONETARY 755 root bin
d none usr/lib/locale/C/LC_NUMERIC 755 root bin
d none usr/lib/locale/C/LC_TIME 755 root bin
f none usr/lib/locale/C/locale_description 444 root bin
s none usr/lib/locale/POSIX=./C
d none usr/lib/localedef 755 root bin
d none usr/lib/localedef/extensions 755 root bin
f none usr/lib/localedef/extensions/generic_eucbc.x 444 root bin
f none usr/lib/localedef/extensions/single_byte.x 444 root bin
d none usr/lib/localedef/src 755 root bin
f none usr/lib/makekey 555 root bin
f none usr/lib/more.help 644 root bin
d none usr/lib/netsvc 755 root sys
f none usr/lib/newsyslog 555 root sys
f none usr/lib/nscd_nischeck 555 root bin
d none usr/lib/pci 755 root bin
f none usr/lib/pci/pcidr 555 root bin
f none usr/lib/pci/pcidr_plugin.so 755 root bin
f none usr/lib/platexec 555 root bin
d none usr/lib/rcm 755 root bin
d none usr/lib/rcm/modules 755 root bin
f none usr/lib/rcm/modules/SUNW_cluster_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_dump_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_filesys_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_ip_anon_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_ip_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_mpxio_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_network_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_vlan_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_aggr_rcm.so 555 root bin
f none usr/lib/rcm/modules/SUNW_swap_rcm.so 555 root bin
f none usr/lib/rcm/rcm_daemon 555 root bin
d none usr/lib/rcm/scripts 755 root bin
s none usr/lib/rsh=../../sbin/sh
d none usr/lib/saf 755 root bin
f none usr/lib/saf/listen 755 root sys
f none usr/lib/saf/nlps_server 755 root sys
f none usr/lib/saf/sac 555 root sys
f none usr/lib/saf/ttymon 555 root sys
```

```
653 d none usr/lib/secure 755 root bin
654 s none usr/lib/secure/32=.
655 d none usr/lib/security 755 root bin
656 d none usr/lib/sysevent 755 root bin
657 d none usr/lib/sysevent/modules 755 root bin
658 f none usr/lib/sysevent/modules/devfsadmd_mod.so 755 root bin
659 f none usr/lib/sysevent/modules/sysevent_conf_mod.so 755 root bin
660 f none usr/lib/sysevent/modules/sysevent_reg_mod.so 755 root bin
661 f none usr/lib/sysevent/syseventconfd 555 root bin
662 f none usr/lib/sysevent/syseventd 555 root bin
663 f none usr/lib/t300 555 root bin
664 f none usr/lib/t300s 555 root bin
665 f none usr/lib/t4014 555 root bin
666 f none usr/lib/t450 555 root bin
667 d none usr/lib/term 755 root bin
668 f none usr/lib/utmp_update 4555 root bin
669 f none usr/lib/utmpd 555 root bin
670 f none usr/lib/vna 555 root bin
671 f none usr/lib/vplot 555 root bin
672 s none usr/mail=../var/mail
673 d none usr/net 755 root sys
674 d none usr/net/nls 755 root sys
675 s none usr/net/nls/listen=../../lib/saf/listen
676 s none usr/net/nls/nlps_server=../../lib/saf/nlps_server
677 d none usr/net/servers 755 root sys
678 s none usr/news=../var/news
679 d none usr/old 755 root bin
680 d none usr/openwin 755 root bin
681 d none usr/platform 755 root sys
682 s none usr/preserve=../var/preserve
683 s none usr/pub=./share/lib/pub
684 d none usr/sadm 755 root bin
685 d none usr/sadm/bin 755 root bin
686 l none usr/sadm/bin/dispgid=../../../usr/bin/ckgid
687 l none usr/sadm/bin/dispuid=../../../usr/bin/ckuid
688 l none usr/sadm/bin/errange=../../../usr/bin/ckrange
689 l none usr/sadm/bin/errdate=../../../usr/bin/ckdate
690 l none usr/sadm/bin/errgid=../../../usr/bin/ckgid
691 l none usr/sadm/bin/errint=../../../usr/bin/ckint
692 l none usr/sadm/bin/erritem=../../../usr/bin/ckitem
693 l none usr/sadm/bin/errpath=../../../usr/bin/ckpath
694 l none usr/sadm/bin/errstr=../../../usr/bin/ckstr
695 l none usr/sadm/bin/errtime=../../../usr/bin/cktime
696 l none usr/sadm/bin/erruid=../../../usr/bin/ckuid
697 l none usr/sadm/bin/erryorn=../../../usr/bin/ckyorn
698 l none usr/sadm/bin/helpdate=../../../usr/bin/ckdate
699 l none usr/sadm/bin/helpgid=../../../usr/bin/ckgid
700 l none usr/sadm/bin/helpint=../../../usr/bin/ckint
701 l none usr/sadm/bin/helpitem=../../../usr/bin/ckitem
702 l none usr/sadm/bin/helppath=../../../usr/bin/ckpath
703 l none usr/sadm/bin/helprange=../../../usr/bin/ckrange
704 l none usr/sadm/bin/helpstr=../../../usr/bin/ckstr
705 l none usr/sadm/bin/helptime=../../../usr/bin/cktime
706 l none usr/sadm/bin/helpuid=../../../usr/bin/ckuid
707 l none usr/sadm/bin/helpyorn=../../../usr/bin/ckyorn
708 f none usr/sadm/bin/puttext 555 root bin
709 l none usr/sadm/bin/valdate=../../../usr/bin/ckdate
710 l none usr/sadm/bin/valgid=../../../usr/bin/ckgid
711 l none usr/sadm/bin/valint=../../../usr/bin/ckint
712 l none usr/sadm/bin/valpath=../../../usr/bin/ckpath
713 l none usr/sadm/bin/valrange=../../../usr/bin/ckrange
714 l none usr/sadm/bin/valstr=../../../usr/bin/ckstr
715 l none usr/sadm/bin/valtime=../../../usr/bin/cktime
716 l none usr/sadm/bin/valuid=../../../usr/bin/ckuid
717 l none usr/sadm/bin/valyorn=../../../usr/bin/ckyorn
718 d none usr/sadm/install 755 root bin
```



```
719 f none usr/sadm/install/miniroot.db 444 root sys
720 d none usr/sadm/install/scripts 755 root bin
721 f none usr/sadm/install/scripts/i.ipsecalgs 555 root sys
722 f none usr/sadm/install/scripts/i.kcfconf 555 root sys
723 f none usr/sadm/install/scripts/i.kmfconf 555 root sys
724 f none usr/sadm/install/scripts/i.manifest 555 root sys
725 f none usr/sadm/install/scripts/i.pkcs11conf 555 root sys
726 f none usr/sadm/install/scripts/i.rbac 555 root sys
727 f none usr/sadm/install/scripts/r.ipsecalgs 555 root sys
728 f none usr/sadm/install/scripts/r.kcfconf 555 root sys
729 f none usr/sadm/install/scripts/r.kmfconf 555 root sys
730 f none usr/sadm/install/scripts/r.manifest 555 root sys
731 f none usr/sadm/install/scripts/r.pkcs11conf 555 root sys
732 f none usr/sadm/install/scripts/r.rbac 555 root sys
733 d none usr/sadm/sysadm 755 root bin
734 d none usr/sadm/sysadm/add-ons 755 root bin
735 d none usr/sadm/sysadm/bin 755 root bin
736 f none usr/sadm/sysadm/bin/mkdtab 755 root bin
737 f none usr/sadm/ugdates 444 root bin
738 d none usr/sbin 755 root bin
739 f none usr/sbin/6to4relay 555 root bin
740 f none usr/sbin/acctadm 555 root bin
741 l none usr/sbin/add_drv=../../usr/lib/isaexec
742 f none usr/sbin/allocate 4555 root bin
743 f none usr/sbin/arp 555 root bin
744 f none usr/sbin/audit 555 root bin
745 f none usr/sbin/auditconfig 555 root bin
746 f none usr/sbin/auditd 555 root bin
747 f none usr/sbin/auditreduce 555 root bin
748 f none usr/sbin/auditstat 555 root bin
749 l none usr/sbin/audlinks=./devfsadm
750 s none usr/sbin/autopush=../../sbin/autopush
751 s none usr/sbin/bootadm=../../sbin/bootadm
752 f none usr/sbin/bsmrecord 555 root bin
753 s none usr/sbin/cachefslog=../lib/fs/cachefs/cachefslog
754 s none usr/sbin/cachefswssize=../lib/fs/cachefs/cachefswssize
755 f none usr/sbin/cfgadm 555 root bin
756 s none usr/sbin/cfsadmin=../lib/fs/cachefs/cfsadmin
757 f none usr/sbin/chroot 555 root bin
758 f none usr/sbin/clear_locks 555 root bin
759 f none usr/sbin/clinfo 555 root bin
760 f none usr/sbin/clri 555 root bin
761 f none usr/sbin/consadm 555 root sys
762 l none usr/sbin/consadmd=../../usr/sbin/consadm
763 f none usr/sbin/cron 555 root sys
764 f none usr/sbin/cryptoadm 555 root bin
765 s none usr/sbin/dcopy=./clri
766 l none usr/sbin/deallocate=../../usr/sbin/allocate
767 f none usr/sbin/devfsadm 755 root sys
768 f none usr/sbin/devinfo 555 root bin
769 l none usr/sbin/devlinks=./devfsadm
770 s none usr/sbin/devnm=./df
771 f none usr/sbin/df 555 root bin
772 f none usr/sbin/dfmounts 555 root bin
773 l none usr/sbin/dfshares=../../usr/sbin/dfmounts
774 l none usr/sbin/disks=./devfsadm
775 f none usr/sbin/dispadmin 555 root bin
776 s none usr/sbin/dladm=../../sbin/dladm
777 f none usr/sbin/dminfo 555 root bin
778 l none usr/sbin/drvconfig=./devfsadm
779 f none usr/sbin/dumpadm 555 root bin
780 s none usr/sbin/edquota=../lib/fs/ufs/edquota
781 f none usr/sbin/eeprom 2555 root sys
782 s none usr/sbin/fdisk=../../sbin/fdisk
783 f none usr/sbin/ff 555 root bin
784 f none usr/sbin/fmthard 555 root sys
```

```
f none usr/sbin/format 555 root bin
f none usr/sbin/fsck 555 root bin
s none usr/sbin/fsdb=./clri
s none usr/sbin/fsirand=../lib/fs/ufs/fsirand
s none usr/sbin/fssnap=./clri
f none usr/sbin/fstyp 555 root sys
f none usr/sbin/fuser 555 root bin
f none usr/sbin/getdevpolicy 555 root sys
f none usr/sbin/getmajor 755 root sys
f none usr/sbin/groupadd 555 root sys
f none usr/sbin/groupdel 555 root sys
f none usr/sbin/groupmod 555 root sys
f none usr/sbin/grpck 555 root bin
f none usr/sbin/halt 755 root bin
s none usr/sbin/hostconfig=../../sbin/hostconfig
f none usr/sbin/idmap 555 root bin
f none usr/sbin/if_mpadm 555 root bin
s none usr/sbin/ifconfig=../../sbin/ifconfig
f none usr/sbin/ikeadm 555 root bin
f none usr/sbin/ikecert 555 root bin
f none usr/sbin/inetadm 555 root bin
f none usr/sbin/inetconv 555 root bin
s none usr/sbin/inetd=../lib/inet/inetd
s none usr/sbin/init=../../sbin/init
f none usr/sbin/install 555 root bin
f none usr/sbin/installboot 555 root sys
f none usr/sbin/ipaddrsel 555 root bin
f none usr/sbin/ipsecalgs 555 root bin
f none usr/sbin/ipsecconf 555 root bin
f none usr/sbin/ipseckey 555 root bin
f none usr/sbin/keyserv 555 root sys
f none usr/sbin/killall 555 root bin
f none usr/sbin/ksslcfg 555 root bin
s none usr/sbin/labelit=./clri
f none usr/sbin/link 555 root bin
l none usr/sbin/list_devices=../../usr/sbin/allocate
f none usr/sbin/locator 555 root bin
s none usr/sbin/lockfs=../lib/fs/ufs/lockfs
f none usr/sbin/lofiadm 555 root bin
f none usr/sbin/logadm 555 root bin
f none usr/sbin/makedbm 555 root bin
f none usr/sbin/mkdevalloc 555 root bin
l none usr/sbin/mkdevmaps=../../usr/sbin/mkdevalloc
f none usr/sbin/mkfile 555 root bin
s none usr/sbin/mkfs=./clri
f none usr/sbin/mknod 555 root bin
l none usr/sbin/modinfo=../../usr/lib/isaexec
l none usr/sbin/modload=../../usr/lib/isaexec
l none usr/sbin/modunload=../../usr/lib/isaexec
s none usr/sbin/mount=../../sbin/mount
f none usr/sbin/mountall 555 root sys
f none usr/sbin/msgid 555 root bin
f none usr/sbin/mvdir 555 root bin
s none usr/sbin/ncheck=./ff
f none usr/sbin/ndd 555 root bin
f none usr/sbin/netservices 0555 root sys
s none usr/sbin/newfs=../lib/fs/ufs/newfs
f none usr/sbin/nlsadmin 755 root adm
f none usr/sbin/nscd 555 root bin
f none usr/sbin/passmgmt 555 root sys
l none usr/sbin/pbind=../../usr/lib/isaexec
f none usr/sbin/pmadm 555 root sys
l none usr/sbin/ports=./devfsadm
l none usr/sbin/poweroff=./halt
f none usr/sbin/praudit 555 root bin
l none usr/sbin/prtconf=../../usr/lib/isaexec
```



```
f none usr/sbin/prtvtoc 555 root sys
f none usr/sbin/psradm 555 root sys
f none usr/sbin/psrinfo 555 root sys
l none usr/sbin/psrset=../../usr/lib/isaexec
f none usr/sbin/pwck 555 root bin
f none usr/sbin/pwconv 555 root sys
s none usr/sbin/quot=../lib/fs/ufs/quot
s none usr/sbin/quota=../lib/fs/ufs/quota
s none usr/sbin/quotacheck=../lib/fs/ufs/quotacheck
s none usr/sbin/quotaoff=../lib/fs/ufs/quotaoff
s none usr/sbin/quotaon=../lib/fs/ufs/quotaon
f none usr/sbin/raidctl 555 root bin
f none usr/sbin/ramdiskadm 555 root bin
f none usr/sbin/rctladm 555 root bin
l none usr/sbin/reboot=./halt
l none usr/sbin/rem_drv=../../usr/lib/isaexec
s none usr/sbin/repquota=../lib/fs/ufs/repquota
l none usr/sbin/roleadd=../../usr/sbin/useradd
l none usr/sbin/roledel=../../usr/sbin/userdel
l none usr/sbin/rolemod=../../usr/sbin/usermod
f none usr/sbin/root_archive 555 root sys
s none usr/sbin/route=../../sbin/route
s none usr/sbin/routeadm=../../sbin/routeadm
f none usr/sbin/rpcbind 555 root bin
f none usr/sbin/sacadm 4755 root sys
f none usr/sbin/setmnt 555 root bin
f none usr/sbin/shareall 555 root bin
f none usr/sbin/shutdown 755 root sys
f none usr/sbin/smbios 555 root bin
f none usr/sbin/stmsboot 555 root bin
f none usr/sbin/strace 555 root sys
f none usr/sbin/strclean 555 root sys
f none usr/sbin/strerr 555 root sys
f none usr/sbin/sttydefs 755 root sys
f none usr/sbin/svcadm 0555 root bin
f none usr/sbin/svccfg 0555 root bin
l none usr/sbin/swap=../../usr/lib/isaexec
s none usr/sbin/sync=../../sbin/sync
f none usr/sbin/syncinit 555 root bin
f none usr/sbin/syncloop 555 root bin
f none usr/sbin/syncstat 555 root bin
l none usr/sbin/sysdef=../../usr/lib/isaexec
f none usr/sbin/syseventadm 555 root sys
f none usr/sbin/syslogd 555 root sys
l none usr/sbin/tapes=./devfsadm
f none usr/sbin/tar 555 root bin
f none usr/sbin/traceroute 4555 root bin
l none usr/sbin/trapstat=../../usr/lib/platexec
f none usr/sbin/ttyadm 755 root sys
s none usr/sbin/tunefs=../lib/fs/ufs/tunefs
s none usr/sbin/uadmin=../../sbin/uadmin
s none usr/sbin/ufsdump=../lib/fs/ufs/ufsdump
s none usr/sbin/ufsrestore=../lib/fs/ufs/ufsrestore
s none usr/sbin/umount=../../sbin/umount
f none usr/sbin/umountall 555 root sys
f none usr/sbin/unlink 555 root bin
f none usr/sbin/sharectl 555 root bin
f none usr/sbin/sharemgr 555 root bin
f none usr/lib/libshare.so.1 755 root bin
l none usr/sbin/share=../../usr/sbin/sharemgr
l none usr/sbin/unshare=../../usr/sbin/sharemgr
f none usr/sbin/unshareall 555 root bin
l none usr/sbin/update_drv=../../usr/lib/isaexec
f none usr/sbin/useradd 555 root sys
f none usr/sbin/userdel 555 root sys
f none usr/sbin/usermod 555 root sys
```

```
 917 f none usr/sbin/volcopy 555 root bin
 918 f none usr/sbin/wall 2555 root tty
 919 l none usr/sbin/whodo=../../usr/lib/isaexec
 920 f none usr/sbin/zdump 555 root bin
 921 f none usr/sbin/zic 555 root bin
 922 d none usr/share 755 root sys
 923 d none usr/share/lib 755 root sys
 924 d none usr/share/lib/mailx 755 root bin
 925 f none usr/share/lib/mailx/mailx.help 644 root bin
 926 f none usr/share/lib/mailx/mailx.help.~ 644 root bin
 927 d none usr/share/lib/pub 755 root bin
 928 d none usr/share/lib/tabset 755 root bin
 929 f none usr/share/lib/tabset/3101 644 root bin
 930 f none usr/share/lib/tabset/beehive 644 root bin
 931 f none usr/share/lib/tabset/hds 644 root bin
 932 f none usr/share/lib/tabset/hds3 644 root bin
 933 f none usr/share/lib/tabset/std 644 root bin
 934 f none usr/share/lib/tabset/stdcrt 644 root bin
 935 f none usr/share/lib/tabset/teleray 644 root bin
 936 f none usr/share/lib/tabset/vt100 644 root bin
 937 f none usr/share/lib/tabset/wyse-adds 644 root bin
 938 f none usr/share/lib/tabset/xerox1720 644 root bin
 939 f none usr/share/lib/termcap 644 root bin
 940 d none usr/share/lib/terminfo 755 root bin
 941 d none usr/share/lib/terminfo/3 755 root bin
 942 l none usr/share/lib/terminfo/3/386AT-M=../../../../../usr/share/lib/terminfo/a/
 943 l none usr/share/lib/terminfo/3/386AT=../../../../../usr/share/lib/terminfo/a/at
 944 l none usr/share/lib/terminfo/3/386at-m=../../../../../usr/share/lib/terminfo/a/
 945 l none usr/share/lib/terminfo/3/386at=../../../../../usr/share/lib/terminfo/a/at
 946 d none usr/share/lib/terminfo/A 755 root bin
 947 f none usr/share/lib/terminfo/A/AT386-DOS 644 root bin
 948 f none usr/share/lib/terminfo/A/AT386-DOS-M 644 root bin
 949 l none usr/share/lib/terminfo/A/AT386-M=../../../../../usr/share/lib/terminfo/a/
 950 l none usr/share/lib/terminfo/A/AT386=../../../../../usr/share/lib/terminfo/a/at
 951 d none usr/share/lib/terminfo/a 755 root bin
 952 f none usr/share/lib/terminfo/a/ansi 644 root bin
 953 f none usr/share/lib/terminfo/a/ansi+arrows 644 root bin
 954 f none usr/share/lib/terminfo/a/ansi+cup 644 root bin
 955 f none usr/share/lib/terminfo/a/ansi+erase 644 root bin
 956 f none usr/share/lib/terminfo/a/ansi+idc 644 root bin
 957 f none usr/share/lib/terminfo/a/ansi+idl 644 root bin
 958 f none usr/share/lib/terminfo/a/ansi+idl1 644 root bin
 959 f none usr/share/lib/terminfo/a/ansi+inittabs 644 root bin
 960 f none usr/share/lib/terminfo/a/ansi+local 644 root bin
 961 f none usr/share/lib/terminfo/a/ansi+local1 644 root bin
 962 f none usr/share/lib/terminfo/a/ansi+pp 644 root bin
 963 f none usr/share/lib/terminfo/a/ansi+rca 644 root bin
 964 f none usr/share/lib/terminfo/a/ansi+rep 644 root bin
 965 f none usr/share/lib/terminfo/a/ansi+sgr 644 root bin
 966 f none usr/share/lib/terminfo/a/ansi+sgrbold 644 root bin
 967 f none usr/share/lib/terminfo/a/ansi+sgrdim 644 root bin
 968 f none usr/share/lib/terminfo/a/ansi+sgrso 644 root bin
 969 f none usr/share/lib/terminfo/a/ansi+sgrul 644 root bin
 970 f none usr/share/lib/terminfo/a/ansi+tabs 644 root bin
 971 f none usr/share/lib/terminfo/a/at386 644 root bin
 972 f none usr/share/lib/terminfo/a/at386-m 644 root bin
 973 d none usr/share/lib/terminfo/s 755 root bin
 974 f none usr/share/lib/terminfo/s/screen 644 root bin
 975 f none usr/share/lib/terminfo/s/screen-w 644 root bin
 976 f none usr/share/lib/terminfo/s/sun 644 root bin
 977 f none usr/share/lib/terminfo/s/sun-1 644 root bin
 978 f none usr/share/lib/terminfo/s/sun-12 644 root bin
 979 f none usr/share/lib/terminfo/s/sun-17 644 root bin
 980 f none usr/share/lib/terminfo/s/sun-24 644 root bin
 981 f none usr/share/lib/terminfo/s/sun-34 644 root bin
 982 f none usr/share/lib/terminfo/s/sun-48 644 root bin
```



```
 983 f none usr/share/lib/terminfo/s/sun-cmd 644 root bin
 984 f none usr/share/lib/terminfo/s/sun-color 644 root bin
 985 f none usr/share/lib/terminfo/s/sun-e 644 root bin
 986 f none usr/share/lib/terminfo/s/sun-e-s 644 root bin
 987 f none usr/share/lib/terminfo/s/sun-na 644 root bin
 988 l none usr/share/lib/terminfo/s/sun-nic=../../../../../usr/share/lib/terminfo/s/
 989 f none usr/share/lib/terminfo/s/sun-s 644 root bin
 990 l none usr/share/lib/terminfo/s/sun-s-e=../../../../../usr/share/lib/terminfo/s/
 991 l none usr/share/lib/terminfo/s/sun1=../../../../../usr/share/lib/terminfo/s/sun
 992 l none usr/share/lib/terminfo/s/sun2=../../../../../usr/share/lib/terminfo/s/sun
 993 l none usr/share/lib/terminfo/s/sune=../../../../../usr/share/lib/terminfo/s/sun
 994 d none usr/share/lib/terminfo/u 755 root bin
 995 f none usr/share/lib/terminfo/u/unknown 644 root bin
 996 d none usr/share/lib/terminfo/v 755 root bin
 997 f none usr/share/lib/terminfo/v/vs100 644 root bin
 998 f none usr/share/lib/terminfo/v/vs100s 644 root bin
 999 f none usr/share/lib/terminfo/v/vt100 644 root bin
1000 l none usr/share/lib/terminfo/v/vt100-am=../../../../../usr/share/lib/terminfo/v
1001 f none usr/share/lib/terminfo/v/vt100-bot-s 644 root bin
1002 f none usr/share/lib/terminfo/v/vt100-nam 644 root bin
1003 f none usr/share/lib/terminfo/v/vt100-nam-w 644 root bin
1004 f none usr/share/lib/terminfo/v/vt100-nav 644 root bin
1005 f none usr/share/lib/terminfo/v/vt100-nav-w 644 root bin
1006 f none usr/share/lib/terminfo/v/vt100-np 644 root bin
1007 f none usr/share/lib/terminfo/v/vt100-s 644 root bin
1008 l none usr/share/lib/terminfo/v/vt100-s-bot=../../../../../usr/share/lib/terminf
1009 l none usr/share/lib/terminfo/v/vt100-s-top=../../../../../usr/share/lib/terminf
1010 l none usr/share/lib/terminfo/v/vt100-top-s=../../../../../usr/share/lib/terminf
1011 f none usr/share/lib/terminfo/v/vt100-w 644 root bin
1012 l none usr/share/lib/terminfo/v/vt100-w-am=../../../../../usr/share/lib/terminfo
1013 l none usr/share/lib/terminfo/v/vt100-w-nam=../../../../../usr/share/lib/terminf
1014 l none usr/share/lib/terminfo/v/vt100-w-nav=../../../../../usr/share/lib/terminf
1015 f none usr/share/lib/terminfo/v/vt100am 644 root bin
1016 f none usr/share/lib/terminfo/v/vt100nam 644 root bin
1017 f none usr/share/lib/terminfo/v/vt100s 644 root bin
1018 f none usr/share/lib/terminfo/v/vt100w 644 root bin
1019 f none usr/share/lib/terminfo/v/vt132 644 root bin
1020 f none usr/share/lib/terminfo/v/vt220 644 root bin
1021 d none usr/share/lib/terminfo/x 755 root bin
1022 l none usr/share/lib/terminfo/x/xterm=../../../../../usr/share/lib/terminfo/v/vs
1023 l none usr/share/lib/terminfo/x/xterm-color=../../../../../usr/share/lib/terminf
1024 f none usr/share/lib/terminfo/x/xtermc 644 root bin
1025 f none usr/share/lib/terminfo/x/xtermm 644 root bin
1026 l none usr/share/lib/terminfo/x/xterms=../../../../../usr/share/lib/terminfo/v/v
1027 f none usr/share/lib/unittab 444 root bin
1028 d none usr/share/lib/xml 755 root sys
1029 d none usr/share/lib/xml/dtd 755 root sys
1030 f none usr/share/lib/xml/dtd/adt_record.dtd.1 444 root bin
1031 f none usr/share/lib/xml/dtd/kmfpolicy.dtd 444 root bin
1032 f none usr/share/lib/xml/dtd/service_bundle.dtd.1 0444 root sys
1033 d none usr/share/lib/xml/style 755 root sys
1034 f none usr/share/lib/xml/style/adt_record.xsl.1 444 root bin
1035 d none usr/share/lib/zoneinfo 755 root bin
1036 d none usr/share/lib/zoneinfo/Africa 755 root bin
1037 f none usr/share/lib/zoneinfo/Africa/Abidjan 644 root bin
1038 f none usr/share/lib/zoneinfo/Africa/Accra 644 root bin
1039 f none usr/share/lib/zoneinfo/Africa/Addis_Ababa 644 root bin
1040 f none usr/share/lib/zoneinfo/Africa/Algiers 644 root bin
1041 f none usr/share/lib/zoneinfo/Africa/Asmara 644 root bin
1042 l none usr/share/lib/zoneinfo/Africa/Asmera=../../../../../usr/share/lib/zoneinf
1043 f none usr/share/lib/zoneinfo/Africa/Bamako 644 root bin
1044 f none usr/share/lib/zoneinfo/Africa/Bangui 644 root bin
1045 f none usr/share/lib/zoneinfo/Africa/Banjul 644 root bin
1046 f none usr/share/lib/zoneinfo/Africa/Bissau 644 root bin
1047 f none usr/share/lib/zoneinfo/Africa/Blantyre 644 root bin
1048 f none usr/share/lib/zoneinfo/Africa/Brazzaville 644 root bin
```

```
1049 f none usr/share/lib/zoneinfo/Africa/Bujumbura 644 root bin
1050 f none usr/share/lib/zoneinfo/Africa/Cairo 644 root bin
1051 f none usr/share/lib/zoneinfo/Africa/Casablanca 644 root bin
1052 f none usr/share/lib/zoneinfo/Africa/Ceuta 644 root bin
1053 f none usr/share/lib/zoneinfo/Africa/Conakry 644 root bin
1054 f none usr/share/lib/zoneinfo/Africa/Dakar 644 root bin
1055 f none usr/share/lib/zoneinfo/Africa/Dar_es_Salaam 644 root bin
1056 f none usr/share/lib/zoneinfo/Africa/Djibouti 644 root bin
1057 f none usr/share/lib/zoneinfo/Africa/Douala 644 root bin
1058 f none usr/share/lib/zoneinfo/Africa/El_Aaiun 644 root bin
1059 f none usr/share/lib/zoneinfo/Africa/Freetown 644 root bin
1060 f none usr/share/lib/zoneinfo/Africa/Gaborone 644 root bin
1061 f none usr/share/lib/zoneinfo/Africa/Harare 644 root bin
1062 f none usr/share/lib/zoneinfo/Africa/Johannesburg 644 root bin
1063 f none usr/share/lib/zoneinfo/Africa/Kampala 644 root bin
1064 f none usr/share/lib/zoneinfo/Africa/Khartoum 644 root bin
1065 f none usr/share/lib/zoneinfo/Africa/Kigali 644 root bin
1066 f none usr/share/lib/zoneinfo/Africa/Kinshasa 644 root bin
1067 f none usr/share/lib/zoneinfo/Africa/Lagos 644 root bin
1068 f none usr/share/lib/zoneinfo/Africa/Libreville 644 root bin
1069 f none usr/share/lib/zoneinfo/Africa/Lome 644 root bin
1070 f none usr/share/lib/zoneinfo/Africa/Luanda 644 root bin
1071 f none usr/share/lib/zoneinfo/Africa/Lubumbashi 644 root bin
1072 f none usr/share/lib/zoneinfo/Africa/Lusaka 644 root bin
1073 f none usr/share/lib/zoneinfo/Africa/Malabo 644 root bin
1074 f none usr/share/lib/zoneinfo/Africa/Maputo 644 root bin
1075 f none usr/share/lib/zoneinfo/Africa/Maseru 644 root bin
1076 f none usr/share/lib/zoneinfo/Africa/Mbabane 644 root bin
1077 f none usr/share/lib/zoneinfo/Africa/Mogadishu 644 root bin
1078 f none usr/share/lib/zoneinfo/Africa/Monrovia 644 root bin
1079 f none usr/share/lib/zoneinfo/Africa/Nairobi 644 root bin
1080 f none usr/share/lib/zoneinfo/Africa/Ndjamena 644 root bin
1081 f none usr/share/lib/zoneinfo/Africa/Niamey 644 root bin
1082 f none usr/share/lib/zoneinfo/Africa/Nouakchott 644 root bin
1083 f none usr/share/lib/zoneinfo/Africa/Ouagadougou 644 root bin
1084 f none usr/share/lib/zoneinfo/Africa/Porto-Novo 644 root bin
1085 f none usr/share/lib/zoneinfo/Africa/Sao_Tome 644 root bin
1086 l none usr/share/lib/zoneinfo/Africa/Timbuktu=../../../../../usr/share/lib/zonei
1087 f none usr/share/lib/zoneinfo/Africa/Tripoli 644 root bin
1088 f none usr/share/lib/zoneinfo/Africa/Tunis 644 root bin
1089 f none usr/share/lib/zoneinfo/Africa/Windhoek 644 root bin
1090 d none usr/share/lib/zoneinfo/America 755 root bin
1091 f none usr/share/lib/zoneinfo/America/Adak 644 root bin
1092 f none usr/share/lib/zoneinfo/America/Anchorage 644 root bin
1093 f none usr/share/lib/zoneinfo/America/Anguilla 644 root bin
1094 f none usr/share/lib/zoneinfo/America/Antigua 644 root bin
1095 f none usr/share/lib/zoneinfo/America/Araguaina 644 root bin
1096 d none usr/share/lib/zoneinfo/America/Argentina 755 root bin
1097 f none usr/share/lib/zoneinfo/America/Argentina/Buenos_Aires 644 root bin
1098 f none usr/share/lib/zoneinfo/America/Argentina/Catamarca 644 root bin
1099 l none usr/share/lib/zoneinfo/America/Argentina/ComodRivadavia=../../../../../..
1100 f none usr/share/lib/zoneinfo/America/Argentina/Cordoba 644 root bin
1101 f none usr/share/lib/zoneinfo/America/Argentina/Jujuy 644 root bin
1102 f none usr/share/lib/zoneinfo/America/Argentina/La_Rioja 644 root bin
1103 f none usr/share/lib/zoneinfo/America/Argentina/Mendoza 644 root bin
1104 f none usr/share/lib/zoneinfo/America/Argentina/Rio_Gallegos 644 root bin
1105 f none usr/share/lib/zoneinfo/America/Argentina/San_Juan 644 root bin
1106 f none usr/share/lib/zoneinfo/America/Argentina/Tucuman 644 root bin
1107 f none usr/share/lib/zoneinfo/America/Argentina/Ushuaia 644 root bin
1108 f none usr/share/lib/zoneinfo/America/Aruba 644 root bin
1109 f none usr/share/lib/zoneinfo/America/Asuncion 644 root bin
1110 f none usr/share/lib/zoneinfo/America/Atikokan 644 root bin
1111 l none usr/share/lib/zoneinfo/America/Atka=../../../../../usr/share/lib/zoneinfo
1112 f none usr/share/lib/zoneinfo/America/Bahia 644 root bin
1113 f none usr/share/lib/zoneinfo/America/Barbados 644 root bin
1114 f none usr/share/lib/zoneinfo/America/Belem 644 root bin
```



```
1115 f none usr/share/lib/zoneinfo/America/Belize 644 root bin
1116 f none usr/share/lib/zoneinfo/America/Blanc-Sablon 644 root bin
1117 f none usr/share/lib/zoneinfo/America/Boa_Vista 644 root bin
1118 f none usr/share/lib/zoneinfo/America/Bogota 644 root bin
1119 f none usr/share/lib/zoneinfo/America/Boise 644 root bin
1120 l none usr/share/lib/zoneinfo/America/Buenos_Aires=../../../../../usr/share/lib/
1121 f none usr/share/lib/zoneinfo/America/Cambridge_Bay 644 root bin
1122 f none usr/share/lib/zoneinfo/America/Campo_Grande 644 root bin
1123 f none usr/share/lib/zoneinfo/America/Cancun 644 root bin
1124 f none usr/share/lib/zoneinfo/America/Caracas 644 root bin
1125 l none usr/share/lib/zoneinfo/America/Catamarca=../../../../../usr/share/lib/zon
1126 f none usr/share/lib/zoneinfo/America/Cayenne 644 root bin
1127 f none usr/share/lib/zoneinfo/America/Cayman 644 root bin
1128 f none usr/share/lib/zoneinfo/America/Chicago 644 root bin
1129 f none usr/share/lib/zoneinfo/America/Chihuahua 644 root bin
1130 l none usr/share/lib/zoneinfo/America/Coral_Harbour=../../../../../usr/share/lib
1131 l none usr/share/lib/zoneinfo/America/Cordoba=../../../../../usr/share/lib/zonei
1132 f none usr/share/lib/zoneinfo/America/Costa_Rica 644 root bin
1133 f none usr/share/lib/zoneinfo/America/Cuiaba 644 root bin
1134 f none usr/share/lib/zoneinfo/America/Curacao 644 root bin
1135 f none usr/share/lib/zoneinfo/America/Danmarkshavn 644 root bin
1136 f none usr/share/lib/zoneinfo/America/Dawson 644 root bin
1137 f none usr/share/lib/zoneinfo/America/Dawson_Creek 644 root bin
1138 f none usr/share/lib/zoneinfo/America/Denver 644 root bin
1139 f none usr/share/lib/zoneinfo/America/Detroit 644 root bin
1140 f none usr/share/lib/zoneinfo/America/Dominica 644 root bin
1141 f none usr/share/lib/zoneinfo/America/Edmonton 644 root bin
1142 f none usr/share/lib/zoneinfo/America/Eirunepe 644 root bin
1143 f none usr/share/lib/zoneinfo/America/El_Salvador 644 root bin
1144 l none usr/share/lib/zoneinfo/America/Ensenada=../../../../../usr/share/lib/zone
1145 l none usr/share/lib/zoneinfo/America/Fort_Wayne=../../../../../usr/share/lib/zo
1146 f none usr/share/lib/zoneinfo/America/Fortaleza 644 root bin
1147 f none usr/share/lib/zoneinfo/America/Glace_Bay 644 root bin
1148 f none usr/share/lib/zoneinfo/America/Godthab 644 root bin
1149 f none usr/share/lib/zoneinfo/America/Goose_Bay 644 root bin
1150 f none usr/share/lib/zoneinfo/America/Grand_Turk 644 root bin
1151 f none usr/share/lib/zoneinfo/America/Grenada 644 root bin
1152 f none usr/share/lib/zoneinfo/America/Guadeloupe 644 root bin
1153 f none usr/share/lib/zoneinfo/America/Guatemala 644 root bin
1154 f none usr/share/lib/zoneinfo/America/Guayaquil 644 root bin
1155 f none usr/share/lib/zoneinfo/America/Guyana 644 root bin
1156 f none usr/share/lib/zoneinfo/America/Halifax 644 root bin
1157 f none usr/share/lib/zoneinfo/America/Havana 644 root bin
1158 f none usr/share/lib/zoneinfo/America/Hermosillo 644 root bin
1159 d none usr/share/lib/zoneinfo/America/Indiana 755 root bin
1160 f none usr/share/lib/zoneinfo/America/Indiana/Indianapolis 644 root bin
1161 f none usr/share/lib/zoneinfo/America/Indiana/Knox 644 root bin
1162 f none usr/share/lib/zoneinfo/America/Indiana/Marengo 644 root bin
1163 f none usr/share/lib/zoneinfo/America/Indiana/Petersburg 644 root bin
1164 f none usr/share/lib/zoneinfo/America/Indiana/Tell_City 644 root bin
1165 f none usr/share/lib/zoneinfo/America/Indiana/Vevay 644 root bin
1166 f none usr/share/lib/zoneinfo/America/Indiana/Vincennes 644 root bin
1167 f none usr/share/lib/zoneinfo/America/Indiana/Winamac 644 root bin
1168 l none usr/share/lib/zoneinfo/America/Indianapolis=../../../../../usr/share/lib/
1169 f none usr/share/lib/zoneinfo/America/Inuvik 644 root bin
1170 f none usr/share/lib/zoneinfo/America/Iqaluit 644 root bin
1171 f none usr/share/lib/zoneinfo/America/Jamaica 644 root bin
1172 l none usr/share/lib/zoneinfo/America/Jujuy=../../../../../usr/share/lib/zoneinf
1173 f none usr/share/lib/zoneinfo/America/Juneau 644 root bin
1174 d none usr/share/lib/zoneinfo/America/Kentucky 755 root bin
1175 f none usr/share/lib/zoneinfo/America/Kentucky/Louisville 644 root bin
1176 f none usr/share/lib/zoneinfo/America/Kentucky/Monticello 644 root bin
1177 l none usr/share/lib/zoneinfo/America/Knox_IN=../../../../../usr/share/lib/zonei
1178 f none usr/share/lib/zoneinfo/America/La_Paz 644 root bin
1179 f none usr/share/lib/zoneinfo/America/Lima 644 root bin
1180 f none usr/share/lib/zoneinfo/America/Los_Angeles 644 root bin
```

```
1181 l none usr/share/lib/zoneinfo/America/Louisville=../../../../../usr/share/lib/zo
1182 f none usr/share/lib/zoneinfo/America/Maceio 644 root bin
1183 f none usr/share/lib/zoneinfo/America/Managua 644 root bin
1184 f none usr/share/lib/zoneinfo/America/Manaus 644 root bin
1185 l none usr/share/lib/zoneinfo/America/Marigot=../../../../../usr/share/lib/zonei
1186 f none usr/share/lib/zoneinfo/America/Martinique 644 root bin
1187 f none usr/share/lib/zoneinfo/America/Mazatlan 644 root bin
1188 l none usr/share/lib/zoneinfo/America/Mendoza=../../../../../usr/share/lib/zonei
1189 f none usr/share/lib/zoneinfo/America/Menominee 644 root bin
1190 f none usr/share/lib/zoneinfo/America/Merida 644 root bin
1191 f none usr/share/lib/zoneinfo/America/Mexico_City 644 root bin
1192 f none usr/share/lib/zoneinfo/America/Miquelon 644 root bin
1193 f none usr/share/lib/zoneinfo/America/Moncton 644 root bin
1194 f none usr/share/lib/zoneinfo/America/Monterrey 644 root bin
1195 f none usr/share/lib/zoneinfo/America/Montevideo 644 root bin
1196 f none usr/share/lib/zoneinfo/America/Montreal 644 root bin
1197 f none usr/share/lib/zoneinfo/America/Montserrat 644 root bin
1198 f none usr/share/lib/zoneinfo/America/Nassau 644 root bin
1199 f none usr/share/lib/zoneinfo/America/New_York 644 root bin
1200 f none usr/share/lib/zoneinfo/America/Nipigon 644 root bin
1201 f none usr/share/lib/zoneinfo/America/Nome 644 root bin
1202 f none usr/share/lib/zoneinfo/America/Noronha 644 root bin
1203 d none usr/share/lib/zoneinfo/America/North_Dakota 755 root bin
1204 f none usr/share/lib/zoneinfo/America/North_Dakota/Center 644 root bin
1205 f none usr/share/lib/zoneinfo/America/North_Dakota/New_Salem 644 root bin
1206 f none usr/share/lib/zoneinfo/America/Panama 644 root bin
1207 f none usr/share/lib/zoneinfo/America/Pangnirtung 644 root bin
1208 f none usr/share/lib/zoneinfo/America/Paramaribo 644 root bin
1209 f none usr/share/lib/zoneinfo/America/Phoenix 644 root bin
1210 f none usr/share/lib/zoneinfo/America/Port-au-Prince 644 root bin
1211 f none usr/share/lib/zoneinfo/America/Port_of_Spain 644 root bin
1212 l none usr/share/lib/zoneinfo/America/Porto_Acre=../../../../../usr/share/lib/zo
1213 f none usr/share/lib/zoneinfo/America/Porto_Velho 644 root bin
1214 f none usr/share/lib/zoneinfo/America/Puerto_Rico 644 root bin
1215 f none usr/share/lib/zoneinfo/America/Rainy_River 644 root bin
1216 f none usr/share/lib/zoneinfo/America/Rankin_Inlet 644 root bin
1217 f none usr/share/lib/zoneinfo/America/Recife 644 root bin
1218 f none usr/share/lib/zoneinfo/America/Regina 644 root bin
1219 f none usr/share/lib/zoneinfo/America/Resolute 644 root bin
1220 f none usr/share/lib/zoneinfo/America/Rio_Branco 644 root bin
1221 l none usr/share/lib/zoneinfo/America/Rosario=../../../../../usr/share/lib/zonei
1222 f none usr/share/lib/zoneinfo/America/Santiago 644 root bin
1223 f none usr/share/lib/zoneinfo/America/Santo_Domingo 644 root bin
1224 f none usr/share/lib/zoneinfo/America/Sao_Paulo 644 root bin
1225 f none usr/share/lib/zoneinfo/America/Scoresbysund 644 root bin
1226 l none usr/share/lib/zoneinfo/America/Shiprock=../../../../../usr/share/lib/zone
1227 l none usr/share/lib/zoneinfo/America/St_Barthelemy=../../../../../usr/share/lib
1228 f none usr/share/lib/zoneinfo/America/St_Johns 644 root bin
1229 f none usr/share/lib/zoneinfo/America/St_Kitts 644 root bin
1230 f none usr/share/lib/zoneinfo/America/St_Lucia 644 root bin
1231 f none usr/share/lib/zoneinfo/America/St_Thomas 644 root bin
1232 f none usr/share/lib/zoneinfo/America/St_Vincent 644 root bin
1233 f none usr/share/lib/zoneinfo/America/Swift_Current 644 root bin
1234 f none usr/share/lib/zoneinfo/America/Tegucigalpa 644 root bin
1235 f none usr/share/lib/zoneinfo/America/Thule 644 root bin
1236 f none usr/share/lib/zoneinfo/America/Thunder_Bay 644 root bin
1237 f none usr/share/lib/zoneinfo/America/Tijuana 644 root bin
1238 f none usr/share/lib/zoneinfo/America/Toronto 644 root bin
1239 f none usr/share/lib/zoneinfo/America/Tortola 644 root bin
1240 f none usr/share/lib/zoneinfo/America/Vancouver 644 root bin
1241 l none usr/share/lib/zoneinfo/America/Virgin=../../../../../usr/share/lib/zonein
1242 f none usr/share/lib/zoneinfo/America/Whitehorse 644 root bin
1243 f none usr/share/lib/zoneinfo/America/Winnipeg 644 root bin
1244 f none usr/share/lib/zoneinfo/America/Yakutat 644 root bin
1245 f none usr/share/lib/zoneinfo/America/Yellowknife 644 root bin
1246 d none usr/share/lib/zoneinfo/Antarctica 755 root bin
```



```
1247 f none usr/share/lib/zoneinfo/Antarctica/Casey 644 root bin
1248 f none usr/share/lib/zoneinfo/Antarctica/Davis 644 root bin
1249 f none usr/share/lib/zoneinfo/Antarctica/DumontDUrville 644 root bin
1250 f none usr/share/lib/zoneinfo/Antarctica/Mawson 644 root bin
1251 f none usr/share/lib/zoneinfo/Antarctica/McMurdo 644 root bin
1252 f none usr/share/lib/zoneinfo/Antarctica/Palmer 644 root bin
1253 f none usr/share/lib/zoneinfo/Antarctica/Rothera 644 root bin
1254 l none usr/share/lib/zoneinfo/Antarctica/South_Pole=../../../../../usr/share/lib
1255 f none usr/share/lib/zoneinfo/Antarctica/Syowa 644 root bin
1256 f none usr/share/lib/zoneinfo/Antarctica/Vostok 644 root bin
1257 d none usr/share/lib/zoneinfo/Arctic 755 root bin
1258 l none usr/share/lib/zoneinfo/Arctic/Longyearbyen=../../../../../usr/share/lib/z
1259 d none usr/share/lib/zoneinfo/Asia 755 root bin
1260 f none usr/share/lib/zoneinfo/Asia/Aden 644 root bin
1261 f none usr/share/lib/zoneinfo/Asia/Almaty 644 root bin
1262 f none usr/share/lib/zoneinfo/Asia/Amman 644 root bin
1263 f none usr/share/lib/zoneinfo/Asia/Anadyr 644 root bin
1264 f none usr/share/lib/zoneinfo/Asia/Aqtau 644 root bin
1265 f none usr/share/lib/zoneinfo/Asia/Aqtobe 644 root bin
1266 f none usr/share/lib/zoneinfo/Asia/Ashgabat 644 root bin
1267 l none usr/share/lib/zoneinfo/Asia/Ashkhabad=../../../../../usr/share/lib/zonein
1268 f none usr/share/lib/zoneinfo/Asia/Baghdad 644 root bin
1269 f none usr/share/lib/zoneinfo/Asia/Bahrain 644 root bin
1270 f none usr/share/lib/zoneinfo/Asia/Baku 644 root bin
1271 f none usr/share/lib/zoneinfo/Asia/Bangkok 644 root bin
1272 f none usr/share/lib/zoneinfo/Asia/Beirut 644 root bin
1273 f none usr/share/lib/zoneinfo/Asia/Bishkek 644 root bin
1274 f none usr/share/lib/zoneinfo/Asia/Brunei 644 root bin
1275 f none usr/share/lib/zoneinfo/Asia/Calcutta 644 root bin
1276 f none usr/share/lib/zoneinfo/Asia/Choibalsan 644 root bin
1277 f none usr/share/lib/zoneinfo/Asia/Chongqing 644 root bin
1278 l none usr/share/lib/zoneinfo/Asia/Chungking=../../../../../usr/share/lib/zonein
1279 f none usr/share/lib/zoneinfo/Asia/Colombo 644 root bin
1280 l none usr/share/lib/zoneinfo/Asia/Dacca=../../../../../usr/share/lib/zoneinfo/A
1281 f none usr/share/lib/zoneinfo/Asia/Damascus 644 root bin
1282 f none usr/share/lib/zoneinfo/Asia/Dhaka 644 root bin
1283 f none usr/share/lib/zoneinfo/Asia/Dili 644 root bin
1284 f none usr/share/lib/zoneinfo/Asia/Dubai 644 root bin
1285 f none usr/share/lib/zoneinfo/Asia/Dushanbe 644 root bin
1286 f none usr/share/lib/zoneinfo/Asia/Gaza 644 root bin
1287 f none usr/share/lib/zoneinfo/Asia/Harbin 644 root bin
1288 f none usr/share/lib/zoneinfo/Asia/Hong_Kong 644 root bin
1289 f none usr/share/lib/zoneinfo/Asia/Hovd 644 root bin
1290 f none usr/share/lib/zoneinfo/Asia/Irkutsk 644 root bin
1291 l none usr/share/lib/zoneinfo/Asia/Istanbul=../../../../../usr/share/lib/zoneinf
1292 f none usr/share/lib/zoneinfo/Asia/Jakarta 644 root bin
1293 f none usr/share/lib/zoneinfo/Asia/Jayapura 644 root bin
1294 f none usr/share/lib/zoneinfo/Asia/Jerusalem 644 root bin
1295 f none usr/share/lib/zoneinfo/Asia/Kabul 644 root bin
1296 f none usr/share/lib/zoneinfo/Asia/Kamchatka 644 root bin
1297 f none usr/share/lib/zoneinfo/Asia/Karachi 644 root bin
1298 f none usr/share/lib/zoneinfo/Asia/Kashgar 644 root bin
1299 f none usr/share/lib/zoneinfo/Asia/Katmandu 644 root bin
1300 f none usr/share/lib/zoneinfo/Asia/Krasnoyarsk 644 root bin
1301 f none usr/share/lib/zoneinfo/Asia/Kuala_Lumpur 644 root bin
1302 f none usr/share/lib/zoneinfo/Asia/Kuching 644 root bin
1303 f none usr/share/lib/zoneinfo/Asia/Kuwait 644 root bin
1304 l none usr/share/lib/zoneinfo/Asia/Macao=../../../../../usr/share/lib/zoneinfo/A
1305 f none usr/share/lib/zoneinfo/Asia/Macau 644 root bin
1306 f none usr/share/lib/zoneinfo/Asia/Magadan 644 root bin
1307 f none usr/share/lib/zoneinfo/Asia/Makassar 644 root bin
1308 f none usr/share/lib/zoneinfo/Asia/Manila 644 root bin
1309 f none usr/share/lib/zoneinfo/Asia/Muscat 644 root bin
1310 f none usr/share/lib/zoneinfo/Asia/Nicosia 644 root bin
1311 f none usr/share/lib/zoneinfo/Asia/Novosibirsk 644 root bin
1312 f none usr/share/lib/zoneinfo/Asia/Omsk 644 root bin
```

```
1313 f none usr/share/lib/zoneinfo/Asia/Oral 644 root bin
1314 f none usr/share/lib/zoneinfo/Asia/Phnom_Penh 644 root bin
1315 f none usr/share/lib/zoneinfo/Asia/Pontianak 644 root bin
1316 f none usr/share/lib/zoneinfo/Asia/Pyongyang 644 root bin
1317 f none usr/share/lib/zoneinfo/Asia/Qatar 644 root bin
1318 f none usr/share/lib/zoneinfo/Asia/Qyzylorda 644 root bin
1319 f none usr/share/lib/zoneinfo/Asia/Rangoon 644 root bin
1320 f none usr/share/lib/zoneinfo/Asia/Riyadh 644 root bin
1321 f none usr/share/lib/zoneinfo/Asia/Riyadh87 644 root bin
1322 f none usr/share/lib/zoneinfo/Asia/Riyadh88 644 root bin
1323 f none usr/share/lib/zoneinfo/Asia/Riyadh89 644 root bin
1324 f none usr/share/lib/zoneinfo/Asia/Saigon 644 root bin
1325 f none usr/share/lib/zoneinfo/Asia/Sakhalin 644 root bin
1326 f none usr/share/lib/zoneinfo/Asia/Samarkand 644 root bin
1327 f none usr/share/lib/zoneinfo/Asia/Seoul 644 root bin
1328 f none usr/share/lib/zoneinfo/Asia/Shanghai 644 root bin
1329 f none usr/share/lib/zoneinfo/Asia/Singapore 644 root bin
1330 f none usr/share/lib/zoneinfo/Asia/Taipei 644 root bin
1331 f none usr/share/lib/zoneinfo/Asia/Tashkent 644 root bin
1332 f none usr/share/lib/zoneinfo/Asia/Tbilisi 644 root bin
1333 f none usr/share/lib/zoneinfo/Asia/Tehran 644 root bin
1334 l none usr/share/lib/zoneinfo/Asia/Tel_Aviv=../../../../../usr/share/lib/zoneinf
1335 l none usr/share/lib/zoneinfo/Asia/Thimbu=../../../../../usr/share/lib/zoneinfo/
1336 f none usr/share/lib/zoneinfo/Asia/Thimphu 644 root bin
1337 f none usr/share/lib/zoneinfo/Asia/Tokyo 644 root bin
1338 l none usr/share/lib/zoneinfo/Asia/Ujung_Pandang=../../../../../usr/share/lib/zo
1339 f none usr/share/lib/zoneinfo/Asia/Ulaanbaatar 644 root bin
1340 l none usr/share/lib/zoneinfo/Asia/Ulan_Bator=../../../../../usr/share/lib/zonei
1341 f none usr/share/lib/zoneinfo/Asia/Urumqi 644 root bin
1342 f none usr/share/lib/zoneinfo/Asia/Vientiane 644 root bin
1343 f none usr/share/lib/zoneinfo/Asia/Vladivostok 644 root bin
1344 f none usr/share/lib/zoneinfo/Asia/Yakutsk 644 root bin
1345 f none usr/share/lib/zoneinfo/Asia/Yekaterinburg 644 root bin
1346 f none usr/share/lib/zoneinfo/Asia/Yerevan 644 root bin
1347 d none usr/share/lib/zoneinfo/Atlantic 755 root bin
1348 f none usr/share/lib/zoneinfo/Atlantic/Azores 644 root bin
1349 f none usr/share/lib/zoneinfo/Atlantic/Bermuda 644 root bin
1350 f none usr/share/lib/zoneinfo/Atlantic/Canary 644 root bin
1351 f none usr/share/lib/zoneinfo/Atlantic/Cape_Verde 644 root bin
1352 l none usr/share/lib/zoneinfo/Atlantic/Faeroe=../../../../../usr/share/lib/zonei
1353 f none usr/share/lib/zoneinfo/Atlantic/Faroe 644 root bin
1354 l none usr/share/lib/zoneinfo/Atlantic/Jan_Mayen=../../../../../usr/share/lib/zo
1355 f none usr/share/lib/zoneinfo/Atlantic/Madeira 644 root bin
1356 f none usr/share/lib/zoneinfo/Atlantic/Reykjavik 644 root bin
1357 f none usr/share/lib/zoneinfo/Atlantic/South_Georgia 644 root bin
1358 f none usr/share/lib/zoneinfo/Atlantic/St_Helena 644 root bin
1359 f none usr/share/lib/zoneinfo/Atlantic/Stanley 644 root bin
1360 d none usr/share/lib/zoneinfo/Australia 755 root bin
1361 l none usr/share/lib/zoneinfo/Australia/ACT=../../../../../usr/share/lib/zoneinf
1362 f none usr/share/lib/zoneinfo/Australia/Adelaide 644 root bin
1363 f none usr/share/lib/zoneinfo/Australia/Brisbane 644 root bin
1364 f none usr/share/lib/zoneinfo/Australia/Broken_Hill 644 root bin
1365 l none usr/share/lib/zoneinfo/Australia/Canberra=../../../../../usr/share/lib/zo
1366 f none usr/share/lib/zoneinfo/Australia/Currie 644 root bin
1367 f none usr/share/lib/zoneinfo/Australia/Darwin 644 root bin
1368 f none usr/share/lib/zoneinfo/Australia/Eucla 644 root bin
1369 f none usr/share/lib/zoneinfo/Australia/Hobart 644 root bin
1370 l none usr/share/lib/zoneinfo/Australia/LHI=../../../../../usr/share/lib/zoneinf
1371 f none usr/share/lib/zoneinfo/Australia/Lindeman 644 root bin
1372 f none usr/share/lib/zoneinfo/Australia/Lord_Howe 644 root bin
1373 f none usr/share/lib/zoneinfo/Australia/Melbourne 644 root bin
1374 l none usr/share/lib/zoneinfo/Australia/NSW=../../../../../usr/share/lib/zoneinf
1375 l none usr/share/lib/zoneinfo/Australia/North=../../../../../usr/share/lib/zonei
1376 f none usr/share/lib/zoneinfo/Australia/Perth 644 root bin
1377 l none usr/share/lib/zoneinfo/Australia/Queensland=../../../../../usr/share/lib/
1378 l none usr/share/lib/zoneinfo/Australia/South=../../../../../usr/share/lib/zonei
```



```
1379 f none usr/share/lib/zoneinfo/Australia/Sydney 644 root bin
1380 l none usr/share/lib/zoneinfo/Australia/Tasmania=../../../../../usr/share/lib/zo
1381 l none usr/share/lib/zoneinfo/Australia/Victoria=../../../../../usr/share/lib/zo
1382 l none usr/share/lib/zoneinfo/Australia/West=../../../../../usr/share/lib/zonein
1383 l none usr/share/lib/zoneinfo/Australia/Yancowinna=../../../../../usr/share/lib/
1384 d none usr/share/lib/zoneinfo/Brazil 755 root bin
1385 l none usr/share/lib/zoneinfo/Brazil/Acre=../../../../../usr/share/lib/zoneinfo/
1386 l none usr/share/lib/zoneinfo/Brazil/DeNoronha=../../../../../usr/share/lib/zone
1387 l none usr/share/lib/zoneinfo/Brazil/East=../../../../../usr/share/lib/zoneinfo/
1388 l none usr/share/lib/zoneinfo/Brazil/West=../../../../../usr/share/lib/zoneinfo/
1389 f none usr/share/lib/zoneinfo/CET 644 root bin
1390 f none usr/share/lib/zoneinfo/CST6CDT 644 root bin
1391 d none usr/share/lib/zoneinfo/Canada 755 root bin
1392 l none usr/share/lib/zoneinfo/Canada/Atlantic=../../../../../usr/share/lib/zonei
1393 l none usr/share/lib/zoneinfo/Canada/Central=../../../../../usr/share/lib/zonein
1394 l none usr/share/lib/zoneinfo/Canada/East-Saskatchewan=../../../../../usr/share/
1395 l none usr/share/lib/zoneinfo/Canada/Eastern=../../../../../usr/share/lib/zonein
1396 l none usr/share/lib/zoneinfo/Canada/Mountain=../../../../../usr/share/lib/zonei
1397 l none usr/share/lib/zoneinfo/Canada/Newfoundland=../../../../../usr/share/lib/z
1398 l none usr/share/lib/zoneinfo/Canada/Pacific=../../../../../usr/share/lib/zonein
1399 l none usr/share/lib/zoneinfo/Canada/Saskatchewan=../../../../../usr/share/lib/z
1400 l none usr/share/lib/zoneinfo/Canada/Yukon=../../../../../usr/share/lib/zoneinfo
1401 d none usr/share/lib/zoneinfo/Chile 755 root bin
1402 l none usr/share/lib/zoneinfo/Chile/Continental=../../../../../usr/share/lib/zon
1403 l none usr/share/lib/zoneinfo/Chile/EasterIsland=../../../../../usr/share/lib/zo
1404 l none usr/share/lib/zoneinfo/Cuba=../../../../usr/share/lib/zoneinfo/America/Ha
1405 f none usr/share/lib/zoneinfo/EET 644 root bin
1406 f none usr/share/lib/zoneinfo/EST 644 root bin
1407 f none usr/share/lib/zoneinfo/EST5EDT 644 root bin
1408 l none usr/share/lib/zoneinfo/Egypt=../../../../usr/share/lib/zoneinfo/Africa/Ca
1409 l none usr/share/lib/zoneinfo/Eire=../../../../usr/share/lib/zoneinfo/Europe/Dub
1410 d none usr/share/lib/zoneinfo/Etc 755 root bin
1411 f none usr/share/lib/zoneinfo/Etc/GMT 644 root bin
1412 l none usr/share/lib/zoneinfo/Etc/GMT+0=../../../../../usr/share/lib/zoneinfo/Et
1413 f none usr/share/lib/zoneinfo/Etc/GMT+1 644 root bin
1414 f none usr/share/lib/zoneinfo/Etc/GMT+10 644 root bin
1415 f none usr/share/lib/zoneinfo/Etc/GMT+11 644 root bin
1416 f none usr/share/lib/zoneinfo/Etc/GMT+12 644 root bin
1417 f none usr/share/lib/zoneinfo/Etc/GMT+2 644 root bin
1418 f none usr/share/lib/zoneinfo/Etc/GMT+3 644 root bin
1419 f none usr/share/lib/zoneinfo/Etc/GMT+4 644 root bin
1420 f none usr/share/lib/zoneinfo/Etc/GMT+5 644 root bin
1421 f none usr/share/lib/zoneinfo/Etc/GMT+6 644 root bin
1422 f none usr/share/lib/zoneinfo/Etc/GMT+7 644 root bin
1423 f none usr/share/lib/zoneinfo/Etc/GMT+8 644 root bin
1424 f none usr/share/lib/zoneinfo/Etc/GMT+9 644 root bin
1425 l none usr/share/lib/zoneinfo/Etc/GMT-0=../../../../../usr/share/lib/zoneinfo/Et
1426 f none usr/share/lib/zoneinfo/Etc/GMT-1 644 root bin
1427 f none usr/share/lib/zoneinfo/Etc/GMT-10 644 root bin
1428 f none usr/share/lib/zoneinfo/Etc/GMT-11 644 root bin
1429 f none usr/share/lib/zoneinfo/Etc/GMT-12 644 root bin
1430 f none usr/share/lib/zoneinfo/Etc/GMT-13 644 root bin
1431 f none usr/share/lib/zoneinfo/Etc/GMT-14 644 root bin
1432 f none usr/share/lib/zoneinfo/Etc/GMT-2 644 root bin
1433 f none usr/share/lib/zoneinfo/Etc/GMT-3 644 root bin
1434 f none usr/share/lib/zoneinfo/Etc/GMT-4 644 root bin
1435 f none usr/share/lib/zoneinfo/Etc/GMT-5 644 root bin
1436 f none usr/share/lib/zoneinfo/Etc/GMT-6 644 root bin
1437 f none usr/share/lib/zoneinfo/Etc/GMT-7 644 root bin
1438 f none usr/share/lib/zoneinfo/Etc/GMT-8 644 root bin
1439 f none usr/share/lib/zoneinfo/Etc/GMT-9 644 root bin
1440 l none usr/share/lib/zoneinfo/Etc/GMT0=../../../../../usr/share/lib/zoneinfo/Etc
1441 l none usr/share/lib/zoneinfo/Etc/Greenwich=../../../../../usr/share/lib/zoneinf
1442 f none usr/share/lib/zoneinfo/Etc/UCT 644 root bin
1443 f none usr/share/lib/zoneinfo/Etc/UTC 644 root bin
1444 l none usr/share/lib/zoneinfo/Etc/Universal=../../../../../usr/share/lib/zoneinf
```

```
1445 l none usr/share/lib/zoneinfo/Etc/Zulu=../../../../../usr/share/lib/zoneinfo/Etc
1446 d none usr/share/lib/zoneinfo/Europe 755 root bin
1447 f none usr/share/lib/zoneinfo/Europe/Amsterdam 644 root bin
1448 f none usr/share/lib/zoneinfo/Europe/Andorra 644 root bin
1449 f none usr/share/lib/zoneinfo/Europe/Athens 644 root bin
1450 l none usr/share/lib/zoneinfo/Europe/Belfast=../../../../../usr/share/lib/zonein
1451 f none usr/share/lib/zoneinfo/Europe/Belgrade 644 root bin
1452 f none usr/share/lib/zoneinfo/Europe/Berlin 644 root bin
1453 l none usr/share/lib/zoneinfo/Europe/Bratislava=../../../../../usr/share/lib/zon
1454 f none usr/share/lib/zoneinfo/Europe/Brussels 644 root bin
1455 f none usr/share/lib/zoneinfo/Europe/Bucharest 644 root bin
1456 f none usr/share/lib/zoneinfo/Europe/Budapest 644 root bin
1457 f none usr/share/lib/zoneinfo/Europe/Chisinau 644 root bin
1458 f none usr/share/lib/zoneinfo/Europe/Copenhagen 644 root bin
1459 f none usr/share/lib/zoneinfo/Europe/Dublin 644 root bin
1460 f none usr/share/lib/zoneinfo/Europe/Gibraltar 644 root bin
1461 l none usr/share/lib/zoneinfo/Europe/Guernsey=../../../../../usr/share/lib/zonei
1462 f none usr/share/lib/zoneinfo/Europe/Helsinki 644 root bin
1463 l none usr/share/lib/zoneinfo/Europe/Isle_of_Man=../../../../../usr/share/lib/zo
1464 f none usr/share/lib/zoneinfo/Europe/Istanbul 644 root bin
1465 l none usr/share/lib/zoneinfo/Europe/Jersey=../../../../../usr/share/lib/zoneinf
1466 f none usr/share/lib/zoneinfo/Europe/Kaliningrad 644 root bin
1467 f none usr/share/lib/zoneinfo/Europe/Kiev 644 root bin
1468 f none usr/share/lib/zoneinfo/Europe/Lisbon 644 root bin
1469 l none usr/share/lib/zoneinfo/Europe/Ljubljana=../../../../../usr/share/lib/zone
1470 f none usr/share/lib/zoneinfo/Europe/London 644 root bin
1471 f none usr/share/lib/zoneinfo/Europe/Luxembourg 644 root bin
1472 f none usr/share/lib/zoneinfo/Europe/Madrid 644 root bin
1473 f none usr/share/lib/zoneinfo/Europe/Malta 644 root bin
1474 l none usr/share/lib/zoneinfo/Europe/Mariehamn=../../../../../usr/share/lib/zone
1475 f none usr/share/lib/zoneinfo/Europe/Minsk 644 root bin
1476 f none usr/share/lib/zoneinfo/Europe/Monaco 644 root bin
1477 f none usr/share/lib/zoneinfo/Europe/Moscow 644 root bin
1478 l none usr/share/lib/zoneinfo/Europe/Nicosia=../../../../../usr/share/lib/zonein
1479 f none usr/share/lib/zoneinfo/Europe/Oslo 644 root bin
1480 f none usr/share/lib/zoneinfo/Europe/Paris 644 root bin
1481 l none usr/share/lib/zoneinfo/Europe/Podgorica=../../../../../usr/share/lib/zone
1482 f none usr/share/lib/zoneinfo/Europe/Prague 644 root bin
1483 f none usr/share/lib/zoneinfo/Europe/Riga 644 root bin
1484 f none usr/share/lib/zoneinfo/Europe/Rome 644 root bin
1485 f none usr/share/lib/zoneinfo/Europe/Samara 644 root bin
1486 l none usr/share/lib/zoneinfo/Europe/San_Marino=../../../../../usr/share/lib/zon
1487 l none usr/share/lib/zoneinfo/Europe/Sarajevo=../../../../../usr/share/lib/zonei
1488 f none usr/share/lib/zoneinfo/Europe/Simferopol 644 root bin
1489 l none usr/share/lib/zoneinfo/Europe/Skopje=../../../../../usr/share/lib/zoneinf
1490 f none usr/share/lib/zoneinfo/Europe/Sofia 644 root bin
1491 f none usr/share/lib/zoneinfo/Europe/Stockholm 644 root bin
1492 f none usr/share/lib/zoneinfo/Europe/Tallinn 644 root bin
1493 f none usr/share/lib/zoneinfo/Europe/Tirane 644 root bin
1494 l none usr/share/lib/zoneinfo/Europe/Tiraspol=../../../../../usr/share/lib/zonei
1495 f none usr/share/lib/zoneinfo/Europe/Uzhgorod 644 root bin
1496 f none usr/share/lib/zoneinfo/Europe/Vaduz 644 root bin
1497 l none usr/share/lib/zoneinfo/Europe/Vatican=../../../../../usr/share/lib/zonein
1498 f none usr/share/lib/zoneinfo/Europe/Vienna 644 root bin
1499 f none usr/share/lib/zoneinfo/Europe/Vilnius 644 root bin
1500 f none usr/share/lib/zoneinfo/Europe/Volgograd 644 root bin
1501 f none usr/share/lib/zoneinfo/Europe/Warsaw 644 root bin
1502 l none usr/share/lib/zoneinfo/Europe/Zagreb=../../../../../usr/share/lib/zoneinf
1503 f none usr/share/lib/zoneinfo/Europe/Zaporozhye 644 root bin
1504 f none usr/share/lib/zoneinfo/Europe/Zurich 644 root bin
1505 f none usr/share/lib/zoneinfo/Factory 644 root bin
1506 l none usr/share/lib/zoneinfo/GB=../../../../usr/share/lib/zoneinfo/Europe/Londo
1507 l none usr/share/lib/zoneinfo/GB-Eire=../../../../usr/share/lib/zoneinfo/Europe/
1508 l none usr/share/lib/zoneinfo/GMT=../../../../usr/share/lib/zoneinfo/Etc/GMT
1509 l none usr/share/lib/zoneinfo/GMT+0=../../../../usr/share/lib/zoneinfo/Etc/GMT
1510 l none usr/share/lib/zoneinfo/GMT-0=../../../../usr/share/lib/zoneinfo/Etc/GMT
```



```
1511 l none usr/share/lib/zoneinfo/GMT0=../../../../usr/share/lib/zoneinfo/Etc/GMT
1512 l none usr/share/lib/zoneinfo/Greenwich=../../../../usr/share/lib/zoneinfo/Etc/G
1513 f none usr/share/lib/zoneinfo/HST 644 root bin
1514 l none usr/share/lib/zoneinfo/Hongkong=../../../../usr/share/lib/zoneinfo/Asia/H
1515 l none usr/share/lib/zoneinfo/Iceland=../../../../usr/share/lib/zoneinfo/Atlanti
1516 d none usr/share/lib/zoneinfo/Indian 755 root bin
1517 f none usr/share/lib/zoneinfo/Indian/Antananarivo 644 root bin
1518 f none usr/share/lib/zoneinfo/Indian/Chagos 644 root bin
1519 f none usr/share/lib/zoneinfo/Indian/Christmas 644 root bin
1520 f none usr/share/lib/zoneinfo/Indian/Cocos 644 root bin
1521 f none usr/share/lib/zoneinfo/Indian/Comoro 644 root bin
1522 f none usr/share/lib/zoneinfo/Indian/Kerguelen 644 root bin
1523 f none usr/share/lib/zoneinfo/Indian/Mahe 644 root bin
1524 f none usr/share/lib/zoneinfo/Indian/Maldives 644 root bin
1525 f none usr/share/lib/zoneinfo/Indian/Mauritius 644 root bin
1526 f none usr/share/lib/zoneinfo/Indian/Mayotte 644 root bin
1527 f none usr/share/lib/zoneinfo/Indian/Reunion 644 root bin
1528 l none usr/share/lib/zoneinfo/Iran=../../../../usr/share/lib/zoneinfo/Asia/Tehra
1529 l none usr/share/lib/zoneinfo/Israel=../../../../usr/share/lib/zoneinfo/Asia/Jer
1530 l none usr/share/lib/zoneinfo/Jamaica=../../../../usr/share/lib/zoneinfo/America
1531 l none usr/share/lib/zoneinfo/Japan=../../../../usr/share/lib/zoneinfo/Asia/Toky
1532 l none usr/share/lib/zoneinfo/Kwajalein=../../../../usr/share/lib/zoneinfo/Pacif
1533 l none usr/share/lib/zoneinfo/Libya=../../../../usr/share/lib/zoneinfo/Africa/Tr
1534 f none usr/share/lib/zoneinfo/MET 644 root bin
1535 f none usr/share/lib/zoneinfo/MST 644 root bin
1536 f none usr/share/lib/zoneinfo/MST7MDT 644 root bin
1537 d none usr/share/lib/zoneinfo/Mexico 755 root bin
1538 l none usr/share/lib/zoneinfo/Mexico/BajaNorte=../../../../../usr/share/lib/zone
1539 l none usr/share/lib/zoneinfo/Mexico/BajaSur=../../../../../usr/share/lib/zonein
1540 l none usr/share/lib/zoneinfo/Mexico/General=../../../../../usr/share/lib/zonein
1541 d none usr/share/lib/zoneinfo/Mideast 755 root bin
1542 l none usr/share/lib/zoneinfo/Mideast/Riyadh87=../../../../../usr/share/lib/zone
1543 l none usr/share/lib/zoneinfo/Mideast/Riyadh88=../../../../../usr/share/lib/zone
1544 l none usr/share/lib/zoneinfo/Mideast/Riyadh89=../../../../../usr/share/lib/zone
1545 l none usr/share/lib/zoneinfo/NZ=../../../../usr/share/lib/zoneinfo/Pacific/Auck
1546 l none usr/share/lib/zoneinfo/NZ-CHAT=../../../../usr/share/lib/zoneinfo/Pacific
1547 l none usr/share/lib/zoneinfo/Navajo=../../../../usr/share/lib/zoneinfo/America/
1548 l none usr/share/lib/zoneinfo/PRC=../../../../usr/share/lib/zoneinfo/Asia/Shangh
1549 f none usr/share/lib/zoneinfo/PST8PDT 644 root bin
1550 d none usr/share/lib/zoneinfo/Pacific 755 root bin
1551 f none usr/share/lib/zoneinfo/Pacific/Apia 644 root bin
1552 f none usr/share/lib/zoneinfo/Pacific/Auckland 644 root bin
1553 f none usr/share/lib/zoneinfo/Pacific/Chatham 644 root bin
1554 f none usr/share/lib/zoneinfo/Pacific/Easter 644 root bin
1555 f none usr/share/lib/zoneinfo/Pacific/Efate 644 root bin
1556 f none usr/share/lib/zoneinfo/Pacific/Enderbury 644 root bin
1557 f none usr/share/lib/zoneinfo/Pacific/Fakaofo 644 root bin
1558 f none usr/share/lib/zoneinfo/Pacific/Fiji 644 root bin
1559 f none usr/share/lib/zoneinfo/Pacific/Funafuti 644 root bin
1560 f none usr/share/lib/zoneinfo/Pacific/Galapagos 644 root bin
1561 f none usr/share/lib/zoneinfo/Pacific/Gambier 644 root bin
1562 f none usr/share/lib/zoneinfo/Pacific/Guadalcanal 644 root bin
1563 f none usr/share/lib/zoneinfo/Pacific/Guam 644 root bin
1564 f none usr/share/lib/zoneinfo/Pacific/Honolulu 644 root bin
1565 f none usr/share/lib/zoneinfo/Pacific/Johnston 644 root bin
1566 f none usr/share/lib/zoneinfo/Pacific/Kiritimati 644 root bin
1567 f none usr/share/lib/zoneinfo/Pacific/Kosrae 644 root bin
1568 f none usr/share/lib/zoneinfo/Pacific/Kwajalein 644 root bin
1569 f none usr/share/lib/zoneinfo/Pacific/Majuro 644 root bin
1570 f none usr/share/lib/zoneinfo/Pacific/Marquesas 644 root bin
1571 f none usr/share/lib/zoneinfo/Pacific/Midway 644 root bin
1572 f none usr/share/lib/zoneinfo/Pacific/Nauru 644 root bin
1573 f none usr/share/lib/zoneinfo/Pacific/Niue 644 root bin
1574 f none usr/share/lib/zoneinfo/Pacific/Norfolk 644 root bin
1575 f none usr/share/lib/zoneinfo/Pacific/Noumea 644 root bin
1576 f none usr/share/lib/zoneinfo/Pacific/Pago_Pago 644 root bin
```

```
1577 f none usr/share/lib/zoneinfo/Pacific/Palau 644 root bin
1578 f none usr/share/lib/zoneinfo/Pacific/Pitcairn 644 root bin
1579 f none usr/share/lib/zoneinfo/Pacific/Ponape 644 root bin
1580 f none usr/share/lib/zoneinfo/Pacific/Port_Moresby 644 root bin
1581 f none usr/share/lib/zoneinfo/Pacific/Rarotonga 644 root bin
1582 f none usr/share/lib/zoneinfo/Pacific/Saipan 644 root bin
1583 l none usr/share/lib/zoneinfo/Pacific/Samoa=../../../../../usr/share/lib/zoneinf
1584 f none usr/share/lib/zoneinfo/Pacific/Tahiti 644 root bin
1585 f none usr/share/lib/zoneinfo/Pacific/Tarawa 644 root bin
1586 f none usr/share/lib/zoneinfo/Pacific/Tongatapu 644 root bin
1587 f none usr/share/lib/zoneinfo/Pacific/Truk 644 root bin
1588 f none usr/share/lib/zoneinfo/Pacific/Wake 644 root bin
1589 f none usr/share/lib/zoneinfo/Pacific/Wallis 644 root bin
1590 l none usr/share/lib/zoneinfo/Pacific/Yap=../../../../../usr/share/lib/zoneinfo/
1591 l none usr/share/lib/zoneinfo/Poland=../../../../usr/share/lib/zoneinfo/Europe/W
1592 l none usr/share/lib/zoneinfo/Portugal=../../../../usr/share/lib/zoneinfo/Europe
1593 l none usr/share/lib/zoneinfo/ROK=../../../../usr/share/lib/zoneinfo/Asia/Seoul
1594 l none usr/share/lib/zoneinfo/Singapore=../../../../usr/share/lib/zoneinfo/Asia/
1595 l none usr/share/lib/zoneinfo/Turkey=../../../../usr/share/lib/zoneinfo/Europe/I
1596 l none usr/share/lib/zoneinfo/UCT=../../../../usr/share/lib/zoneinfo/Etc/UCT
1597 d none usr/share/lib/zoneinfo/US 755 root bin
1598 l none usr/share/lib/zoneinfo/US/Alaska=../../../../../usr/share/lib/zoneinfo/Am
1599 l none usr/share/lib/zoneinfo/US/Aleutian=../../../../../usr/share/lib/zoneinfo/
1600 l none usr/share/lib/zoneinfo/US/Arizona=../../../../../usr/share/lib/zoneinfo/A
1601 l none usr/share/lib/zoneinfo/US/Central=../../../../../usr/share/lib/zoneinfo/A
1602 l none usr/share/lib/zoneinfo/US/East-Indiana=../../../../../usr/share/lib/zonei
1603 l none usr/share/lib/zoneinfo/US/Eastern=../../../../../usr/share/lib/zoneinfo/A
1604 l none usr/share/lib/zoneinfo/US/Hawaii=../../../../../usr/share/lib/zoneinfo/Pa
1605 l none usr/share/lib/zoneinfo/US/Indiana-Starke=../../../../../usr/share/lib/zon
1606 l none usr/share/lib/zoneinfo/US/Michigan=../../../../../usr/share/lib/zoneinfo/
1607 l none usr/share/lib/zoneinfo/US/Mountain=../../../../../usr/share/lib/zoneinfo/
1608 l none usr/share/lib/zoneinfo/US/Pacific=../../../../../usr/share/lib/zoneinfo/A
1609 l none usr/share/lib/zoneinfo/US/Pacific-New=../../../../../usr/share/lib/zonein
1610 l none usr/share/lib/zoneinfo/US/Samoa=../../../../../usr/share/lib/zoneinfo/Pac
1611 l none usr/share/lib/zoneinfo/UTC=../../../../usr/share/lib/zoneinfo/Etc/UTC
1612 l none usr/share/lib/zoneinfo/Universal=../../../../usr/share/lib/zoneinfo/Etc/U
1613 l none usr/share/lib/zoneinfo/W-SU=../../../../usr/share/lib/zoneinfo/Europe/Mos
1614 f none usr/share/lib/zoneinfo/WET 644 root bin
1615 l none usr/share/lib/zoneinfo/Zulu=../../../../usr/share/lib/zoneinfo/Etc/UTC
1616 d none usr/share/lib/zoneinfo/src 755 root bin
1617 f none usr/share/lib/zoneinfo/src/README 644 root bin
1618 f none usr/share/lib/zoneinfo/src/africa 644 root bin
1619 f none usr/share/lib/zoneinfo/src/antarctica 644 root bin
1620 f none usr/share/lib/zoneinfo/src/asia 644 root bin
1621 f none usr/share/lib/zoneinfo/src/australasia 644 root bin
1622 f none usr/share/lib/zoneinfo/src/backward 644 root bin
1623 f none usr/share/lib/zoneinfo/src/etcetera 644 root bin
1624 f none usr/share/lib/zoneinfo/src/europe 644 root bin
1625 f none usr/share/lib/zoneinfo/src/factory 644 root bin
1626 f none usr/share/lib/zoneinfo/src/northamerica 644 root bin
1627 f none usr/share/lib/zoneinfo/src/pacificnew 644 root bin
1628 f none usr/share/lib/zoneinfo/src/solar87 644 root bin
1629 f none usr/share/lib/zoneinfo/src/solar88 644 root bin
1630 f none usr/share/lib/zoneinfo/src/solar89 644 root bin
1631 f none usr/share/lib/zoneinfo/src/southamerica 644 root bin
1632 f none usr/share/lib/zoneinfo/src/systemv 644 root bin
1633 d none usr/share/lib/zoneinfo/tab 755 root bin
1634 f none usr/share/lib/zoneinfo/tab/continent.tab 644 root bin
1635 f none usr/share/lib/zoneinfo/tab/country.tab 644 root bin
1636 f none usr/share/lib/zoneinfo/tab/zone_sun.tab 644 root bin
1637 d none usr/share/src 755 root sys
1638 s none usr/spool=../var/spool
1639 s none usr/src=./share/src
1640 s none usr/tmp=../var/tmp
1641 d none usr/xpg4 755 root bin
1642 d none usr/xpg4/bin 755 root bin
```



```
1643 f none usr/xpg4/bin/sh 555 root bin
```

```
**********************************************************
    6923 Mon Mar 24 15:32:41 2008
new/usr/src/pkgdefs/SUNWcsu/prototype_i386
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
   1 #
   2 # CDDL HEADER START
   3 #
   4 # The contents of this file are subject to the terms of the
   5 # Common Development and Distribution License (the "License").
   6 # You may not use this file except in compliance with the License.
   7 #
   8 # You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
   9 # or http://www.opensolaris.org/os/licensing.
  10 # See the License for the specific language governing permissions
  11 # and limitations under the License.
  12 #
  13 # When distributing Covered Code, include this CDDL HEADER in each
  14 # file and include the License file at usr/src/OPENSOLARIS.LICENSE.
  15 # If applicable, add the following below this CDDL HEADER, with the
  16 # fields enclosed by brackets "[]" replaced with your own identifying
  17 # information: Portions Copyright [yyyy] [name of copyright owner]
  18 #
  19 # CDDL HEADER END
  20 #
  21 #
  22 # Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
  22 # Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
  23 # Use is subject to license terms.
  24 #
  25 # ident "@(#)prototype_i386     1.92    08/03/20 SMI"
  25 # ident "@(#)prototype_i386     1.91    07/09/18 SMI"
  26 #
  27 # This required package information file contains a list of package contents.
  28 # The 'pkgmk' command uses this file to identify the contents of a package
  29 # and their location on the development machine when building the package.
  30 # Can be created via a text editor or through use of the 'pkgproto' command.

  32 #!search <pathname pathname ...>        # where to find pkg objects
  33 #!include <filename>                    # include another 'prototype' file
  34 #!default <mode> <owner> <group>        # default used if not specified on entry
  35 #!<param>=<value>                       # puts parameter in pkg environment

  37 #
  38 # Include ISA independent files (prototype_com)
  39 #
  40 !include prototype_com
  41 #
  42 #
  43 # List files which are i386 specific here
  44 #
  45 # source locations relative to the prototype file
  46 #
  47 # SUNWcsu
  48 #
  49 f none usr/bin/addbadsec 555 root bin
  50 f none usr/bin/i86/amt 555 root bin
  51 f none usr/bin/diskscan 555 root bin
  52 d none usr/bin/i86 755 root bin
  53 f none usr/bin/i86/digest 555 root bin
  54 f none usr/bin/i86/ksh93 555 root bin
  55 f none usr/bin/i86/newtask 4555 root sys
  56 f none usr/bin/i86/nohup 555 root bin
  57 l none usr/bin/i86/mac=digest
  58 f none usr/bin/i86/prctl 555 root bin
  59 f none usr/bin/i86/prstat 555 root bin
```



```
  60 f none usr/bin/i86/ps 555 root bin
  61 l none usr/bin/i86/rksh93=ksh93
  62 f none usr/bin/i86/savecore 555 root bin
  63 f none usr/bin/i86/setuname 555 root bin
  64 f none usr/bin/i86/uptime 4555 root bin
  65 l none usr/bin/i86/w=uptime
  66 f none usr/kernel/drv/dump 755 root sys
  67 f none usr/kernel/drv/fssnap 755 root sys
  68 f none usr/kernel/drv/kstat 755 root sys
  69 f none usr/kernel/drv/ksyms 755 root sys
  70 f none usr/kernel/drv/logindmux 755 root sys
  71 f none usr/kernel/drv/ptm 755 root sys
  72 f none usr/kernel/drv/pts 755 root sys
  73 f none usr/kernel/exec/javaexec 755 root sys
  74 f none usr/kernel/fs/fdfs 755 root sys
  75 f none usr/kernel/fs/pcfs 755 root sys
  76 f none usr/kernel/sched/FX 755 root sys
  77 f none usr/kernel/sched/FX_DPTBL 755 root sys
  78 f none usr/kernel/sched/IA 755 root sys
  79 f none usr/kernel/sched/RT 755 root sys
  80 f none usr/kernel/sched/RT_DPTBL 755 root sys
  81 f none usr/kernel/strmod/rlmod 755 root sys
  82 f none usr/kernel/strmod/telmod 755 root sys
  83 f none usr/kernel/strmod/cryptmod 755 root sys
  84 f none usr/kernel/sys/acctctl 755 root sys
  85 f none usr/kernel/sys/exacctsys 755 root sys
  86 f none usr/kernel/sys/sysacct 755 root sys
  87 f none usr/lib/devfsadm/linkmod/SUNW_ieee1394_link.so 755 root sys
  88 f none usr/lib/devfsadm/linkmod/SUNW_misc_link_i386.so 755 root sys
  89 f none usr/lib/devfsadm/linkmod/SUNW_xen_link.so 755 root sys
  90 s none usr/sbin/installgrub=../../sbin/installgrub
  91 f none usr/sbin/prtdiag 2755 root sys
  92 f none usr/sbin/rtc 555 root bin
  93 f none usr/sbin/ucodeadm 555 root bin
  94 d none usr/sbin/i86 755 root bin
  95 f none usr/sbin/i86/add_drv 555 root sys
  96 f none usr/sbin/i86/modinfo 555 root sys
  97 f none usr/sbin/i86/modload 555 root sys
  98 f none usr/sbin/i86/modunload 555 root sys
  99 f none usr/sbin/i86/pbind 555 root sys
 100 f none usr/sbin/i86/prtconf 2555 root sys
 101 f none usr/sbin/i86/psrset 555 root sys
 102 f none usr/sbin/i86/rem_drv 555 root sys
 103 f none usr/sbin/i86/swap 2555 root sys
 104 f none usr/sbin/i86/sysdef 2555 root sys
 105 f none usr/sbin/i86/update_drv 555 root sys
 106 f none usr/sbin/i86/whodo 4555 root bin
 107 d none usr/bin/amd64 755 root bin
 108 f none usr/bin/amd64/amt 555 root bin
 109 f none usr/bin/amd64/crle 555 root bin
 110 f none usr/bin/amd64/digest 555 root bin
 111 f none usr/bin/amd64/ksh93 555 root bin
 112 f none usr/bin/amd64/ls 555 root bin
 113 l none usr/bin/amd64/mac=digest
 114 f none usr/bin/amd64/moe 555 root bin
 115 f none usr/bin/amd64/newtask 4555 root sys
 116 f none usr/bin/amd64/nohup 555 root bin
 117 f none usr/bin/amd64/prctl 555 root bin
 118 f none usr/bin/amd64/prstat 555 root bin
 119 f none usr/bin/amd64/ps 555 root bin
 120 l none usr/bin/amd64/rksh93=ksh93
 121 f none usr/bin/amd64/savecore 555 root bin
 122 f none usr/bin/amd64/setuname 555 root bin
 123 f none usr/bin/amd64/uptime 4555 root bin
 124 l none usr/bin/amd64/w=uptime
 125 d none usr/kernel/drv/amd64 755 root sys
```

```
 126 f none usr/kernel/drv/amd64/dump 755 root sys
 127 f none usr/kernel/drv/amd64/fssnap 755 root sys
 128 f none usr/kernel/drv/amd64/kstat 755 root sys
 129 f none usr/kernel/drv/amd64/ksyms 755 root sys
 130 f none usr/kernel/drv/amd64/logindmux 755 root sys
 131 f none usr/kernel/drv/amd64/ptm 755 root sys
 132 f none usr/kernel/drv/amd64/pts 755 root sys
 133 d none usr/kernel/exec/amd64 755 root sys
 134 f none usr/kernel/exec/amd64/javaexec 755 root sys
 135 d none usr/kernel/fs/amd64 755 root sys
 136 f none usr/kernel/fs/amd64/fdfs 755 root sys
 137 f none usr/kernel/fs/amd64/pcfs 755 root sys
 138 d none usr/kernel/pcbe/amd64 755 root sys
 139 d none usr/kernel/sched/amd64 755 root sys
 140 f none usr/kernel/sched/amd64/FX 755 root sys
 141 f none usr/kernel/sched/amd64/FX_DPTBL 755 root sys
 142 f none usr/kernel/sched/amd64/IA 755 root sys
 143 f none usr/kernel/sched/amd64/RT 755 root sys
 144 f none usr/kernel/sched/amd64/RT_DPTBL 755 root sys
 145 d none usr/kernel/strmod/amd64 755 root sys
 146 f none usr/kernel/strmod/amd64/rlmod 755 root sys
 147 f none usr/kernel/strmod/amd64/telmod 755 root sys
 148 f none usr/kernel/strmod/amd64/cryptmod 755 root sys
 149 d none usr/kernel/sys/amd64 755 root sys
 150 f none usr/kernel/sys/amd64/acctctl 755 root sys
 151 f none usr/kernel/sys/amd64/exacctsys 755 root sys
 152 f none usr/kernel/sys/amd64/sysacct 755 root sys
 153 d none usr/lib/secure/amd64 755 root bin
 154 s none usr/lib/secure/64=amd64
 155 d none usr/lib/amd64 755 root bin
 156 s none usr/lib/amd64/ld.so.1=../../../lib/amd64/ld.so.1
 157 f none usr/lib/amd64/libshare.so.1 755 root bin
 158 d none usr/lib/fs/nfs 755 root sys
 159 d none usr/lib/fs/nfs/amd64 755 root sys
 160 d none usr/sbin/amd64 755 root bin
 161 f none usr/sbin/amd64/add_drv 555 root sys
 162 f none usr/sbin/amd64/modinfo 555 root sys
 163 f none usr/sbin/amd64/modload 555 root sys
 164 f none usr/sbin/amd64/modunload 555 root sys
 165 f none usr/sbin/amd64/pbind 555 root sys
 166 f none usr/sbin/amd64/prtconf 2555 root sys
 167 f none usr/sbin/amd64/psrset 555 root sys
 168 f none usr/sbin/amd64/rem_drv 555 root sys
 169 f none usr/sbin/amd64/swap 2555 root sys
 170 f none usr/sbin/amd64/sysdef 2555 root sys
 171 f none usr/sbin/amd64/update_drv 555 root sys
 172 f none usr/sbin/amd64/whodo 4555 root bin
```

```
**********************************************************
    5227 Mon Mar 24 15:32:46 2008
new/usr/src/pkgdefs/SUNWcsu/prototype_sparc
6658907 digest(1) and mac(1) could benefit from being 64-bit programs
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Copyright 2007 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)prototype_sparc    1.133   08/03/20 SMI"
# ident "@(#)prototype_sparc    1.132   07/11/29 SMI"
#
# This required package information file contains a list of package contents.
# The 'pkgmk' command uses this file to identify the contents of a package
# and their location on the development machine when building the package.
# Can be created via a text editor or through use of the 'pkgproto' command.
#

#!search <pathname pathname ...>        # where to find pkg objects
#!include <filename>                    # include another 'prototype' file
#!default <mode> <owner> <group>        # default used if not specified on entry
#!<param>=<value>                       # puts parameter in pkg environment

#
# Include ISA independent files (prototype_com)
#
!include prototype_com
#
# List files which are SPARC specific here
#
# source locations relative to the prototype file
#
# SUNWcsu
#
d none usr/bin/sparcv7 755 root bin
f none usr/bin/sparcv7/ksh93 555 root bin
l none usr/bin/sparcv7/rksh93=ksh93
f none usr/bin/sparcv7/savecore 555 root bin
f none usr/bin/sparcv7/digest 555 root bin
l none usr/bin/sparcv7/mac=digest
d none usr/bin/sparcv9 755 root bin
f none usr/bin/sparcv9/amt 555 root bin
f none usr/bin/sparcv9/crle 555 root bin
f none usr/bin/sparcv9/digest 555 root bin
f none usr/bin/sparcv9/ksh93 555 root bin
```



```
f none usr/bin/sparcv9/ls 555 root bin
l none usr/bin/sparcv9/mac=digest
f none usr/bin/sparcv9/moe 555 root bin
f none usr/bin/sparcv9/newtask 4555 root sys
f none usr/bin/sparcv9/nohup 555 root bin
f none usr/bin/sparcv9/prctl 555 root bin
f none usr/bin/sparcv9/prstat 555 root bin
f none usr/bin/sparcv9/ps 555 root bin
l none usr/bin/sparcv9/rksh93=ksh93
f none usr/bin/sparcv9/savecore 555 root bin
f none usr/bin/sparcv9/setuname 555 root bin
f none usr/bin/sparcv9/uptime 4555 root bin
l none usr/bin/sparcv9/w=uptime
d none usr/kernel/drv/sparcv9 755 root sys
f none usr/kernel/drv/sparcv9/dump 755 root sys
f none usr/kernel/drv/sparcv9/fssnap 755 root sys
f none usr/kernel/drv/sparcv9/kstat 755 root sys
f none usr/kernel/drv/sparcv9/ksyms 755 root sys
f none usr/kernel/drv/sparcv9/logindmux 755 root sys
f none usr/kernel/drv/sparcv9/ptm 755 root sys
f none usr/kernel/drv/sparcv9/pts 755 root sys
d none usr/kernel/exec/sparcv9 755 root sys
f none usr/kernel/exec/sparcv9/javaexec 755 root sys
d none usr/kernel/fs/sparcv9 755 root sys
f none usr/kernel/fs/sparcv9/fdfs 755 root sys
f none usr/kernel/fs/sparcv9/pcfs 755 root sys
d none usr/kernel/pcbe/sparcv9 755 root sys
d none usr/kernel/sched/sparcv9 755 root sys
f none usr/kernel/sched/sparcv9/FX 755 root sys
f none usr/kernel/sched/sparcv9/FX_DPTBL 755 root sys
f none usr/kernel/sched/sparcv9/IA 755 root sys
f none usr/kernel/sched/sparcv9/RT 755 root sys
f none usr/kernel/sched/sparcv9/RT_DPTBL 755 root sys
d none usr/kernel/strmod/sparcv9 755 root sys
f none usr/kernel/strmod/sparcv9/rlmod 755 root sys
f none usr/kernel/strmod/sparcv9/telmod 755 root sys
f none usr/kernel/strmod/sparcv9/cryptmod 755 root sys
d none usr/kernel/sys/sparcv9 755 root sys
f none usr/kernel/sys/sparcv9/acctctl 755 root sys
f none usr/kernel/sys/sparcv9/exacctsys 755 root sys
f none usr/kernel/sys/sparcv9/sysacct 755 root sys
f none usr/lib/ld.so 755 root bin
f none usr/lib/devfsadm/linkmod/SUNW_ieee1394_link.so 755 root sys
f none usr/lib/devfsadm/linkmod/SUNW_misc_link_sparc.so 755 root sys
f none usr/lib/rcm/modules/SUNW_ttymux_rcm.so 555 root bin
d none usr/lib/secure/sparcv9 755 root bin
s none usr/lib/secure/64=sparcv9
d none usr/lib/sparcv9 755 root bin
s none usr/lib/sparcv9/ld.so.1=../../../lib/sparcv9/ld.so.1
f none usr/lib/sparcv9/libshare.so.1 755 root bin
d none usr/lib/fs/nfs 755 root sys
d none usr/lib/fs/nfs/sparcv9 755 root sys
s none usr/sbin/fiocompress=../../sbin/fiocompress
l none usr/sbin/prtdiag=../../usr/lib/platexec
d none usr/sbin/sparcv9 755 root bin
f none usr/sbin/sparcv9/add_drv 555 root sys
f none usr/sbin/sparcv9/modinfo 555 root sys
f none usr/sbin/sparcv9/modload 555 root sys
f none usr/sbin/sparcv9/modunload 555 root sys
f none usr/sbin/sparcv9/pbind 555 root sys
f none usr/sbin/sparcv9/prtconf 2555 root sys
f none usr/sbin/sparcv9/psrset 555 root sys
f none usr/sbin/sparcv9/rem_drv 555 root sys
f none usr/sbin/sparcv9/swap 2555 root sys
f none usr/sbin/sparcv9/sysdef 2555 root sys
f none usr/sbin/sparcv9/update_drv 555 root sys
```

```
 126 f none usr/sbin/sparcv9/whodo 4555 root bin
```

```
**********************************************************
    6002 Mon Mar 24 15:32:50 2008
new/usr/src/tools/opensolaris/license-list
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
   1 usr/closed/cmd/man/src/util/solbookv1/THIRDPARTYLICENSE
   2 usr/closed/cmd/ndmpd/LICENSE
   3 usr/closed/lib/smartcard/ocfserv/opencard/core/event/THIRDPARTYLICENSE
   4 usr/src/cmd/agents/snmp/THIRDPARTYLICENSE
   5 usr/src/cmd/ast/THIRDPARTYLICENSE
   6 usr/src/cmd/backup/dump/THIRDPARTYLICENSE
   7 usr/src/cmd/bnu/THIRDPARTYLICENSE
   8 usr/src/cmd/checkeq/THIRDPARTYLICENSE
   9 usr/src/cmd/checknr/THIRDPARTYLICENSE
  10 usr/src/cmd/cmd-inet/THIRDPARTYLICENSE.kcmd
  11 usr/src/cmd/cmd-inet/sbin/ifparse/THIRDPARTYLICENSE
  12 usr/src/cmd/cmd-inet/usr.bin/THIRDPARTYLICENSE.rcp
  13 usr/src/cmd/cmd-inet/usr.bin/THIRDPARTYLICENSE.rsh
  14 usr/src/cmd/cmd-inet/usr.bin/ftp/THIRDPARTYLICENSE
  15 usr/src/cmd/cmd-inet/usr.bin/pppd/THIRDPARTYLICENSE
  16 usr/src/cmd/cmd-inet/usr.bin/pppd/plugins/THIRDPARTYLICENSE.minconnect
  17 usr/src/cmd/cmd-inet/usr.bin/pppd/plugins/THIRDPARTYLICENSE.passwd
  18 usr/src/cmd/cmd-inet/usr.bin/pppdump/LICENSE.top
  19 usr/src/cmd/cmd-inet/usr.bin/rdist/THIRDPARTYLICENSE
  20 usr/src/cmd/cmd-inet/usr.bin/telnet/THIRDPARTYLICENSE
  21 usr/src/cmd/cmd-inet/usr.lib/in.mpathd/THIRDPARTYLICENSE
  22 usr/src/cmd/cmd-inet/usr.sbin/THIRDPARTYLICENSE.arp
  23 usr/src/cmd/cmd-inet/usr.sbin/THIRDPARTYLICENSE.comsat
  24 usr/src/cmd/cmd-inet/usr.sbin/THIRDPARTYLICENSE.rlogind
  25 usr/src/cmd/cmd-inet/usr.sbin/THIRDPARTYLICENSE.route
  26 usr/src/cmd/cmd-inet/usr.sbin/ifconfig/THIRDPARTYLICENSE
  27 usr/src/cmd/cmd-inet/usr.sbin/in.ftpd/LICENSE
  28 usr/src/cmd/cmd-inet/usr.sbin/in.rdisc/THIRDPARTYLICENSE
  29 usr/src/cmd/cmd-inet/usr.sbin/in.routed/THIRDPARTYLICENSE
  30 usr/src/cmd/cmd-inet/usr.sbin/traceroute/THIRDPARTYLICENSE
  31 usr/src/cmd/compress/THIRDPARTYLICENSE
  32 usr/src/cmd/csh/THIRDPARTYLICENSE
  33 usr/src/cmd/eeprom/THIRDPARTYLICENSE
  34 usr/src/cmd/eqn/THIRDPARTYLICENSE
  35 usr/src/cmd/fs.d/udfs/fsck/THIRDPARTYLICENSE
  36 usr/src/cmd/fs.d/ufs/THIRDPARTYLICENSE
  37 usr/src/cmd/ipf/tools/IPFILTER.LICENCE
  38 usr/src/cmd/lastcomm/THIRDPARTYLICENSE
  39 usr/src/cmd/ldap/THIRDPARTYLICENSE
  40 usr/src/cmd/look/THIRDPARTYLICENSE
  41 usr/src/cmd/lp/cmd/lptest/THIRDPARTYLICENSE
  42 usr/src/cmd/man/src/THIRDPARTYLICENSE
  43 usr/src/cmd/man/src/util/THIRDPARTYLICENSE
  44 usr/src/cmd/man/src/util/instant.src/THIRDPARTYLICENSE
  45 usr/src/cmd/man/src/util/nsgmls.src/COPYING
  46 usr/src/cmd/man/src/util/solbookv2/THIRDPARTYLICENSE
  47 usr/src/cmd/mdb/common/libstand/THIRDPARTYLICENSE
  48 usr/src/cmd/mt/THIRDPARTYLICENSE
  49 usr/src/cmd/perl/5.8.4/distrib/ext/Cwd/THIRDPARTYLICENSE
  50 usr/src/cmd/perl/THIRDPARTYLICENSE
  51 usr/src/cmd/refer/THIRDPARTYLICENSE
  52 usr/src/cmd/script/THIRDPARTYLICENSE
  53 usr/src/cmd/sendmail/THIRDPARTYLICENSE
  54 usr/src/cmd/soelim/THIRDPARTYLICENSE
  55 usr/src/cmd/ssh/THIRDPARTYLICENSE
  56 usr/src/cmd/stat/vmstat/THIRDPARTYLICENSE
  57 usr/src/cmd/tbl/THIRDPARTYLICENSE
  58 usr/src/cmd/tcpd/THIRDPARTYLICENSE
  59 usr/src/cmd/terminfo/THIRDPARTYLICENSE
  60 usr/src/cmd/tip/THIRDPARTYLICENSE
```



```
  61 usr/src/cmd/ul/THIRDPARTYLICENSE
  62 usr/src/cmd/units/THIRDPARTYLICENSE
  63 usr/src/cmd/vgrind/THIRDPARTYLICENSE
  64 usr/src/cmd/vi/THIRDPARTYLICENSE
  65 usr/src/cmd/which/THIRDPARTYLICENSE
  66 usr/src/cmd/xntpd/THIRDPARTYLICENSE
  67 usr/src/cmd/xstr/THIRDPARTYLICENSE
  68 usr/src/common/crypto/arcfour/amd64/THIRDPARTYLICENSE
  69 usr/src/common/crypto/sha1/amd64/THIRDPARTYLICENSE
  70 usr/src/common/crypto/sha2/amd64/THIRDPARTYLICENSE
  71 usr/src/common/openssl/LICENSE
  72 usr/src/grub/grub-0.95/COPYING
  73 usr/src/lib/gss_mechs/mech_krb5/THIRDPARTYLICENSE
  74 usr/src/lib/krb5/THIRDPARTYLICENSE
  75 usr/src/lib/libast/THIRDPARTYLICENSE
  76 usr/src/lib/libbc/THIRDPARTYLICENSE
  77 usr/src/lib/libbsdmalloc/THIRDPARTYLICENSE
  78 usr/src/lib/libcmd/THIRDPARTYLICENSE
  79 usr/src/lib/libdll/THIRDPARTYLICENSE
  80 usr/src/lib/libgss/THIRDPARTYLICENSE
  81 usr/src/lib/libinetutil/common/THIRDPARTYLICENSE
  82 usr/src/lib/libkmf/THIRDPARTYLICENSE
  83 usr/src/lib/libldap5/THIRDPARTYLICENSE
  84 usr/src/lib/libmp/common/THIRDPARTYLICENSE
  85 usr/src/lib/libpp/THIRDPARTYLICENSE
  86 usr/src/lib/libresolv/THIRDPARTYLICENSE
  87 usr/src/lib/libresolv2/THIRDPARTYLICENSE
  88 usr/src/lib/libsasl/THIRDPARTYLICENSE
  89 usr/src/lib/libshell/THIRDPARTYLICENSE
  90 usr/src/lib/libtecla/THIRDPARTYLICENSE
  91 usr/src/lib/pam_modules/authtok_check/THIRDPARTYLICENSE
  92 usr/src/lib/passwdutil/THIRDPARTYLICENSE
  93 usr/src/lib/pkcs11/include/THIRDPARTYLICENSE
  94 usr/src/stand/lib/tcp/THIRDPARTYLICENSE
  95 usr/src/tools/ctf/dwarf/THIRDPARTYLICENSE
  96 usr/src/ucbcmd/basename/THIRDPARTYLICENSE
  97 usr/src/ucbcmd/echo/THIRDPARTYLICENSE
  98 usr/src/ucbcmd/from/THIRDPARTYLICENSE
  99 usr/src/ucbcmd/groups/THIRDPARTYLICENSE
 100 usr/src/ucbcmd/ln/THIRDPARTYLICENSE
 101 usr/src/ucbcmd/ls/THIRDPARTYLICENSE
 102 usr/src/ucbcmd/plot/THIRDPARTYLICENSE
 103 usr/src/ucbcmd/sum/THIRDPARTYLICENSE
 104 usr/src/ucbcmd/test/THIRDPARTYLICENSE
 105 usr/src/ucbcmd/tset/THIRDPARTYLICENSE
 106 usr/src/ucbcmd/users/THIRDPARTYLICENSE
 107 usr/src/ucbcmd/whereis/THIRDPARTYLICENSE
 108 usr/src/ucbcmd/whoami/THIRDPARTYLICENSE
 109 usr/src/ucblib/libcurses/THIRDPARTYLICENSE
 110 usr/src/ucblib/libtermcap/THIRDPARTYLICENSE
 111 usr/src/ucblib/libucb/THIRDPARTYLICENSE
 112 usr/src/uts/common/gssapi/mechs/krb5/THIRDPARTYLICENSE
 113 usr/src/uts/common/inet/ip/THIRDPARTYLICENSE.rts
 114 usr/src/uts/common/inet/tcp/THIRDPARTYLICENSE
 115 usr/src/uts/common/io/THIRDPARTYLICENSE.etheraddr
 116 usr/src/uts/common/io/aac/THIRDPARTYLICENSE
 117 usr/src/uts/common/io/afe/THIRDPARTYLICENSE
 118 usr/src/uts/common/io/chxge/com/THIRDPARTYLICENSE
 119 usr/src/uts/common/io/ib/clients/rds/THIRDPARTYLICENSE
 120 usr/src/uts/common/io/iwk/THIRDPARTYLICENSE
 121 usr/src/uts/common/io/iwk/fw-iw/LICENSE
 122 usr/src/uts/common/io/mxfe/THIRDPARTYLICENSE
 123 usr/src/uts/common/io/sfe/THIRDPARTYLICENSE
 124 usr/src/uts/common/io/wpi/fw-wpi/LICENSE
 125 usr/src/uts/common/sys/THIRDPARTYLICENSE.agpgart
 126 usr/src/uts/common/sys/THIRDPARTYLICENSE.icu
```

```
 127 usr/src/uts/common/sys/THIRDPARTYLICENSE.unicode
 128 usr/src/uts/common/sys/i2o/THIRDPARTYLICENSE
 129 usr/src/uts/common/zmod/THIRDPARTYLICENSE
 130 usr/src/uts/intel/THIRDPARTYLICENSE
 131 usr/src/uts/intel/io/acpica/THIRDPARTYLICENSE
 132 usr/src/uts/intel/io/amr/THIRDPARTYLICENSE
 133 usr/src/common/crypto/ecc/THIRDPARTYLICENSE
 134 usr/src/common/mpi/THIRDPARTYLICENSE
 135 usr/src/lib/libsmbfs/smb/THIRDPARTYLICENSE.apple
 136 usr/src/lib/libsmbfs/smb/THIRDPARTYLICENSE.boris_popov
 137 usr/src/lib/libsmbfs/smb/THIRDPARTYLICENSE.bsd4
 138 usr/src/lib/libsmbfs/smb/THIRDPARTYLICENSE.microsoft
```

```
**********************************************************
   16832 Mon Mar 24 15:32:54 2008
new/usr/src/uts/common/sys/crypto/common.h
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
```

```
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License (the "License").
 * You may not use this file except in compliance with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#ifndef _SYS_CRYPTO_COMMON_H
#define _SYS_CRYPTO_COMMON_H

#pragma ident   "@(#)common.h   1.27    08/03/20 SMI"
#pragma ident   "@(#)common.h   1.26    08/01/04 SMI"

/*
 * Header file for the common data structures of the cryptographic framework
 */

#ifdef __cplusplus
extern "C" {
#endif

#include <sys/types.h>
#include <sys/uio.h>
#include <sys/stream.h>
#include <sys/mutex.h>
#include <sys/condvar.h>


/* Cryptographic Mechanisms */

#define CRYPTO_MAX_MECH_NAME 32
typedef char crypto_mech_name_t[CRYPTO_MAX_MECH_NAME];

typedef uint64_t crypto_mech_type_t;

typedef struct crypto_mechanism {
        crypto_mech_type_t      cm_type;        /* mechanism type */
        caddr_t                 cm_param;       /* mech. parameter */
        size_t                  cm_param_len;   /* mech. parameter len */
} crypto_mechanism_t;
```

*_____unchanged_portion_omitted_*

```
#endif  /* _SYSCALL32 */
```



```
#endif /* _KERNEL */

/*
 * The measurement unit bit flag for a mechanism's minimum or maximum key size.
 * The unit are mechanism dependant.  It can be in bits or in bytes.
 */
typedef uint32_t crypto_keysize_unit_t;

/*
 * The following bit flags are valid in cm_mech_flags field in
 * the crypto_mech_info_t structure of the SPI.
 *
 * Only the first two bit flags are valid in mi_keysize_unit
 * field in the crypto_mechanism_info_t structure of the API.
 */
#define CRYPTO_KEYSIZE_UNIT_IN_BITS     0x00000001
#define CRYPTO_KEYSIZE_UNIT_IN_BYTES    0x00000002
#define CRYPTO_CAN_SHARE_OPSTATE        0x00000004 /* supports sharing */


/* Mechanisms supported out-of-the-box */
#define SUN_CKM_MD4                     "CKM_MD4"
#define SUN_CKM_MD5                     "CKM_MD5"
#define SUN_CKM_MD5_HMAC                "CKM_MD5_HMAC"
#define SUN_CKM_MD5_HMAC_GENERAL        "CKM_MD5_HMAC_GENERAL"
#define SUN_CKM_SHA1                    "CKM_SHA_1"
#define SUN_CKM_SHA1_HMAC               "CKM_SHA_1_HMAC"
#define SUN_CKM_SHA1_HMAC_GENERAL       "CKM_SHA_1_HMAC_GENERAL"
#define SUN_CKM_SHA256                  "CKM_SHA256"
#define SUN_CKM_SHA256_HMAC             "CKM_SHA256_HMAC"
#define SUN_CKM_SHA256_HMAC_GENERAL     "CKM_SHA256_HMAC_GENERAL"
#define SUN_CKM_SHA384                  "CKM_SHA384"
#define SUN_CKM_SHA384_HMAC             "CKM_SHA384_HMAC"
#define SUN_CKM_SHA384_HMAC_GENERAL     "CKM_SHA384_HMAC_GENERAL"
#define SUN_CKM_SHA512                  "CKM_SHA512"
#define SUN_CKM_SHA512_HMAC             "CKM_SHA512_HMAC"
#define SUN_CKM_SHA512_HMAC_GENERAL     "CKM_SHA512_HMAC_GENERAL"
#define SUN_CKM_DES_CBC                 "CKM_DES_CBC"
#define SUN_CKM_DES3_CBC                "CKM_DES3_CBC"
#define SUN_CKM_DES_ECB                 "CKM_DES_ECB"
#define SUN_CKM_DES3_ECB                "CKM_DES3_ECB"
#define SUN_CKM_BLOWFISH_CBC            "CKM_BLOWFISH_CBC"
#define SUN_CKM_BLOWFISH_ECB            "CKM_BLOWFISH_ECB"
#define SUN_CKM_AES_CBC                 "CKM_AES_CBC"
#define SUN_CKM_AES_ECB                 "CKM_AES_ECB"
#define SUN_CKM_AES_CTR                 "CKM_AES_CTR"
#define SUN_CKM_AES_CCM                 "CKM_AES_CCM"
#define SUN_CKM_RC4                     "CKM_RC4"
#define SUN_CKM_RSA_PKCS                "CKM_RSA_PKCS"
#define SUN_CKM_RSA_X_509               "CKM_RSA_X_509"
#define SUN_CKM_MD5_RSA_PKCS            "CKM_MD5_RSA_PKCS"
#define SUN_CKM_SHA1_RSA_PKCS           "CKM_SHA1_RSA_PKCS"
#define SUN_CKM_SHA256_RSA_PKCS         "CKM_SHA256_RSA_PKCS"
#define SUN_CKM_SHA384_RSA_PKCS         "CKM_SHA384_RSA_PKCS"
#define SUN_CKM_SHA512_RSA_PKCS         "CKM_SHA512_RSA_PKCS"
#define SUN_CKM_EC_KEY_PAIR_GEN         "CKM_EC_KEY_PAIR_GEN"
#define SUN_CKM_ECDH1_DERIVE            "CKM_ECDH1_DERIVE"
#define SUN_CKM_ECDSA_SHA1              "CKM_ECDSA_SHA1"
#define SUN_CKM_ECDSA                   "CKM_ECDSA"

/* Shared operation context format for CKM_RC4 */
typedef struct {
#if defined(__amd64)
        uint32_t i, j;
        uint32_t arr[256];
typedef uint64_t arcfour_key_int_t;
```

```
 194 #else
 195         uchar_t arr[256];
 196         uchar_t i, j;
 193 typedef uchar_t arcfour_key_int_t;
 197 #endif /* __amd64 */

 196 typedef struct {
 197         arcfour_key_int_t arr[256];
 198         arcfour_key_int_t i, j;
 198         uint64_t pad;           /* For 64-bit alignment */
 199 } arcfour_state_t;
```

_____unchanged_portion_omitted_

```
**********************************************************
    4323 Mon Mar 24 15:32:59 2008
new/usr/src/uts/common/sys/sha2.h
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
```

```
/*
 * CDDL HEADER START
 *
 * The contents of this file are subject to the terms of the
 * Common Development and Distribution License (the "License").
 * You may not use this file except in compliance with the License.
 *
 * You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
 * or http://www.opensolaris.org/os/licensing.
 * See the License for the specific language governing permissions
 * and limitations under the License.
 *
 * When distributing Covered Code, include this CDDL HEADER in each
 * file and include the License file at usr/src/OPENSOLARIS.LICENSE.
 * If applicable, add the following below this CDDL HEADER, with the
 * fields enclosed by brackets "[]" replaced with your own identifying
 * information: Portions Copyright [yyyy] [name of copyright owner]
 *
 * CDDL HEADER END
 */
/*
 * Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
 * Copyright 2006 Sun Microsystems, Inc.  All rights reserved.
 * Use is subject to license terms.
 */

#ifndef _SYS_SHA2_H
#define _SYS_SHA2_H

#pragma ident   "@(#)sha2.h     1.5     08/03/20 SMI"
#pragma ident   "@(#)sha2.h     1.4     06/03/28 SMI"

#include <sys/types.h>          /* for uint_* */

#ifdef  __cplusplus
extern "C" {
#endif

#define SHA2_HMAC_MIN_KEY_LEN   8       /* SHA2-HMAC min key length in bits */
#define SHA2_HMAC_MAX_KEY_LEN   INT_MAX /* SHA2-HMAC max key length in bits */

#define SHA256_DIGEST_LENGTH    32      /* SHA256 digest length in bytes */
#define SHA384_DIGEST_LENGTH    48      /* SHA384 digest length in bytes */
#define SHA512_DIGEST_LENGTH    64      /* SHA512 digest length in bytes */

#define SHA256_HMAC_BLOCK_SIZE  64      /* SHA256-HMAC block size */
#define SHA512_HMAC_BLOCK_SIZE  128     /* SHA512-HMAC block size */

#define SHA256                  0
#define SHA256_HMAC             1
#define SHA256_HMAC_GEN         2
#define SHA384                  3
#define SHA384_HMAC             4
#define SHA384_HMAC_GEN         5
#define SHA512                  6
#define SHA512_HMAC             7
#define SHA512_HMAC_GEN         8

/*
 * SHA2 context.
 * The contents of this structure are a private interface between the
```



```
 * Init/Update/Final calls of the functions defined below.
 * Callers must never attempt to read or write any of the fields
 * in this structure directly.
 * in this strucutre directly.
 */
typedef struct  {
        uint32_t algotype;              /* Algorithm Type */

        /* state (ABCDEFGH) */
        union {
                uint32_t s32[8];        /* for SHA256 */
                uint64_t s64[8];        /* for SHA384/512 */
        } state;
        /* number of bits */
        union {
                uint32_t c32[2];        /* for SHA256 , modulo 2^64 */
                uint64_t c64[2];        /* for SHA384/512, modulo 2^128 */
        } count;
        union {
                uint8_t         buf8[128];      /* undigested input */
                uint32_t        buf32[32];      /* realigned input */
                uint64_t        buf64[16];      /* realigned input */
        } buf_un;
} SHA2_CTX;
______unchanged_portion_omitted_
```

```
**********************************************************
    2610 Mon Mar 24 15:33:03 2008
new/usr/src/uts/intel/arcfour/Makefile
6652716 Need an ARCFOUR implementation optimized for Intel EM64T
**********************************************************
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
# ident "@(#)Makefile   1.8     08/03/20 SMI"
# ident "@(#)Makefile   1.7     08/01/02 SMI"
#
#       This makefile drives the production of the ARCFOUR KEF provider.
#
#       intel implementation architecture dependent
#


#
#       Path to the base of the uts directory tree (usually /usr/src/uts).
#
UTSBASE = ../..
COM_DIR = $(COMMONBASE)/crypto/arcfour

#
#       Define the module and object file sets.
#
MODULE          = arcfour
LINTS           = $(ARCFOURPROV_OBJS:%.o=$(LINTS_DIR)/%.ln)
ARCFOURPROV_OBJS_32 =
ARCFOURPROV_OBJS_64 = arcfour-x86_64.o
ARCFOURPROV_OBJS_64 = arcfour_crypt_amd64.o
ARCFOURPROV_OBJS += $(ARCFOURPROV_OBJS_$(CLASS))
OBJECTS         = $(ARCFOURPROV_OBJS:%=$(OBJS_DIR)/%)
ROOTMODULE      = $(ROOT_CRYPTO_DIR)/$(MODULE)

#
#       Include common rules.
#
include $(UTSBASE)/intel/Makefile.intel

#       set signing mode
ELFSIGN_MOD     = $(ELFSIGN_CRYPTO)

#
#       Define targets
#
```



```
ALL_TARGET      = $(BINARY)
LINT_TARGET     = $(MODULE).lint
INSTALL_TARGET  = $(BINARY) $(ROOTMODULE)

#
# Overrides
#
CPPFLAGS        += -I$(COM_DIR)
CLEANFILES      += arcfour-x86_64.s

#
# For now, disable these lint checks; maintainers should endeavor
# to investigate and remove these for maximum lint coverage.
# Please do not carry these forward to new Makefiles.
#
LINTTAGS        += -erroff=E_PTRDIFF_OVERFLOW

#
#       Default build targets.
#
.KEEP_STATE:

def:            $(DEF_DEPS)

all:            $(ALL_DEPS)

clean:          $(CLEAN_DEPS)

clobber:        $(CLOBBER_DEPS)

lint:           $(LINT_DEPS)

modlintlib:     $(MODLINTLIB_DEPS)

clean.lint:     $(CLEAN_LINT_DEPS)

install:        $(INSTALL_DEPS)

#
#       Include common targets.
#
include $(UTSBASE)/intel/Makefile.targ

$(OBJS_DIR)/arcfour-x86_64.o: arcfour-x86_64.s
        $(COMPILE.s) -o $@ ${@F:.o=.s}
$(OBJS_DIR)/arcfour_crypt_amd64.o: $(COM_DIR)/amd64/arcfour_crypt_amd64.s
        $(COMPILE.s) -o $@ $(COM_DIR)/amd64/arcfour_crypt_amd64.s
        $(POST_PROCESS_O)

$(OBJS_DIR)/arcfour-x86_64.ln: arcfour-x86_64.s
        @($(LHEAD) $(LINT.s) ${@F:.ln=.s} $(LTAIL))
$(OBJS_DIR)/arcfour_crypt_amd64.ln: $(COM_DIR)/amd64/arcfour_crypt_amd64.s
        @($(LHEAD) $(LINT.c) $(COM_DIR)/amd64/arcfour_crypt_amd64.s $(LTAIL))

arcfour-x86_64.s: $(COM_DIR)/amd64/arcfour-x86_64.pl
        $(PERL) $? $@
```

```
**********************************************************
    2794 Mon Mar 24 15:33:07 2008
new/usr/src/uts/intel/sha2/Makefile
6665607 Need a SHA256/SHA384/SHA512 implementation optimized for 64-bit x86
**********************************************************
```

```
#
# CDDL HEADER START
#
# The contents of this file are subject to the terms of the
# Common Development and Distribution License (the "License").
# You may not use this file except in compliance with the License.
#
# You can obtain a copy of the license at usr/src/OPENSOLARIS.LICENSE
# or http://www.opensolaris.org/os/licensing.
# See the License for the specific language governing permissions
# and limitations under the License.
#
# When distributing Covered Code, include this CDDL HEADER in each
# file and include the License file at usr/src/OPENSOLARIS.LICENSE.
# If applicable, add the following below this CDDL HEADER, with the
# fields enclosed by brackets "[]" replaced with your own identifying
# information: Portions Copyright [yyyy] [name of copyright owner]
#
# CDDL HEADER END
#
#
# Copyright 2008 Sun Microsystems, Inc.  All rights reserved.
# Copyright 2006 Sun Microsystems, Inc.  All rights reserved.
# Use is subject to license terms.
#
#ident  "@(#)Makefile   1.4     08/03/20 SMI"
#ident  "@(#)Makefile   1.3     06/11/02 SMI"
#
#       This makefile drives the production of the sha2 crypto kernel module.
#
#       intel architecture dependent
#


#
#       Path to the base of the uts directory tree (usually /usr/src/uts).
#
UTSBASE = ../..
COMDIR  = $(COMMONBASE)/crypto/sha2

#
#       Define the module and object file sets.
#
MODULE          = sha2
LINTS           = $(SHA2_OBJS:%.o=$(LINTS_DIR)/%.ln)
SHA2_OBJS_32    =
SHA2_OBJS_64    = sha512-x86_64.o sha256-x86_64.o
SHA2_OBJS       += $(SHA2_OBJS_$(CLASS))
OBJECTS         = $(SHA2_OBJS:%=$(OBJS_DIR)/%)
LINTS           = $(SHA2_OBJS:%.o=$(LINTS_DIR)/%.ln)
ROOTMODULE      = $(ROOT_CRYPTO_DIR)/$(MODULE)
ROOTLINK        = $(ROOT_MISC_DIR)/$(MODULE)

#
#       Include common rules.
#
include $(UTSBASE)/intel/Makefile.intel

#
#       Override defaults
#
CLEANFILES += sha512-x86_64.s sha256-x86_64.s
```



```
#
#       Define targets
#
ALL_TARGET      = $(BINARY)
LINT_TARGET     = $(MODULE).lint
INSTALL_TARGET  = $(BINARY) $(ROOTMODULE) $(ROOTLINK)

#
# For now, disable these lint checks; maintainers should endeavor
# to investigate and remove these for maximum lint coverage.
# Please do not carry these forward to new Makefiles.
#
LINTTAGS        += -erroff=E_BAD_PTR_CAST_ALIGN
LINTTAGS        += -erroff=E_SUPPRESSION_DIRECTIVE_UNUSED
LINTTAGS        += -erroff=E_PTRDIFF_OVERFLOW
LINTTAGS        += -erroff=E_ASSIGN_NARROW_CONV

#
#       Default build targets.
#
.KEEP_STATE:

def:            $(DEF_DEPS)

all:            $(ALL_DEPS)

clean:          $(CLEAN_DEPS)

clobber:        $(CLOBBER_DEPS)

lint:           $(LINT_DEPS)

modlintlib:     $(MODLINTLIB_DEPS)

clean.lint:     $(CLEAN_LINT_DEPS)

install:        $(INSTALL_DEPS)

$(ROOTLINK):    $(ROOT_MISC_DIR) $(ROOTMODULE)
        -$(RM) $@; ln $(ROOTMODULE) $@

#
#       Include common targets.
#
include $(UTSBASE)/intel/Makefile.targ

$(OBJS_DIR)/%.o: %.s
        $(COMPILE.s) -o $@ ${@F:.o=.s}
        $(POST_PROCESS_O)

$(OBJS_DIR)/%.ln: %.s
        @($(LHEAD) $(LINT.c) ${@F:.ln=.s} $(LTAIL))

sha512-x86_64.s: $(COMDIR)/amd64/sha512-x86_64.pl
        $(PERL) $? $@

sha256-x86_64.s: $(COMDIR)/amd64/sha512-x86_64.pl
        $(PERL) $? $@
```