IBM より 5 倍速かった SHA-1　論理図面編

2016/03/29 版 (ICF3 の URL を変更)

2015/07/21 版 (初版)

平山　直紀

著者概略

1992 年 早稲田大学理工学部　電気工学科卒

1994 年 早稲田大学理工学研究科 計算機工学専攻卒

1994 年 日立製作所 中央研究所　超高速プロセッサ部　入社

1995 年 日立製作所 汎用コンピュータ事業部に転勤

2005 年 日立製作所　退職

2006 年 株式会社ｉＣａｎａｌ設立、代表取締役社長

著作権について

注意事項

この論理図面は原案です。実際に製品になっているものは、これを改良したものです。

私、平山直紀が論理の勉強のために初めて作成したものなので過度の期待はできないかもしれません。

このファイルを公開しているサイト URL

http://www.canal.mokuren.ne.jp/memo/sha1ronri.html

初版(2015/07/21)のファイルでも過去に作成した資料のすべてが添付されているので、それほどバージョンアップされることはありませんが、最新版を確認したほうがいいかもしれません。

1. はじめに

SHA-1 とはハッシュアルゴリズムです。CPU が作りたくて 1994 年に日立製作所に入社したが、その数年後、自宅で論理の勉強を始めたときに作った論理が SHA-1 でした。しかし、それが 1999 年にメインフレームの暗号装置として製品化され IBM の 5 倍以上の性能が出たのです。製品化された論理は、多少、改良が加えられていますが、ここで公開する論理図面をみれば 5 倍以上の性能が出た理由がわかると思います。

２. 論理シミュレータ CHDL

自分が考えた方法が、本当に論理実装できるのかを確認するため CHDL という論理シミュレータを使いました。CHDL は富士通の人がフリーで公開した論理シミュレータです。「お仕着せの CPU では、つまらない。スーパースカラの CPU を設計したい。」そんな説明のあった論理シミュレータです。
その後、VHDL を自費で 20 万円で購入したため、以降、使うことはありませんでしたが。

３. 製品化された製品の名称

日立製作所　中型メインフレーム MP5600EX の暗号装置　(1999 年 発売)
LSI 開発コード名　ICF3
ICF3 には、世界一高速な RSA 暗号の演算装置も実装されています。これも私が開発したもの。
参考 URL
http://icanal.idletime.tokyo/ESD.html

４. おわりに

あまり過度の期待は、しないでください。論理の勉強のために、ちょっと作ったものなので。

HASH ｱﾙｺﾞﾘｽﾞﾑ(FIPS 180-1)の論理実現方法

1. 目的

「安全なﾊｯｼｭ標準」(SECURE HASH STANDARD) FIPS(Federal Information Processing Standards Publication) 180-1 で記述されるﾊｯｼｭｱﾙｺﾞﾘｽﾞﾑ SHA-1 について説明を行い、論理による実現を行う。

2. 概要

2-1 HASH ｱﾙｺﾞﾘｽﾞﾑ(FIPS 180-1) SHA-1 ｱﾙｺﾞﾘｽﾞﾑの説明

SHA-1 は、2^{64} bit 以下の入力ﾃﾞｰﾀ(ﾒｯｾｰｼﾞ)からﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄと呼ばれる 160bit の出力ﾃﾞｰﾀを生成するｱﾙｺﾞﾘｽﾞﾑである。

- ﾃﾞｰﾀを 512bit のﾌﾞﾛｯｸに分割し、ﾌﾞﾛｯｸ単位で処理する。
  「3.ﾌﾞﾛｯｸ処理方法」で解説
- 最後のﾌﾞﾛｯｸの長さがちょうど 512bit となるようﾃﾞｰﾀを付加する。
  「4.最後のﾌﾞﾛｯｸの長さを 512bit にする方法」で解説

2-2 論理実現方法

「3-2.ｱﾙｺﾞﾘｽﾞﾑ1」で示される SHA-1 のｱﾙｺﾞﾘｽﾞﾑを C 言語でｲﾝﾌﾟﾘﾒﾝﾄした。ﾘｽﾄと実行結果をｼｰﾄの 4,5 に示す。HIPO をｼｰﾄ 6,7 に、簡易論理ｼﾐｭﾚｰﾀのﾘｽﾄをｼｰﾄ 8,9 に、その実行結果をｼｰﾄ 10,11 に示す。

このままの論理では、32bit の加算器 3 段のﾃﾞｨﾚｲが懸念される。そこで「3-2. ｱﾙｺﾞﾘｽﾞﾑ1」の Step.4 を、数列を用いて以下のように式変形し、1cyc での加算器の段数を 1 とする。

TEMP= a_{t+5} ; A=a_{t+4} ; B=a_{t+3} ; C=$S^{30}(a_{t+2})$; D=$S^{30}(a_{t+1})$; E=$S^{30}(a_t)$

(変形前)

$$a_{t+5} = S^5(a_{t+4}) + f_t(a_{t+3}, S^{30}(a_{t+2}), S^{30}(a_{t+1})) + S^{30}(a_t) + W_t + K_t$$

($0 \leqq t \leqq 79$)

(変形後)

$$a_{t+5} = S^5(a_{t+4}) + X \qquad \text{--- (1)}$$

$$X = f_{t+1}(a_{t+4}, S^{30}(a_{t+3}), S^{30}(a_{t+2})) + Y \qquad \text{--- (2)}$$

$$Y = S^{30}(a_{t+2}) + Z \qquad \text{--- (3)}$$

$$Z = W_{t+3} + K_{t+3} \qquad \text{--- (4)}$$

($-3 \leqq t \leqq 79$)

式(1),(2),(3),(4)間には、依存関係がないため同時実行が可能である。

式変形後のｱﾙｺﾞﾘｽﾞﾑを C 言語でｲﾝﾌﾟﾘﾒﾝﾄしたﾘｽﾄと結果をｼｰﾄ 12,13 に示す。HIPO をｼｰﾄ 14,15 に、簡易論理ｼﾐｭﾚｰﾀのﾘｽﾄをｼｰﾄ 16 に、その実行結果をｼｰﾄ 17,18 に示す。

3. ﾌﾞﾛｯｸ処理方法

512bit のﾌﾞﾛｯｸを 16 ﾜｰﾄﾞ (1 ﾜｰﾄﾞ=32bit)に分割し、ﾜｰﾄﾞ単位でｵﾍﾟﾚｰｼｮﾝを行う。

3-1 準備

(1) 関数 $S^n(X)$

$S^n(X) = (X << n)\ OR\ (X >> 32-n)$ 循環左ｼﾌﾄｵﾍﾟﾚｰｼｮﾝ

(2) 関数 $f_t(B,C,D)$

$f_t(B,C,D) = (B\ AND\ C)\ OR\ ((NOT\ B)\ AND\ D)$ $(0 <= t <= 19)$

$f_t(B,C,D) = B\ XOR\ C\ XOR\ D$ $(20 <= t <= 39)$

$f_t(B,C,D) = (B\ AND\ C)\ OR\ (B\ AND\ D)\ OR\ (C\ AND\ D)$ $(40 <= t <= 59)$

$f_t(B,C,D) = B\ XOR\ C\ XOR\ D$ $(60 <= t <= 79)$

(3) 定数 K_t

K_t = 5A827999 $(0 <= t <= 19)$

K_t = 6ED9EBA1 $(20 <= t <= 39)$

K_t = 8F1BBCDC $(40 <= t <= 59)$

K_t = CA62C1D6 $(60 <= t <= 79)$

(4) ﾌﾞﾛｯｸﾃﾞｰﾀ

ﾌﾞﾛｯｸ → (W_0, W_1, W_2, W_3, W_4, W_5, W_6, W_7, W_8, W_9, W_{10}, W_{11}, W_{12}, W_{13}, W_{14}, W_{15})

↑先頭ﾃﾞｰﾀ

3-2 ｱﾙｺﾞﾘｽﾞﾑ 1

Step. 1

H_0 = 67452301

H_1 = EFCDAB89

H_2 = 98BADCFE

H_3 = 10325476

H_4 = C3D2E1F0

Step. 2

For t=16 to 79 let $W_t = S^1(W_{t-3}\ XOR\ W_{t-8}\ XOR\ W_{t-14}\ XOR\ W_{t-16})$

Step. 3

Let $A=H_0$, $B=H_1$, $C=H_2$, $D=H_3$, $E=H_4$

Step. 4

For t=0 to 79 do

$TEMP = S^5(A)+f_t(B,C,D)+E+W_t+K_t$

$E=D, D=C, C=S_{30}(B); B=A; A=TEMP$

Step. 5

Let $H_0=H_0+A, H_1=H_1+B, H_2=H_2+C, H_3=H_3+D, H_4=H_4+E$

ﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄ (H_0 H_1 H_2 H_3 H_4)

3-3 ｱﾙｺﾞﾘｽﾞﾑ 2

Step. 1

H_0 = 67452301

H_1 = EFCDAB89

H_2 = 98BADCFE

H_3 = 10325476

H_4 = C3D2E1F0

Step. 2

Let $A=H_0$, $B=H_1$, $C=H_2$, $D=H_3$, $E=H_4$

Step. 3

For t=0 to 79 do

s = t ^ MASK

if(t>=16) $W[s]=S^1(W[(s+13)\text{^}MASK] \text{ XOR } W[(s+8) \text{ AND MASK}] \text{ XOR } W[(s+2)\text{^}MASK] \text{ XOR } W[s])$;

$TEMP = S^5(A)+f_t(B,C,D)+E+W_t+K_t$

$E=D, D=C, C=S_{30}(B)$; $B=A$; $A=TEMP$

Step. 4

Let $H_0=H_0+A, H_1=H_1+B, H_2=H_2+C, H_3=H_3+D, H_4=H_4+E$

ﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄ (H_0 H_1 H_2 H_3 H_4)

3-4 ｱﾙｺﾞﾘｽﾞﾑ比較

ｱﾙｺﾞﾘｽﾞﾑ 1, 2 は同じﾒｯｾｰｼﾞﾀﾞｲｼﾞｪｽﾄを生成するが、ｱﾙｺﾞﾘｽﾞﾑ 2 では 1 に比べて 64Word の記憶領域を節約できる。但し、ｱﾙｺﾞﾘｽﾞﾑ2 Step. 3 で、W のｱﾄﾞﾚｽ計算が複雑になっている。

4. 最後のﾌﾞﾛｯｸの長さを 512bit にする方法

Step. 1

ﾒｯｾｰｼﾞの最後に、'1' を付加する。

Step. 2

ﾒｯｾｰｼﾞの長さ全体が、448bit となるまで、'0' を付加。

Step. 3

最初のﾒｯｾｰｼﾞの長さ(Step. 1 で'1' を付加する前の長さ)を、64bit で表現し、それを付加する。

例　2 進数表現　01100001 01100010 01100011 01100100 01100101
　　16 進数表現　61　62　63　64　65

Step. 1

2 進数表現　01100001 01100010 01100011 01100100 01100101 1
16 進数表現　61　62　63　64　65　8

Step. 2

16 進数表現

61626364 65800000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000

Step. 3

16 進数表現

61626364 65800000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000000
00000000 00000000 00000000 00000028

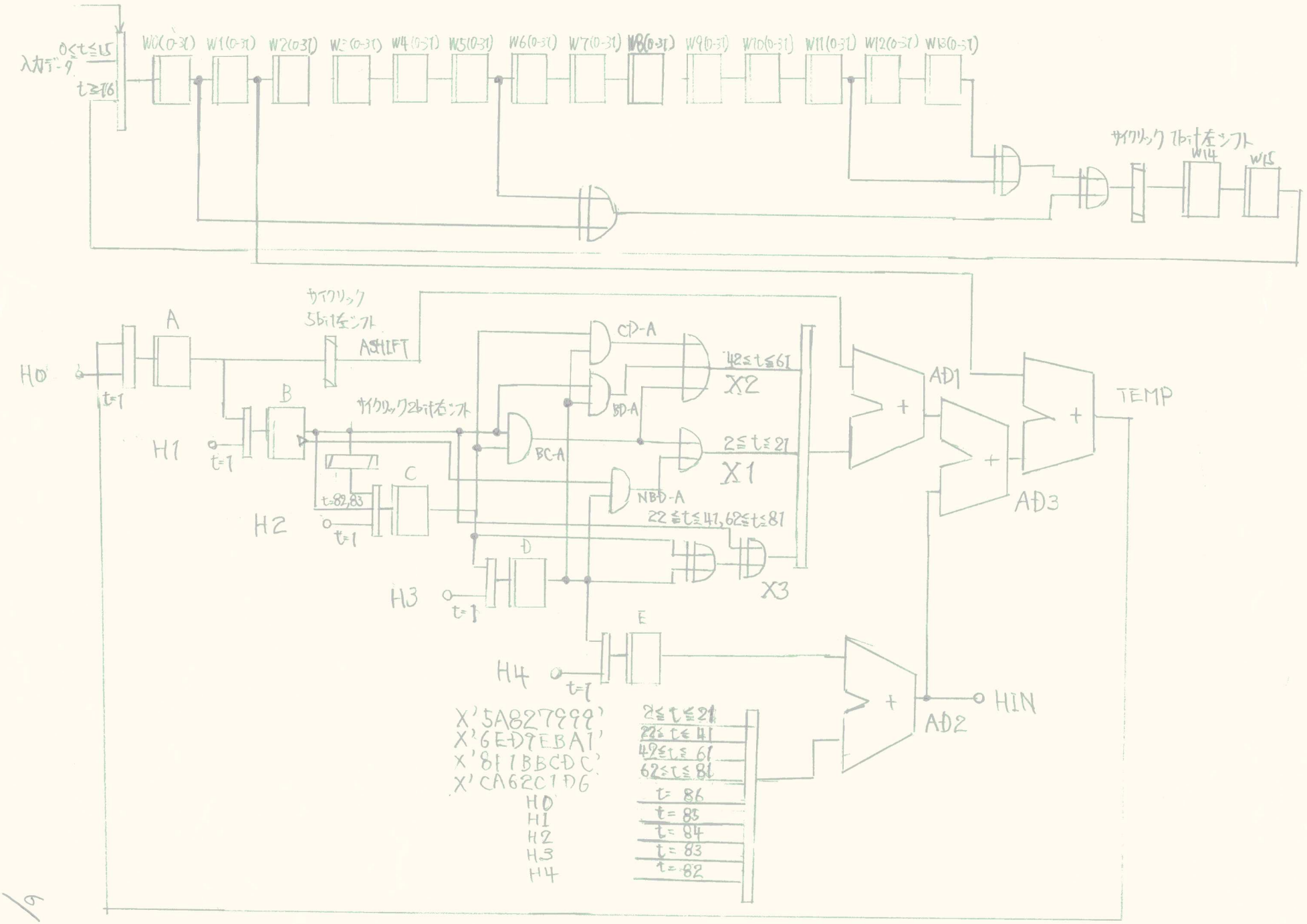
```
#include <stdio.h>
typedef unsigned long int Word;

Word A,B,C,D,E;
Word H0 = 0x67452301;
Word H1 = 0xEFCDAB89;
Word H2 = 0x98BADCFE;
Word H3 = 0x10325476;
Word H4 = 0xC3D2E1F0;
Word W[80];
Word TEMP;
const Word K[80] = {
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6
};

inline Word sn(int n,Word X) {
  return (X << n) | (X >> 32-n);
}

Word ft(int t,Word B,Word C,Word D) {
  if(0<=t && t<=19) {
    return (B & C) | ((~ B) & D);
  }
  if((20<=t && t<=39) || (60<=t && t<=79)) {
    return B ^ C ^ D;
  }
  if(40<=t && t<=59) {
    return (B & C) | (B & D) | (C & D);
  }
  printf("function ft range error. t=%d\n",t);
  exit(-1);
}

void main() {
  int t;
  W[0]  = 0x61626380;
  for(t=1 ; t<15 ; t++) {W[t] = 0;}
  W[15] = 0x00000018;
  for(t=16 ; t<80 ; t++) {
    W[t] = sn(1,W[t-3]^W[t-8]^W[t-14]^W[t-16]);
  }
  A=H0 ; B=H1 ; C=H2 ; D=H3 ; E=H4;

  for(t=0 ; t<80 ; t++) {
    TEMP = sn(5,A) + ft(t,B,C,D) + E + W[t] + K[t];
    E=D ; D=C ; C=sn(30,B); B=A ; A=TEMP;
    printf("t= %2d: %X %X %X %X %X\n",t,A,B,C,D,E);
  }

  H0+=A ; H1+=B ; H2+=C ; H3+=D ; H4+=E ;
  printf("H : %X %X %X %X %X\n",H0,H1,H2,H3,H4);
}
```

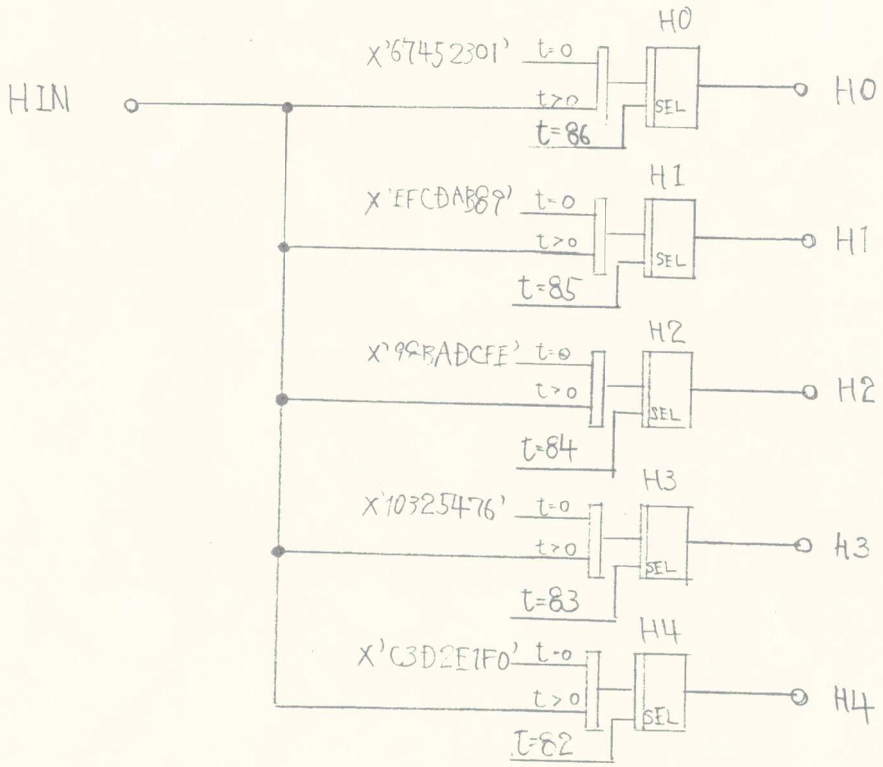
```
t=  0: 116FC33 67452301 7BF36AE2 98BADCFE 10325476
t=  1: 8990536D 116FC33 59D148C0 7BF36AE2 98BADCFE
t=  2: A1390F08 8990536D C045BF0C 59D148C0 7BF36AE2
t=  3: CDD8E11B A1390F08 626414DB C045BF0C 59D148C0
t=  4: CFD499DE CDD8E11B 284E43C2 626414DB C045BF0C
t=  5: 3FC7CA40 CFD499DE F3763846 284E43C2 626414DB
t=  6: 993E30C1 3FC7CA40 B3F52677 F3763846 284E43C2
t=  7: 9E8C07D4 993E30C1 FF1F290 B3F52677 F3763846
t=  8: 4B6AE328 9E8C07D4 664F8C30 FF1F290 B3F52677
t=  9: 8351F929 4B6AE328 27A301F5 664F8C30 FF1F290
t= 10: FBDA9E89 8351F929 12DAB8CA 27A301F5 664F8C30
t= 11: 63188FE4 FBDA9E89 60D47E4A 12DAB8CA 27A301F5
t= 12: 4607B664 63188FE4 7EF6A7A2 60D47E4A 12DAB8CA
t= 13: 9128F695 4607B664 18C623F9 7EF6A7A2 60D47E4A
t= 14: 196BEE77 9128F695 1181ED99 18C623F9 7EF6A7A2
t= 15: 20BDD62F 196BEE77 644A3DA5 1181ED99 18C623F9
t= 16: 4E925823 20BDD62F C65AFB9D 644A3DA5 1181ED99
t= 17: 82AA6728 4E925823 C82F758B C65AFB9D 644A3DA5
t= 18: DC64901D 82AA6728 D3A49608 C82F758B C65AFB9D
t= 19: FD9E1D7D DC64901D 20AA99CA D3A49608 C82F758B
t= 20: 1A37B0CA FD9E1D7D 77192407 20AA99CA D3A49608
t= 21: 33A23BFC 1A37B0CA 7F67875F 77192407 20AA99CA
t= 22: 21283486 33A23BFC 868DEC32 7F67875F 77192407
t= 23: D541F12D 21283486 CE88EFF 868DEC32 7F67875F
t= 24: C7567DC6 D541F12D 884A0D21 CE88EFF 868DEC32
t= 25: 48413BA4 C7567DC6 75507C4B 884A0D21 CE88EFF
t= 26: BE35FBD5 48413BA4 B1D59F71 75507C4B 884A0D21
t= 27: 4AA84D97 BE35FBD5 12104EE9 B1D59F71 75507C4B
t= 28: 8370B52E 4AA84D97 6F8D7EF5 12104EE9 B1D59F71
t= 29: C5FBAF5D 8370B52E D2AA1365 6F8D7EF5 12104EE9
t= 30: 1267B407 C5FBAF5D A0DC2D4B D2AA1365 6F8D7EF5
t= 31: 3B845D33 1267B407 717EEBD7 A0DC2D4B D2AA1365
t= 32: 46FAA0A 3B845D33 C499ED01 717EEBD7 A0DC2D4B
t= 33: 2C0EBC11 46FAA0A CEE1174C C499ED01 717EEBD7
t= 34: 21796AD4 2C0EBC11 811BEA82 CEE1174C C499ED01
t= 35: DCBBB0CB 21796AD4 4B03AF04 811BEA82 CEE1174C
t= 36: F511FD8 DCBBB0CB 85E5AB5 4B03AF04 811BEA82
t= 37: DC63973F F511FD8 F72EEC32 85E5AB5 4B03AF04
t= 38: 4C986405 DC63973F 3D447F6 F72EEC32 85E5AB5
t= 39: 32DE1CBA 4C986405 F718E5CF 3D447F6 F72EEC32
t= 40: FC87DEDF 32DE1CBA 53261901 F718E5CF 3D447F6
t= 41: 970A0D5C FC87DEDF 8CB7872E 53261901 F718E5CF
t= 42: 7F193DC5 970A0D5C FF21F7B7 8CB7872E 53261901
t= 43: EE1B1AAF 7F193DC5 25C28357 FF21F7B7 8CB7872E
t= 44: 40F28E09 EE1B1AAF 5FC64F71 25C28357 FF21F7B7
t= 45: 1C51E1F2 40F28E09 FB86C6AB 5FC64F71 25C28357
t= 46: A01B846C 1C51E1F2 503CA382 FB86C6AB 5FC64F71
t= 47: BEAD02CA A01B846C 8714787C 503CA382 FB86C6AB
t= 48: BAF39337 BEAD02CA 2806E11B 8714787C 503CA382
t= 49: 120731C5 BAF39337 AFAB40B2 2806E11B 8714787C
t= 50: 641DB2CE 120731C5 EEBCE4CD AFAB40B2 2806E11B
t= 51: 3847AD66 641DB2CE 4481CC71 EEBCE4CD AFAB40B2
t= 52: E490436D 3847AD66 99076CB3 4481CC71 EEBCE4CD
t= 53: 27E9F1D8 E490436D 8E11EB59 99076CB3 4481CC71
t= 54: 7B71F76D 27E9F1D8 792410DB 8E11EB59 99076CB3
t= 55: 5E6456AF 7B71F76D 9FA7C76 792410DB 8E11EB59
t= 56: C846093F 5E6456AF 5EDC7DDB 9FA7C76 792410DB
t= 57: D262FF50 C846093F D79915AB 5EDC7DDB 9FA7C76
t= 58: 9D785FD D262FF50 F211824F D79915AB 5EDC7DDB
t= 59: 3F52DE5A 9D785FD 3498BFD4 F211824F D79915AB
t= 60: D756C147 3F52DE5A 4275E17F 3498BFD4 F211824F
t= 61: 548C9CB2 D756C147 8FD4B796 4275E17F 3498BFD4
t= 62: B66C020B 548C9CB2 F5D5B051 8FD4B796 4275E17F
t= 63: 6B61C9E1 B66C020B 9523272C F5D5B051 8FD4B796
t= 64: 19DFA7AC 6B61C9E1 ED9B0082 9523272C F5D5B051
t= 65: 101655F9 19DFA7AC 5AD87278 ED9B0082 9523272C
t= 66: C3DF2B4 101655F9 677E9EB 5AD87278 ED9B0082
t= 67: 78DD4D2B C3DF2B4 4405957E 677E9EB 5AD87278
t= 68: 497093C0 78DD4D2B 30F7CAD 4405957E 677E9EB
```



```
t= 69: 3F2588C2 497093C0 DE37534A 30F7CAD 4405957E
t= 70: C199F8C7 3F2588C2 125C24F0 DE37534A 30F7CAD
t= 71: 39859DE7 C199F8C7 8FC96230 125C24F0 DE37534A
t= 72: EDB42DE4 39859DE7 F0667E31 8FC96230 125C24F0
t= 73: 11793F6F EDB42DE4 CE616779 F0667E31 8FC96230
t= 74: 5EE76897 11793F6F 3B6D0B79 CE616779 F0667E31
t= 75: 53F7DAB7 5EE76897 C45E4FDB 3B6D0B79 CE616779
t= 76: A079B7D9 63F7DAB7 D7B9DA25 C45E4FDB 3B6D0B79
t= 77: 860D21CC A079B7D9 D8FDF6AD D7E9DA25 C45E4FDB
t= 78: 5738D5E1 860D21CC 681E6DF6 D8FDF6AD D7B9DA25
t= 79: 42541B35 5738D5E1 21834873 681E6DF6 D8FDF6AD
H : A9993E36 4706816A BA3E2571 7850C26C 9CD0D89D
```

H0 H1 H2 H3 H4


入力データ
0≦t≦15
t≧16
W0(0-31)
W1(0-31)
W2(0-31)
W3(0-31)
W4(0-31)
W5(0-31)
W6(0-31)
W7(0-31)
W8(0-31)
W9(0-31)
W10(0-31)
W11(0-31)
W12(0-31)
W13(0-31)
サイクリック 1bit左シフト
W14
W15
H0
H1
H2
H3
H4
A
B
C
D
E
t=1
サイクリック
3bit左シフト
ASHIFT
サイクリック2bit右シフト
t=82,83
CD-A
BD-A
BC-A
NBD-A
42≦t≦61
X2
2≦t≦21
X1
22≦t≦41,62≦t≦81
X3
AD1
AD2
AD3
TEMP
HIN
X'5A827999'
X'6ED7EBA1'
X'8F1BBCDC'
X'CA62C1D6'
2≦t≦21
22≦t≦41
42≦t≦61
62≦t≦81
t=86
t=85
t=84
t=83
t=82


HIN
H0
X'67452301'
t=0
t>0
t=86
SEL
H0
H1
X'EFCDAB89'
t=0
t>0
t=85
SEL
H1
H2
X'98BADCFE'
t=0
t>0
t=84
SEL
H2
H3
X'10325476'
t=0
t>0
t=83
SEL
H3
H4
X'C3D2E1F0'
t=0
t>0
t=82
SEL
H4

```
##
## SHA basic                Rev.0  97.10.13
##


if( 0<=t && t<=15 ) {
        W0 := SID[t]
} else {
        W0 := W15
}

W1 := W0
W2 := W1
W3 := W2
W4 := W3
W5 := W4
W6 := W5
W7 := W6
W8 := W7
W9 := W8
W10 := W9
W11 := W10
W12 := W11
W13 := W12

XW = W0 ^ W5 ^ W11 ^ W13
W14 := (XW << 1) | (XW >> 31)           # 1bit left cyclic shift
W15 := W14

ASHIFT = (A << 5) | (A >> 27)           # 5bit left cyclic shift

BC-A = B & C
BD-A = B & D
CD-A = C & D
NBD-A =  (~B) & D

X1 = BC-A | NBD-A
X2 = BC-A | BD-A  | CD-A
X3 = B ^ C ^ D

AD1 = 0

if( 2<=t && t<=21 ) {
        AD1 = X1 + ASHIFT
}
if( 42<=t && t<=61 ) {
        AD1 = X2 + ASHIFT
}
if( (22<=t && t<=41) || (62<=t && t<=81) ) {
        AD1 = X3 + ASHIFT
}

if( 2<=t && t<=21 ) {
        AD2 = 0x5A827999 + E
}
if( 22<=t && t<=41 ) {
        AD2 = 0x6ED9EBA1 + E
}
if( 42<=t && t<=61 ) {
        AD2 = 0x8F1BBCDC + E
}
if( 62<=t && t<=81 ) {
        AD2 = 0xCA62C1D6 + E
}
if( t==86 ) {
        AD2 = H0 + E
}
if( t==85 ) {
        AD2 = H1 + E
}
if( t==84 ) {
        AD2 = H2 + E
}
if( t==83 ) {
        AD2 = H3 + E
}
if( t==82 ) {
        AD2 = H4 + E
```

```
}

AD3 = AD1 + AD2
TEMP = AD3 + W1
HIN = AD2

if( t==1 ) {
        A := H0
        B := H1
        C := H2
        D := H3
        E := H4
} else {
        A := TEMP
        B := A
        C := (t==82||t==83) ? B : ((B<<30)|(B>>2))# 2bit right cyclic shift
        D := C
        E := D
}

if( t==0 ) {
        H0 := 0x67452301
        H1 := 0xEFCDAB89
        H2 := 0x98BADCFE
        H3 := 0x10325476
        H4 := 0xC3D2E1F0
}

if( t==86 ) {
        H0 := HIN
}

if( t==85 ) {
        H1 := HIN
}

if( t==84 ) {
        H2 := HIN
}

if( t==83 ) {
        H3 := HIN
}

if( t==82 ) {
        H4 := HIN
}

## counter
T = t
t = t + 1
```

T	A	B	C	D	E	ASHIFT	X1	X2	X3	AD1	AD2	AD3	TEMP	H0	H1	H2	H3	H4

0000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0001	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0002	67452301	efcdab89	98badcfe	10325476	c3d2e1f0	e8a4602c	98badcfe	98badcfe	67452301	815f3d2a	1e555b89	9fb498b3	0116fc33	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0003	0116fc33	67452301	7bf36ae2	98badcfe	10325476	22df8660	fbfbfefe	7bf36ae2	840c951d	1edb855e	6ab4ce0f	8990536d	8990536d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0004	8990536d	0116fc33	59d148c0	7bf36ae2	98badcfe	320a6db1	7bf14ac0	59d368e2	2334de11	adfbb871	f33d5697	a1390f08	a1390f08	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0005	a1390f08	8990536d	c045bf0c	59d148c0	7bf36ae2	2721e114	d0411b8c	c9d15b4c	1004a4a1	f762fca0	d675e47b	cdd8e11b	cdd8e11b	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0006	cdd8e11b	a1390f08	626414db	c045bf0c	59d148c0	bb1c2379	6064b40c	e0651f08	0318a4df	1b80d785	b453c259	cfd499de	cfd499de	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0007	cfd499de	cdd8e11b	284e43c2	626414db	c045bf0c	fa933bd9	2a6c55c2	684c41db	87f2b602	24ff919b	1ac838a5	3fc7ca40	3fc7ca40	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0008	3fc7ca40	cfd499de	f3763846	284e43c2	626414db	f8f94807	e35e5a46	eb5619c6	14ece25a	dc57a24d	bce68e74	993e30c1	993e30c1	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0009	993e30c1	3fc7ca40	b3f52677	f3763846	284e43c2	27c61833	f3f53246	b3f72a46	7f44d471	1bbb4a79	82d0bd5b	9e8c07d4	9e8c07d4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000a	9e8c07d4	993e30c1	0ff1f290	b3f52677	f3763846	d180fa93	2bf136b6	9bf532d1	253ae426	fd723149	4df8b1df	4b6ae328	4b6ae328	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000b	4b6ae328	9e8c07d4	664f8c30	0ff1f290	b3f52677	6d5c6509	077df410	0ecd8690	f7327974	74da5919	0e77a010	8351f929	8351f929	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000c	8351f929	4b6ae328	27a301f5	664f8c30	0ff1f290	6a3f2530	27270d30	676b8130	0a866eed	91663260	6a746c29	fbda9e89	fbda9e89	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000d	fbda9e89	8351f929	12dab8ca	27a301f5	664f8c30	7b53d13f	26f2b8dc	03d3b9e9	b6284016	a2468a1b	c0d205c9	63188fe4	63188fe4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000e	63188fe4	fbda9e89	60d47e4a	12dab8ca	27a301f5	6311fc8c	60d03e4a	72dabeca	89d45809	c3e23ad6	82257b8e	4607b664	4607b664	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000f	4607b664	63188fe4	7ef6a7a2	60d47e4a	12dab8ca	c0f6cc88	62d4f7aa	62d4afe2	7d3a560c	23cbc432	6d5d3263	9128f695	9128f695	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0010	9128f695	4607b664	18c623f9	7ef6a7a2	60d47e4a	251ed2b2	38f623e2	5ec5a7e0	2037323f	5e14f694	bb56f7e3	196bee77	196bee77	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0011	196bee77	9128f695	1181ed99	18c623f9	7ef6a7a2	2d7dcee3	19c6e5f9	1180e799	986f38f5	4744b4dc	d979213b	20bdd617	20bdd62f	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0012	20bdd62f	196bee77	644a3da5	1181ed99	18c623f9	17bac5e4	00ca2dad	114bedb5	6ca03e4b	1884f391	73489d92	8bcd9123	4e925823	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0013	4e925823	20bdd62f	c65afb9d	644a3da5	1181ed99	d24b0469	445afb8d	645affad	82ad1017	16a5fff6	6c046732	82aa6728	82aa6728	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0014	82aa6728	4e925823	c82f758b	c65afb9d	644a3da5	554ce510	c84af39f	ce1a798b	40e7d635	1d97d8af	beccb73e	dc648fed	dc64901d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0015	dc64901d	82aa6728	d3a49608	c82f758b	c65afb9d	8c9203bb	caa5168b	c2ae7708	992184ab	57371a46	20dd7536	78148f7c	fd9e1d7d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0016	fd9e1d7d	dc64901d	20aa99ca	d3a49608	c82f758b	b3c3afbf	03a09608	d0a49008	2f6a9fdf	e32e4f9e	3709612c	1a37b0ca	1a37b0ca	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0017	1a37b0ca	fd9e1d7d	77192407	20aa99ca	d3a49608	46f61943	75388487	759a1d4f	aa2da0b0	f123b9f3	427e81a9	33a23b9c	33a23bfc	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0018	33a23bfc	1a37b0ca	7f67875f	77192407	20aa99ca	74477f86	7f2f844f	7f37a44f	12491392	86909318	8f84856b	16151883	21283486	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0019	21283486	33a23bfc	868dec32	7f67875f	77192407	250690c4	4ec5ac33	37a7af7e	ca485091	ef4ee155	e5f30fa8	d541f0fd	d541f12d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001a	d541f12d	21283486	0ce88eff	868dec32	7f67875f	a83e25ba	86adccb6	04a8acb6	ab4d564b	538b7c05	ee417300	41ccef05	c7567dc6	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001b	c7567dc6	d541f12d	884a0d21	0ce88eff	868dec32	eacfb8d8	88e80ff3	8c488d2d	51e372f3	3cb32bcb	f567d7d3	321b039e	48413ba4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001c	48413ba4	c7567dc6	75507c4b	884a0d21	0ce88eff	08277489	4d587c63	c5527d43	3a4c0cac	42738135	7bc27aa0	be35fbd5	be35fbd5	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001d	be35fbd5	48413ba4	b1d59f71	75507c4b	884a0d21	c6bf7ab7	35515f6b	71513f61	8cc4d89e	53845355	f723f8c2	4aa84c17	4aa84d97	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001e	4aa84d97	be35fbd5	12104ee9	b1d59f71	75507c4b	5509b2e9	13d04ee1	b215dff1	1df02a4d	72f9dd36	e42a67ec	57244522	8370b52e	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001f	8370b52e	4aa84d97	6f8d7ef5	12104ee9	b1d59f71	6e16a5d0	5a984efd	4a884ef5	37357d8b	a54c235b	20af8b12	c5fbae6d	c5fbaf5d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0020	c5fbaf5d	8370b52e	d2aa1365	6f8d7ef5	12104ee9	bf75ebb8	eead5bf5	c3a83765	3e57d8be	fdcdc476	80ea3a8a	7eb7ff00	1267b407	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0021	1267b407	c5fbaf5d	a0dc2d4b	d2aa1365	6f8d7ef5	4cf680e2	92d83d69	c0fa2f4d	b78d9173	04841255	de676a96	e2eb7ceb	3b845d33	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0022	3b845d33	1267b407	717eebd7	a0dc2d4b	d2aa1365	708ba667	b0fea94f	307ead47	c3c5729b	34511902	4183ff06	75d51808	046faa0a	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0023	046faa0a	3b845d33	c499ed01	717eebd7	a0dc2d4b	8df54140	40faefc5	719ced13	8e635be5	1c589d25	0fb618ec	2c0eb611	2c0ebc11	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0024	2c0ebc11	046faa0a	cee1174c	c499ed01	717eebd7	81d78225	c4f14709	c4e9af08	0e175047	8feed26c	e058d778	7047a9e4	21796ad4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0025	21796ad4	2c0ebc11	811bea82	cee1174c	c499ed01	2f2d5a84	c2ebab4c	8c0bbe00	63f441df	93219c63	3373d8a2	c6957505	dcbbb0cb	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0026	dcbbb0cb	21796ad4	4b03af04	811bea82	cee1174c	9776197b	8103aa06	011bea84	eb612f52	82d748cd	3dbb02ed	c0924bba	0f511fd8	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0027	0f511fd8	dcbbb0cb	085e5ab5	4b03af04	811bea82	ea23fb01	0b1a1f85	481bba85	9fe6457a	8a0a407b	eff5d623	7a00169e	dc63973f	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0028	dc63973f	0f511fd8	f72eec32	085e5ab5	4b03af04	8c72e7fb	070e4c35	0f5e5eb0	f021a95f	7c94915a	b9dd9aa5	36722bff	4c986405	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0029	4c986405	dc63973f	03d447f6	f72eec32	085e5ab5	930c80a9	234c6f36	d766c736	28993cfb	bba5bda4	77384656	32de03fa	32de1cba	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002a	32de1cba	4c986405	f718e5cf	03d447f6	f72eec32	5bc39746	475c67f7	479865c7	b854c63c	a35bfd0d	864aa90e	29a6a61b	fc87dedf	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002b	fc87dedf	32de1cba	53261901	f718e5cf	03d447f6	90fbdbff	d706f945	731e1d8b	95e0e074	0419f98a	92f004d2	9709fe5c	970a0d5c	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002c	970a0d5c	fc87dedf	8cb7872e	53261901	f718e5cf	e141ab92	8fa7870e	dca79f0f	231640f0	bde94aa1	8634a2ab	441ded4c	7f193dc5	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002d	7f193dc5	970a0d5c	ff21f7b7	8cb7872e	53261901	e327b8af	9fb58736	9f23873e	e49c7dc5	824b3fed	e241d5dd	648d15ca	ee1b1aaf	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002e	ee1b1aaf	7f193dc5	25c28357	ff21f7b7	8cb7872e	c36355fd	a520c377	7f01b7d7	a5fa4925	42650dd4	1bd3440a	5e3851de	40f28e09	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002f	40f28e09	ee1b1aaf	5fc64f71	25c28357	ff21f7b7	1e51c128	4fc28b71	6fc20b77	941fd689	8e13cc9f	8e3db493	1c518132	1c51e1f2	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0030	1c51e1f2	40f28e09	fb86c6ab	5fc64f71	25c28357	8a3c3e43	5f86c779	5bc6ce29	e4b207d3	e6030c6c	b4de4033	9ae14c9f	a01b846c	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0031	a01b846c	1c51e1f2	503ca382	fb86c6ab	5fc64f71	03708d94	f396a78b	5814e3a2	b7eb84db	5b857136	eee20c4d	4a677d83	bead02ca	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0032	bead02ca	a01b846c	8714787c	503ca382	fb86c6ab	d5a05957	d03423ee	801ca06c	77335f92	55bcf9c3	8aa28387	e05f7d4a	baf39337	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0033	baf39337	bead02ca	2806e11b	8714787c	503ca382	5e7266f7	2914783e	ae04605a	11bf9bad	0c76c751	df58605e	ebcf27af	120731c5	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0034	120731c5	baf39337	afab40b2	2806e11b	8714787c	40e638a2	aaa7603a	aaa3c133	3d5e329e	eb89f9d5	16303558	01ba2f2d	641db2ce	67452301	efcdab89	98badcfe	10325476	c3d2e1f0

1-01

```
0035 641db2ce 120731c5 eebce4cd afab40b2 2806e11b 83b659cc afac60f7 aeaf60c5 531095ba 3265ba91 b7229df7 e9885888 3847ad66 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0036 3847ad66 641db2ce 4481cc71 eebce4cd afab40b2 08f5acc7 cea1c441 649de4cd ce209a72 6d939194 3ec6fd8e ac5a8f22 e490436d 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0037 e490436d 3847ad66 99076cb3 4481cc71 eebce4cd 92086dbc 5c876c33 1807ec73 e5c10da4 aa105a2f 7dd8a1a9 27e8fbd8 27e9f1d8 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0038 27e9f1d8 e490436d 8e11eb59 99076cb3 4481cc71 fd3e3b04 9d176fdb 8c116b79 f386c487 894fa67d d39d894d 5ced2fca 7b71f76d 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0039 7b71f76d 27e9f1d8 792410db 8e11eb59 99076cb3 6e3eedaf a9301ad9 2f21f1d9 d0dc0a5a 9d60df88 2823298f c5840917 5e6456af 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003a 5e6456af 7b71f76d 09fa7c76 792410db 8e11eb59 cc8ad5eb 097474f6 7970747f 0baf9bc0 45fb4a6a 1d2da835 6328f29f c846093f 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003b c846093f 5e6456af 5edc7ddb 09fa7c76 792410db 08c127f9 5fde7cdb 5efc7cff 09425702 67bda4f8 083fcdb7 6ffd72af d262ff50 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003c d262ff50 c846093f d79915ab 5edc7ddb 09fa7c76 4c5fea1a d69875eb dedc1dbb 4103614f 2b3c07d5 99163952 c4524127 09d785fd 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003d 09d785fd d262ff50 f211824f d79915ab 5edc7ddb 3af0bfa1 d79982eb d211974b f7ea68b4 0d0256ec edf83ab7 fafa91a3 3f52de5a 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003e 3f52de5a 09d785fd 3498bfd4 f211824f d79915ab ea5bcb47 f29087d6 309187dd cf5eb866 b9ba83ad a1fbd781 5bb65b2e d756c147 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003f d756c147 3f52de5a 4275e17f 3498bfd4 f211824f ead828fa 02d8e1de 3650ff5e 49bf80f1 3497a9eb bc744425 f10bee10 548c9cb2 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0040 548c9cb2 d756c147 8fd4b796 4275e17f 3498bfd4 9193964a 8775a13e c754e157 1af797ae ac8b2df8 fefb81aa ab86afa2 b66c020b 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0041 b66c020b 548c9cb2 f5d5b051 8fd4b796 4275e17f cd804176 dfd4b314 d5d4b492 2e8d9b75 fc0ddceb 0cd8a355 08e68040 6b61c9e1 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0042 6b61c9e1 b66c020b 9523272c f5d5b051 8fd4b796 6c393c2d d5b1b258 b5652209 d69a9576 42d3d1a3 5a37796c 9d0b4b0f 19dfa7ac 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0043 19dfa7ac 6b61c9e1 ed9b0082 9523272c f5d5b051 3bf4f583 fd03268c ed2301a0 13d9ee4f 4fcee3d2 c0387227 100755f9 101655f9 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0044 101655f9 19dfa7ac 5ad87278 ed9b0082 9523272c 02cabf22 fcd8222a 59db22a8 ae9cd556 b1679478 5f85e902 10ed7d7a 0c3df2b4 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0045 0c3df2b4 101655f9 0677e9eb 5ad87278 ed9b0082 87be5681 4ade63e9 125671f9 4cb9ce6a d47824eb b7fdc258 8c75e743 78dd4d2b 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0046 78dd4d2b 0c3df2b4 4405957e 0677e9eb 5ad87278 1ba9a56f 0647997f 0435f1fe 4e4f8e21 69f93390 253b344e 8f3467de 497093c0 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0047 497093c0 78dd4d2b 030f7cad 4405957e 0677e9eb 2e127809 040ddc7d 400d5d2f 3fd7a4f8 6dea1d01 d0daabc1 3ec4c8c2 3f2588c2 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0048 3f2588c2 497093c0 de37534a 030f7cad 4405957e e4b11847 4a3f7f6d 4b3753c8 9448bc27 78f9d46e 0e685754 87622bc2 c199f8c7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0049 c199f8c7 3f2588c2 125c24f0 de37534a 030f7cad 333f18f8 d21653c8 1e3500c2 f34eff78 268e1870 cd723e83 f40056f3 39859de7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004a 39859de7 c199f8c7 8fc96230 125c24f0 de37534a 30b3bce7 93cd6430 83d960f0 5c0cbe07 8cc07aee a89a1520 355a900e edb42de4 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004b edb42de4 39859de7 f0667e31 8fc96230 125c24f0 b685bc9d b64c7e31 b9c57e31 462a81e6 fcb03e83 dcbee5c6 d96f2549 11793f6f 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004c 11793f6f edb42de4 ce616779 f0667e31 8fc96230 2f27ede2 dc627771 ec646f71 d3b334ac 02db228e 5a2c2406 5d074694 5ee76897 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004d 5ee76897 11793f6f 3b6d0b79 ce616779 f0667e31 dced12eb df694b79 1b692f79 e475536f c162665a bac94007 7c2ba661 63f7dab7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004e 63f7dab7 5ee76897 c45e4fdb 3b6d0b79 ce616779 7efb56ec 654e4bfb 5e6f4bdb a1d42c35 20cf8321 98c4294f b993ac70 a079b7d9 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004f a079b7d9 63f7dab7 d7b9da25 c45e4fdb 3b6d0b79 0f36fb34 c7b9df6d c7ffdab7 70104f49 7f474a7d 05cfcd4f 851717cc 860d21cc 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0050 860d21cc a079b7d9 d8fdf6ad d7b9da25 c45e4fdb c1a43990 d7f9fead d0f9f6ad af3d9b51 70e1d4e1 8ec111b1 ffa2e692 5738d5e1 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0051 5738d5e1 860d21cc 681e6df6 d8fdf6ad d7b9da25 e71abc2a 58fcf7e5 c81d65ec 36eeba97 1e0976c1 a21c9bfb c02612bc 42541b35 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0052 42541b35 5738d5e1 21834873 681e6df6 d8fdf6ad 4a8366a8 29066877 611a4df3 1ea5f064 00000000 9cd0d89d 9cd0d89d 1b28557f 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0053 1b28557f 42541b35 5738d5e1 21834873 681e6df6 650aafe3 63935163 43105971 34ef86a7 00000000 7850c26c 7850c26c 803fe36f 67452301 efcdab89 98badcfe 10325476 9cd0d89d
0054 803fe36f 1b28557f 42541b35 5738d5e1 21834873 07fc6df0 461091b5 53385575 0e449bab 00000000 ba3e2571 ba3e2571 3f830eb6 67452301 efcdab89 98badcfe 7850c26c 9cd0d89d
0055 3f830eb6 803fe36f c6ca155f 42541b35 5738d5e1 f061d6c7 c24a195f c25e137f 04a1ed05 00000000 4706816a 4706816a 32405c22 67452301 efcdab89 ba3e2571 7850c26c 9cd0d89d
0056 32405c22 3f830eb6 e00ff8db c6ca155f 42541b35 480b8446 e04b19db e68b1cdf 1946e332 00000000 a9993e36 a9993e36 6b9ed750 67452301 4706816a ba3e2571 7850c26c 9cd0d89d
0057 6b9ed750 32405c22 8fe0c3ad e00ff8db c6ca155f 73daea0d c24fe0f9 a240d8ab 5daf6754 00000000 a9993e36 a9993e36 2a480999 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
0058 2a480999 6b9ed750 8c901708 8fe0c3ad e00ff8db 49013325 8cf017ad 8f90d708 68ee03f5 00000000 a9993e36 a9993e36 271e087e a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
0059 271e087e 2a480999 1ae7b5d4 8c901708 8fe0c3ad e3c10fc4 8ed01790 0ac01598 bc3fab45 00000000 a9993e36 a9993e36 24e2d998 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005a 24e2d998 271e087e 4a920266 1ae7b5d4 8c901708 9c5b3304 1af3b5e6 0a960076 776bbfcc 00000000 a9993e36 a9993e36 38194ede a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005b 38194ede 24e2d998 89c7821f 4a920266 1ae7b5d4 0329dbc7 4ad2827e 08c2821e e7b759e1 00000000 a9993e36 a9993e36 f4f4c8ad a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005c f4f4c8ad 38194ede 0938b666 89c7821f 4a920266 9e9915be 89de8647 0919865e b8e67aa7 00000000 a9993e36 a9993e36 dbaff4d0 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005d dbaff4d0 f4f4c8ad 8e0653b7 0938b666 89c7821f 75fe9a1b 8d0c76e7 8c34d2a7 73ca2d7c 00000000 a9993e36 a9993e36 aea126c3 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005e aea126c3 dbaff4d0 7d3d322b 8e0653b7 0938b666 d424d875 5d2d3327 df2f72b3 2894954c 00000000 a9993e36 a9993e36 19f52ccc a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
005f 19f52ccc aea126c3 36ebfd34 7d3d322b 8e0653b7 3ea59983 77bd3428 3ea93623 e577e9dc 00000000 a9993e36 a9993e36 0a5a3d36 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```

Oct 14 1997 08:31

siml.res

T	W 0	W 1	W 2	W 3	W 4	W 5	W 6	W 7	W 8	W 9	W 10	W 11	W 12	W 13	W 14	W 15
0000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0001	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700	00000000
0002	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700
0003	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0004	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0005	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0006	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700	00000000
0007	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700
0008	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0009	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000	00000000
000a	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000	00000000
000b	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	00000000	00000000	00000000
000c	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	00000000	c2c4c700	00000000
000d	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	61626380	00000000	c2c4c700	00000000
000e	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700
000f	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	c2c4c700
0010	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000030	00000000
0011	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	85898e01	00000030
0012	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	85898e01
0013	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000060	00000000
0014	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	0b131c03	00000060
0015	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000030	0b131c03
0016	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	00000000	85898ec1	00000030
0017	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	16263806	85898ec1
0018	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000000	00000000	16263806
0019	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	00000000	00000180	00000000
001a	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	00000000	2c4c700c	00000180
001b	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	00000000	000000f0	2c4c700c
001c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	00000000	93afb507	000000f0
001d	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	c2c4c700	00000018	5898e048	93afb507
001e	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	00000018	8e9a9202	5898e048
001f	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	00000600	8e9a9202
0020	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	00000030	00000000	00000600
0021	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	85898e01	b131c0f0	00000600
0022	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	00000000	16263bc6	b131c0f0
0023	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	00000060	4ebed41e	16263bc6
0024	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	0b131c03	626380a1	4ebed41e
0025	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	00000030	16263806	626380a1
0026	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	85898ec1	000018c0	16263806
0027	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	16263806	d2e138c4	000018c0
0028	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	00000000	00000f00	d2e138c4
0029	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	00000180	3afb5079	00000f00
002a	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	2c4c700c	898e04e5	3afb5079
002b	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000000f0	e2ba3c2b	898e04e5
002c	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	93afb507	000060c0	e2ba3c2b
002d	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	5898e048	053a37cd	000060c0
002e	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	8e9a9202	74458547	053a37cd
002f	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	00000600	da9415ed	74458547
0030	74458547	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	b131c0f0	26380a16	da9415ed
0031	da9415ed	74458547	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	16263bc6	626383a1	26380a16
0032	26380a16	da9415ed	74458547	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	4ebed41e	4ebf54de	626383a1
0033	626383a1	26380a16	da9415ed	74458547	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	626380a1	3835b44b	4ebf54de
0034	4ebf54de	626383a1	26380a16	da9415ed	74458547	053a37cd	000060c0	e2ba3c2b	898e04e5	3afb5079	00000f00	d2e138c4	000018c0	16263806	0000f600	3835b44b

```
0035 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 3afb5079 00000f00 d2e138c4 000018c0 1e84c7a3 0000f500
0036 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 3afb5079 00000f00 d2e138c4 98e04d98 1e84c7a3
0037 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 3afb5079 00000f00 651d16a0 98e04d98
0038 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 3afb5079 00000f00 651d16a0
0039 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 3afb5079 62658ca1
003a 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 898e04e5 458544d6
003b 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 e2ba3c2b 44584cb7
003c 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 000060c0 7ba06619
003d 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547 053a37cd 6380aea2
003e 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed 74458547
003f 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16 da9415ed
0040 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1 26380a16
0041 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de 626383a1
0042 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b 4ebf54de
0043 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600 3835b44b
0044 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3 0000f600
0045 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98 1e84c7a3
0046 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0 98e04d98
0047 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1 651d16a0
0048 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6 62658ca1
0049 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7 458544d6
004a 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619 44584cb7
004b 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2 7ba06619
004c e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269 6380aea2
004d e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1 0ae55269
004e 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d 627b49a1
004f 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000 7cd45c9d
0050 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a 000f0000
0051 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8 fb50753a
0052 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2 ec6765e8
0053 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000 ba3c2be2
0054 eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05 0060c000
0055 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4 3a37cd05
0056 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6 458546f4
0057 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26 b8599dd6
0058 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203 380a1a26
0059 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456 01e02203
005a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69 e7cc3456
005b 3216b69a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00 e6e60b69
005c 0507e88d 3216b69a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f 00f60a00
005d 705bee96 0507e88d 3216b69a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879 5795ef4f
005e 60c0ff00 705bee96 0507e88d 3216b69a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2 822e0879
005f a28362d0 60c0ff00 705bee96 0507e88d 3216b69a 4b5b8a77 8e8010a8 7b499b62 7d84ca48 80aecb63 c205991a eb39dab8 8544e945 07ef2103 7e577ce2
```

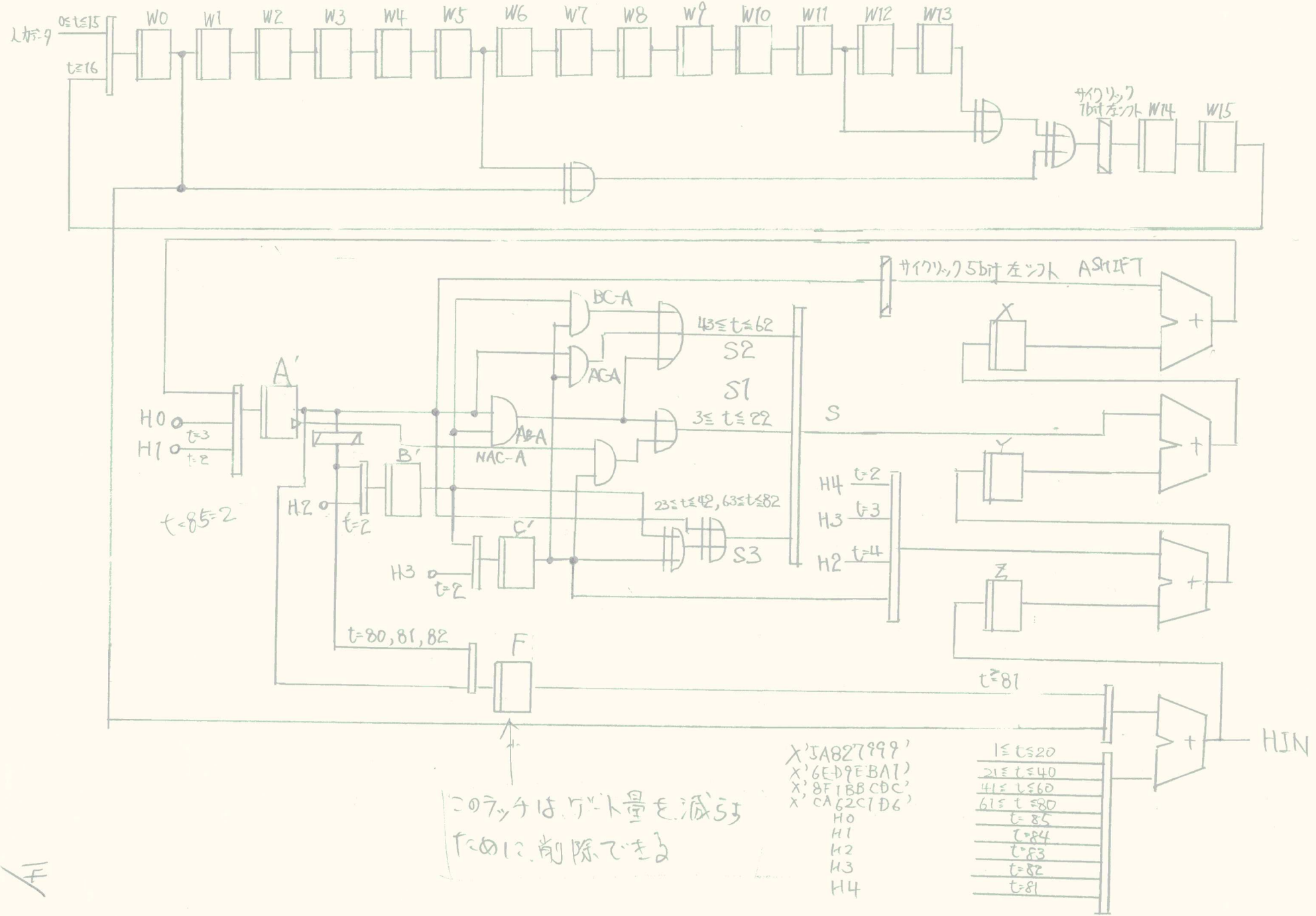
```
#include <stdio.h>
typedef unsigned long int Word;

Word A,B,C,D,E;
Word H0 = 0x67452301;
Word H1 = 0xEFCDAB89;
Word H2 = 0x98BADCFE;
Word H3 = 0x10325476;
Word H4 = 0xC3D2E1F0;
Word W[80];
Word TEMP;
const Word K[80] = {
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,  0x5A827999,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,  0x6ED9EBA1,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,  0x8F1BBCDC,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,
  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6,  0xCA62C1D6
};

inline Word sn(int n,Word X) {
  return (X << n) | (X >> 32-n);
}

Word ft(int t,Word B,Word C,Word D) {
  if(0<=t && t<=19) {
    return (B & C) | ((~ B) & D);
  }
  if((20<=t && t<=39) || (60<=t && t<=79)) {
    return B ^ C ^ D;
  }
  if(40<=t && t<=59) {
    return (B & C) | (B & D) | (C & D);
  }
  return 0xffffffff ;
}

void main() {
  int t;
  Word X,Y,Z;

  W[0]  = 0x61626380;
  for(t=1 ; t<15 ; t++) {W[t] = 0;}
  W[15] = 0x00000018;
  for(t=16 ; t<80 ; t++) {
    W[t] = sn(1,W[t-3]^W[t-8]^W[t-14]^W[t-16]);
  }

  Z = W[0] + K[0];
  for(t=-2 ; t<81 ; t++) {
    TEMP = sn(5,A) + X;
    X = (t==-1) ? ft(t+1,H1,H2,H3) + Y :
        (t==0)  ? ft(t+1,H0,sn(30,H1),H2) + Y :
        (t==1)  ? ft(t+1,A,sn(30,H0),sn(30,H1)) + Y : ft(t+1,A,B,C) + Y;
    Y = (t==-2) ? H4 + Z:
        (t==-1) ? H3 + Z :
        (t==0 ) ? H2 + Z : C + Z;
    Z = W[t+3] + K[t+3];
    C=B ; B = sn(30,A) ; A = (t==-2) ? H1 : (t==-1) ? H0 : TEMP;
    printf("t= %2d: A=%8x B=%8x C=%8x X=%8x Y=%8x Z=%8x TEMP=%8x\n",t,A,B,C,X,Y,Z,TEMP);
    H4 += (t==76) ? B : 0;
    H3 += (t==77) ? B : 0;
    H2 += (t==78) ? B : 0;
    H1 += (t==78) ? A : 0;
    H0 += (t==79) ? A : 0;
  }
  printf("H : %8x %8x %8x %8x %8x\n",H0,H1,H2,H3,H4);
}
```

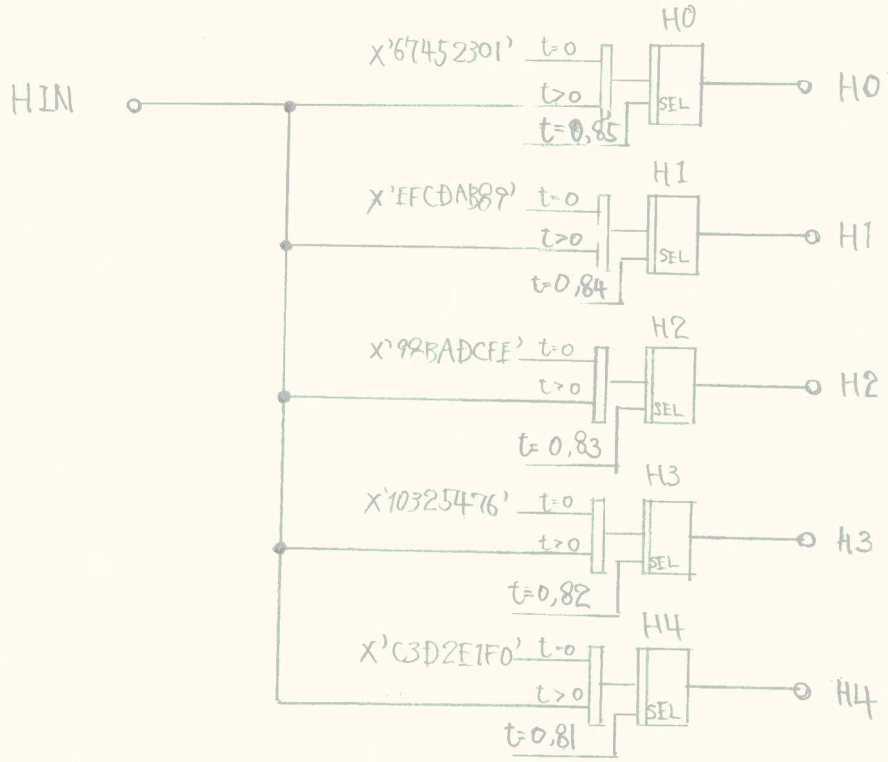
```
t= -2: A=efcdab89 B=       0 C=       0 X= 805b27e Y=7fb7bf09 Z=5a827999 TEMP=    1020
t= -1: A=67452301 B=7bf36ae2 C=       0 X=18729c07 Y=6ab4ce0f Z=5a827999 TEMP= 1bb23bb
t=  0: A= 116fc33 B=59d148c0 C=7bf36ae2 X=66b0cd0d Y=f33d5697 Z=5a827999 TEMP= 116fc33
t=  1: A=8990536d B=c045bf0c C=59d148c0 X=6f2ea157 Y=d675e47b Z=5a827999 TEMP=8990536d
t=  2: A=a1390f08 B=626414db C=c045bf0c X=a6b70007 Y=b453c259 Z=5a827999 TEMP=a1390f08
t=  3: A=cdd8e11b B=284e43c2 C=626414db X=14b87665 Y=1ac838a5 Z=5a827999 TEMP=cdd8e11b
t=  4: A=cfd499de B=f3763846 C=284e43c2 X=45348e67 Y=bce68e74 Z=5a827999 TEMP=cfd499de
t=  5: A=3fc7ca40 B=b3f52677 C=f3763846 X=a044e8ba Y=82d0bd5b Z=5a827999 TEMP=3fc7ca40
t=  6: A=993e30c1 B= ff1f290 C=b3f52677 X=76c5efa1 Y=4df8b1df Z=5a827999 TEMP=993e30c1
t=  7: A=9e8c07d4 B=564f8c30 C= ff1f290 X=79e9e895 Y= e77a010 Z=5a827999 TEMP=9e8c07d4
t=  8: A=4b6ae328 B=27a301f5 C=664f8c30 X=15f59420 Y=6a746c29 Z=5a827999 TEMP=4b6ae328
t=  9: A=8351f929 B=12dab8ca C=27a301f5 X=919b7959 Y=c0d205c9 Z=5a827999 TEMP=8351f929
t= 10: A=fbda9e89 B=50d47e4a C=12dab8ca X=e7c4bea5 Y=82257b8e Z=5a827999 TEMP=fbda9e89
t= 11: A=63188fe4 B=7ef6a7a2 C=60d47e4a X=e2f5b9d8 Y=6d5d3263 Z=5a827999 TEMP=63188fe4
t= 12: A=4607b664 B=18c623f9 C=7ef6a7a2 X=d0322a0d Y=bb56f7e3 Z=5a8279b1 TEMP=4607b664
t= 13: A=9128f695 B=1181ed99 C=18c623f9 X=f44d1bc5 Y=d9792153 Z=1d474099 TEMP=9128f695
t= 14: A=196bee77 B=544a3da5 C=1181ed99 X=f340074c Y=360d6492 Z=5a827999 TEMP=196bee77
t= 15: A=20bdd62f B=c65afb9d C=644a3da5 X=36d7923f Y=6c046732 Z=5a8279c9 TEMP=20bdd62f
t= 16: A=4e925823 B=c82f758b C=c65afb9d X=b05f62bf Y=beccb76e Z=e00c079a TEMP=4e925823
t= 17: A=82aa6728 B=d3a49608 C=c82f758b X=8717ab0d Y=a6670337 Z=6ed9eba1 TEMP=82aa6728
t= 18: A=dc64901d B=20aa99ca C=d3a49608 X=710c19c2 Y=3709612c Z=6ed9ec01 TEMP=dc64901d
t= 19: A=fd9e1d7d B=77192407 C=20aa99ca X=6674010b Y=427e8209 Z=79ed07a4 TEMP=fd9e1d7d
t= 20: A=1a37b0ca B=7f67875f C=77192407 X=ecac22b9 Y=9a97a16e Z=6ed9ebd1 TEMP=1a37b0ca
t= 21: A=33a23bfc B=868dec32 C=7f67875f X=ace0b500 Y=e5f30fd8 Z=f4637a62 TEMP=33a23bfc
t= 22: A=21283486 B= ce88eff C=868dec32 X=b03b6069 Y=73cb01c1 Z=850023a7 TEMP=21283486
t= 23: A=d541f12d B=884a0d21 C= ce88eff X=1f18580c Y= b8e0fd9 Z=6ed9eba1 TEMP=d541f12d
t= 24: A=c7567dc6 B=75507c4b C=884a0d21 X=5d7182cc Y=7bc27aa0 Z=6ed9ed21 TEMP=c7567dc6
t= 25: A=48413ba4 B=b1d59f71 C=75507c4b X=b60e874c Y=f723fa42 Z=9b265bad TEMP=48413ba4
t= 26: A=be35fbd5 B=12104ee9 C=b1d59f71 X=83e8d2e0 Y=1076d7f8 Z=6ed9ec91 TEMP=be35fbd5
t= 27: A=4aa84d97 B=5f8d7ef5 C=12104ee9 X=2e670245 Y=20af8c02 Z= 289a0a8 TEMP=4aa84d97
t= 28: A=8370b52e B=d2aa1365 C=6f8d7ef5 X=57e5098d Y=1499ef91 Z=c772cbe9 TEMP=8370b52e
t= 29: A=c5fbaf5d B=a0dc2d4b C=d2aa1365 X=52f1c84f Y=37004ade Z=fd747da3 TEMP=c5fbaf5d
t= 30: A=1267b407 B=717eebd7 C=a0dc2d4b X=ee8ddc51 Y=d01e9108 Z=6ed9f1a1 TEMP=1267b407
t= 31: A=3b845d33 B=c499ed01 C=717eebd7 X=93e403a3 Y= fb61eec Z=200bac91 TEMP=3b845d33
t= 32: A= 46faa0a B=ceel174c C=c499ed01 X=9e197ad1 Y=918a9868 Z=85002767 TEMP= 46faa0a
t= 33: A=2c0ebc11 B=811bea82 C=ceel174c X=9fa1e8af Y=499a1468 Z=bd98bfbf TEMP=2c0ebc11
t= 34: A=21796ad4 B=4b03af04 C=811bea82 X=ad8e5647 Y=8c79d70b Z=d13d6c42 TEMP=21796ad4
t= 35: A=dcbbb0cb B= 85e5ab5 C=4b03af04 X=77db065d Y=525956c4 Z=850023a7 TEMP=dcbbb0cb
t= 36: A= f511fd8 B=f72eec32 C= 85e5ab5 X=f23f9c3e Y=d003d2ab Z=6eda0461 TEMP= f511fd8
t= 37: A=dc63973f B= 3d447f6 C=f72eec32 X=c0257c0a Y=77385f16 Z=61fcf5a0 TEMP=dc63973f
t= 38: A=4c986405 B=f718e5cf C= 3d447f6 X=9fd19c11 Y=592be1d2 Z=8f1bcbdc TEMP=4c986405
t= 39: A=32de1cba B=53261901 C=f718e5cf X=a0c44799 Y=92f013d2 Z=ca170d55 TEMP=32de1cba
t= 40: A=fc87dedf B=8cb7872e C=53261901 X= 60e315d Y=c12ff324 Z=18a9c1c1 TEMP=fc87dedf
t= 41: A=970a0d5c B=ff21f7b7 C=8cb7872e X=9dd79233 Y=6bcfdac2 Z=71d5f907 TEMP=970a0d5c
t= 42: A=7f193dc5 B=25c28357 C=ff21f7b7 X= af36200 Y=fe8d8035 Z=8f1c1d9c TEMP=7f193dc5
t= 43: A=ee1b1aaf B=5fc64f71 C=25c28357 X=7d8f380c Y=8e3e1553 Z=9455f4a9 TEMP=ee1b1aaf
t= 44: A=40f28e09 B=fb86c6ab C=5fc64f71 X=fe0020ca Y=ba187800 Z= 3614223 TEMP=40f28e09
t= 45: A=1c51e1f2 B=503ca382 C=fb86c6ab X=15df4629 Y=63279194 Z=69afd2c9 TEMP=1c51e1f2
t= 46: A=a01b846c B=8714787c C=503ca382 X=bb3c7536 Y=65369974 Z=b553c6f2 TEMP=a01b846c
t= 47: A=bead02ca B=2806e11b C=8714787c X=e55339e0 Y= 5906a74 Z=f17f407d TEMP=bead02ca
t= 48: A=baf39337 B=afab40b2 C=2806e11b X=b394cace Y=7893b8f9 Z=dddb11ba TEMP=baf39337
t= 49: A=120731c5 B=eebce4cd C=afab40b2 X=23377a2c Y= 5e1f2d5 Z=c7517127 TEMP=120731c5
t= 50: A=641db2ce B=4481cc71 C=eebce4cd X=b491539a Y=76fcb1d9 Z=8f1cb2dc TEMP=641db2ce
t= 51: A=3847ad66 B=99076cb3 C=4481cc71 X=db9a96a6 Y=7dd997a9 Z=ada0847f TEMP=3847ad66
t= 52: A=e490436d B=8e11eb59 C=99076cb3 X=95e1841c Y=f22250f0 Z=27fc0a74 TEMP=e490436d
t= 53: A=27e9f1d8 B=792410db C=8e11eb59 X=7e33bc69 Y=c1037727 Z=f438d37c TEMP=27e9f1d8
t= 54: A=7b71f76d B= 9fa7c76 C=792410db X=f0256900 Y=824abed5 Z=f181497d TEMP=7b71f76d
t= 55: A=5e6456af B=5edc7ddb C= 9fa7c76 X=fbbb3354 Y=6aa55a58 Z=d4a101b2 TEMP=5e6456af
t= 56: A=c846093f B=d79915ab C=5edc7ddb X=c9a1d757 Y=de9b7e28 Z=d3740993 TEMP=c846093f
t= 57: A=d262ff50 B=f211824f C=d79915ab X=bd779be3 Y=3250876e Z=460327ef TEMP=d262ff50
t= 58: A= 9d785fd B=3498bfd4 C=f211824f X= 4621eb9 Y=1d9c3d9a Z=2de37078 TEMP= 9d785fd
t= 59: A=3f52de5a B=4275e17f C=3498bfd4 X=ecfaf600 Y=1ff4f2c7 Z=d548143f TEMP=3f52de5a
t= 60: A=d756c147 B=8fd4b796 C=4275e17f X=69b473b8 Y= 9e0d413 Z=2cde0b77 TEMP=d756c147
t= 61: A=548c9cb2 B=f5d5b051 C=8fd4b796 X=24d86bc1 Y=6f53ecf6 Z=47371e73 TEMP=548c9cb2
t= 62: A=b66c020b B=9523272c C=f5d5b051 X=9de1886b Y=d70bd609 Z=ca71c1d6 TEMP=b66c020b
t= 63: A=6b61c9e1 B=ed9b0082 C=9523272c X=ada66b7f Y=c0477227 Z=c5b33710 TEMP=6b61c9e1
t= 64: A=19dfa7ac B=5ad87278 C=ed9b0082 X=d4216075 Y=5ad65e3c Z=b6ca27be TEMP=19dfa7ac
t= 65: A=101655f9 B= 677e9eb C=5ad87278 X= 9733392 Y=a4652840 Z=849eedb8 TEMP=101655f9
t= 66: A= c3df2b4 B=4405957e C= 677e9eb X=f11ef6aa Y=df776030 Z=cac381d6 TEMP= c3df2b4
```



```
t= 67: A=78dd4d2b B= 30f7cad C=4405957e X=2dc6ee51 Y=d13b6bc1 Z= 49a8edb TEMP=78dd4d2b
t= 68: A=497093c0 B=de37534a C= 30f7cad X=111310b9 Y=48a02459 Z= fe808ca TEMP=497093c0
t= 69: A=3f2588c2 B=125c24f0 C=de37534a X=dce8e080 Y=12f78577 Z=82bc5fac TEMP=3f2588c2
t= 70: A=c199f8c7 B=8fc96230 C=125c24f0 X= 64684ef Y=60f3b2f6 Z= 26cdbfc TEMP=c199f8c7
t= 71: A=39859de7 B=f0667e31 C=8fc96230 X=bd0070fd Y=14c900ec Z=cc42e3d9 TEMP=39859de7
t= 72: A=edb42de4 B=ce616779 C=f0667e31 X=5af382d2 Y=5c0c4609 Z=b22ef62c TEMP=edb42de4
t= 73: A=11793f6f B=3b6d0b79 C=ce616779 X=2fbf7ab5 Y=a295745d Z=b148cd3f TEMP=11793f6f
t= 74: A=5ee76897 B=c45e4fdb C=3b6d0b79 X=870ac7cc Y=7faa34b8 Z=cb58cbd6 TEMP=5ee76897
t= 75: A=63f7dab7 B=d7b9da25 C=c45e4fdb X=217e60ed Y= 6c5d74f Z=21f8b125 TEMP=63f7dab7
t= 76: A=a079b7d9 B=d8fdf6ad C=d7b9da25 X=76d62698 Y=e6570100 Z=4c90ca4f TEMP=a079b7d9
t= 77: A=860d21cc B=681e6df6 C=d8fdf6ad X=95949c51 Y=244aa474 Z=56e58955 TEMP=860d21cc
t= 78: A=5738d5e1 B=21834873 C=681e6df6 X=5b395f0b Y=2fe38002 Z= c558b53 TEMP=5738d5e1
t= 79: A=42541b35 B=55ce3578 C=21834873 X=2fe38001 Y=7473f949 Z=6f0f18fc TEMP=42541b35
t= 80: A=7a66e6a9 B=509506cd C=55ce3578 X=7473f948 Y=9092616f Z=dd641b7b TEMP=7a66e6a9
H : a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```

83. ディレイ改善版


入力データ
0≦t≦15
t≧16
W0
W1
W2
W3
W4
W5
W6
W7
W8
W9
W10
W11
W12
W13
サイクリック 16bit 左シフト
W14
W15
サイクリック 5bit 左シフト ASHIFT
BC-A
AC-A
43≦t≦62
S2
S1
3≦t≦22
A-A
NAC-A
23≦t≦42, 63≦t≦82
S3
S
A'
B'
C'
H0
H1
t=3
t=2
H2
t=2
H3
t=2
t=85=2
H4 t=2
H3 t=3
H2 t=4
X
Y
Z
t=80, 81, 82
F
t=81
HIN
X'3A827999'
X'6ED9EBA1'
X'8F1BBCDC'
X'CA62C1D6'
H0
H1
H2
H3
H4
1≦t≦20
21≦t≦40
41≦t≦60
61≦t≦80
t=85
t=84
t=83
t=82
t=81
このラッチはゲート量を減らすために削除できる


HIN
H0
X'67452301'
t=0
t>0
t=0,85
SEL
H0
H1
X'EFCDAB89'
t=0
t>0
t=0,84
SEL
H1
H2
X'98BADCFE'
t=0
t>0
t=0,83
SEL
H2
H3
X'10325476'
t=0
t>0
t=0,82
SEL
H3
H4
X'C3D2E1F0'
t=0
t>0
t=0,81
SEL
H4

```
##
## SHA delay                Rev.0  97.11.02
##

W0 := ( 0<=t && t<=15 )? SID[t] : W15

W1 := W0
W2 := W1
W3 := W2
W4 := W3
W5 := W4
W6 := W5
W7 := W6
W8 := W7
W9 := W8
W10 := W9
W11 := W10
W12 := W11
W13 := W12

XW = W0 ^ W5 ^ W11 ^ W13
W14 := (XW << 1) | (XW >> 31)           # 1bit left cyclic shift
W15 := W14

ASHIFT = (A << 5) | (A >> 27)           # 5bit left cyclic shift

AB-A = A & B
BC-A = B & C
AC-A = A & C
NAC-A = (~A) & C

CC = (t==2) ? H4 :
     (t==3) ? H3 :
     (t==4) ? H2 : C

S1 = AB-A | NAC-A
S2 = AB-A | BC-A | AC-A
S3 = A ^ B ^ C
S  = (3<=t  && t<=22) ? S1 :
     (43<=t && t<=62) ? S2 :
     ((23<=t && t<=42) || (63<=t && t<=82)) ? S3 : 0xffffffff

AD1 = ASHIFT + X
X  := S  + Y
Y  := CC  + Z

A := (t==2) ? H1 :
     (t==3) ? H0 : AD1
B := (t==2) ? H2 : ((A<<30)|(A>>2))     # 2bit right cyclic shift
C := (t==2) ? H3 : B

WF = (t>=81) ? F : W0
F  := (t==80 || t==81 || t==82)? ((A<<30)|(A>>2)) : A
K  = ( 1<=t && t<=20) ? 0x5A827999 :
     (21<=t && t<=40) ? 0x6ED9EBA1 :
     (41<=t && t<=60) ? 0x8F1BBCDC :
     (61<=t && t<=80) ? 0xCA62C1D6 :
     ( t==85 )        ? H0         :
     ( t==84 )        ? H1         :
     ( t==83 )        ? H2         :
     ( t==82 )        ? H3         :
     ( t==81 )        ? H4         : 0xffffffff

Z  := WF + K
HIN = WF + K

H0 := (t==0) ? 0x67452301 : (t==85)? HIN : H0;
H1 := (t==0) ? 0xEFCDAB89 : (t==84)? HIN : H1;
H2 := (t==0) ? 0x98BADCFE : (t==83)? HIN : H2;
H3 := (t==0) ? 0x10325476 : (t==82)? HIN : H3;
H4 := (t==0) ? 0xC3D2E1F0 : (t==81)? HIN : H4;

## counter
T = t
t = t + 1
```

T	A	B	C	A SHIFT	X	Y	Z	F	S	S 1	S 2	S 3	A D 1	H 0	H 1	H 2	H 3	H 4

t=3 →

0000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	ffffffff	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000	00000000
0001	00000000	00000000	00000000	00000000	ffffffff	00000000	ffffffff	00000000	ffffffff	00000000	00000000	00000000	ffffffff	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0002	ffffffff	00000000	00000000	ffffffff	ffffffff	ffffffff	bbe4dd19	00000000	ffffffff	00000000	00000000	00000000	ffffffff	ffffffff	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0003	efcdab89	98badcfe	10325476	f9b5713d	ffffffff	7fb7bf09	5a827999	ffffffff	98badcfe	98badcfe	98badcfe	98badcfe	57452301	f9b5713b	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0004	67452301	7bf36ae2	98badcfe	e8a4602c	18729c07	6ab4ce0f	5a827999	efcdab89	fbfbfefe	fbfbfefe	7bf36ae2	840c951d	0116fc33	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0005	0116fc33	59d148c0	7bf36ae2	22df8660	66b0cd0d	f33d5697	5a827999	67452301	7bf14ac0	7bf14ac0	59d368e2	2334de11	8990536d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0006	8990536d	c045bf0c	59d148c0	320a6db1	6f2ea157	d675e47b	5a827999	0116fc33	d0411b8c	d0411b8c	c9d15b4c	1004a4a1	a1390f08	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0007	a1390f08	625414db	c045bf0c	2721e114	a6b70007	b453c259	5a827999	8990536d	6064b40c	6064b40c	e0651f08	0318a4df	cdd8e11b	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0008	cdd8e11b	284e43c2	626414db	bb1c2379	14b87665	1ac838a5	5a827999	a1390f08	2a6c55c2	2a6c55c2	684c41db	87f2b602	cfd499de	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0009	cfd499de	f3763846	284e43c2	fa933bd9	45348e67	bce68e74	5a827999	cdd8e11b	e35e5a46	e35e5a46	eb5619c6	14ece25a	3fc7ca40	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000a	3fc7ca40	b3f52677	f3763846	f8f94807	a044e8ba	82d0bd5b	5a827999	cfd499de	f3f53246	f3f53246	b3f72a46	7f44d471	993e30c1	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000b	993e30c1	0ff1f290	b3f52677	27c61833	76c5efa1	4df8b1df	5a827999	3fc7ca40	2bf136b6	2bf136b6	9bf532d1	253ae426	9e8c07d4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000c	9e8c07d4	664f8c30	0ff1f290	d180fa93	79e9e895	0e77a010	5a827999	993e30c1	077df410	077df410	0ecd8690	f7327974	4b6ae328	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000d	4b6ae328	27a301f5	664f8c30	6d5c6509	15f59420	6a746c29	5a827999	9e8c07d4	27270d30	27270d30	676b8130	0a866eed	8351f929	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000e	8351f929	12dab8ca	27a301f5	6a3f2530	919b7959	c0d205c9	5a827999	4b6ae328	26f2b8dc	26f2b8dc	03d3b9e9	b6284016	fbda9e89	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
000f	fbda9e89	60d47e4a	12dab8ca	7b53d13f	e7c4bea5	82257b8e	5a827999	8351f929	60d03e4a	60d03e4a	72dabeca	89d45809	63188fe4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0010	63188fe4	7ef6a7a2	60d47e4a	6311fc8c	e2f5b9d8	6d5d3263	5a827999	fbda9e89	62d4f7aa	62d4f7aa	62d4afe2	7d3a560c	4607b664	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0011	4607b664	18c623f9	7ef6a7a2	c0f6cc88	d0322a0d	bb56f7e3	5a8279b1	63188fe4	38f623e2	38f623e2	5ec6a7e0	2037323f	9128f695	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0012	9128f695	1181ed99	18c623f9	251ed2b2	f44d1bc5	d9792153	1d474099	4607b664	19c6e5f9	19c6e5f9	1180e799	986f38f5	196bee77	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0013	196bee77	644a3da5	1181ed99	2d7dcee3	f340074c	360d6492	5a827999	9128f695	00ca2dad	00ca2dad	114bedb5	6ca03e4b	20bdd62f	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0014	20bdd62f	c65afb9d	644a3da5	17bac5e4	36d7923f	6c046732	5a8279c9	196bee77	445afb8d	445afb8d	645affad	82ad1017	4e925823	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0015	4e925823	c82f758b	c65afb9d	d24b0469	b05f62bf	beccb76e	e00c079a	20bdd62f	c84af39f	c84af39f	ce1a798b	40e7d635	82aa6728	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0016	82aa6728	d3a49608	c82f758b	554ce510	8717ab0d	a6670337	6ed9eba1	4e925823	caa5168b	caa5168b	c2ae7708	992184ab	dc64901d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0017	dc64901d	20aa99ca	d3a49608	8c9203bb	710c19c2	3709612c	6ed9ec01	82aa6728	2f6a9fdf	03a09608	d0a49008	2f6a9fdf	fd9e1d7d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0018	fd9e1d7d	77192407	20aa99ca	b3c3afbf	6674010b	427e8209	79ed07a4	dc64901d	aa2da0b0	75388487	759a1d4f	aa2da0b0	1a37b0ca	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0019	1a37b0ca	7f67875f	77192407	46f61943	ecac22b9	9a97a16e	6ed9ebd1	fd9e1d7d	12491392	7f2f844f	7f37a44f	12491392	33a23bfc	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001a	33a23bfc	868dec32	7f67875f	74477f86	ace0b500	e5f30fd8	f4637a62	1a37b0ca	ca485091	4ec5ac33	37a7af7e	ca485091	21283486	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001b	21283486	0ce88eff	868dec32	250690c4	b03b6069	73cb01c1	850023a7	33a23bfc	ab4d564b	86adccb6	04a8acb6	ab4d564b	d541f12d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001c	d541f12d	884a0d21	0ce88eff	a83e25ba	1f18580c	0b8e0fd9	6ed9eba1	21283486	51e372f3	88e80ff3	8c488d2d	51e372f3	c7567dc6	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001d	c7567dc6	75507c4b	884a0d21	eacfb8d8	5d7182cc	7bc27aa0	6ed9ed21	d541f12d	3a4c0cac	4d587c63	c5527d43	3a4c0cac	48413ba4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001e	48413ba4	b1d59f71	75507c4b	08277489	b60e874c	f723fa42	9b265bad	c7567dc6	8cc4d89e	35515f6b	71513f61	8cc4d89e	be35fbd5	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
001f	be35fbd5	12104ee9	b1d59f71	c6bf7ab7	83e8d2e0	1076d7f8	6ed9ec91	48413ba4	1df02a4d	13d04ee1	b215dff1	1df02a4d	4aa84d97	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0020	4aa84d97	6f8d7ef5	12104ee9	5509b2e9	2e670245	20af8c02	0289a0a8	be35fbd5	37357d8b	5a984efd	4a884ef5	37357d8b	8370b52e	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0021	8370b52e	d2aa1365	6f8d7ef5	6e16a5d0	57e5098d	1499ef91	c772cbe9	4aa84d97	3e57d8be	eead5bf5	c3a83765	3e57d8be	c5fbaf5d	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0022	c5fbaf5d	a0dc2d4b	d2aa1365	bf75ebb8	52f1c84f	37004ade	fd747da3	8370b52e	b78d9173	92d83d69	c0fa2f4d	b78d9173	1267b407	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0023	1267b407	717eebd7	a0dc2d4b	4cf680e2	ee8ddc51	d01e9108	6ed9f1a1	c5fbaf5d	c3c5729b	b0fea94f	307ead47	c3c5729b	3b845d33	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0024	3b845d33	c499ed01	717eebd7	708ba667	93e403a3	0fb61eec	200bac91	1267b407	8e635be5	40faefc5	719ced13	8e635be5	046faa0a	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0025	046faa0a	cee1174c	c499ed01	8df54140	9e197ad1	918a9868	85002767	3b845d33	0e175047	c4f14709	c4e9af08	0e175047	2c0ebc11	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0026	2c0ebc11	811bea82	cee1174c	81d78225	9fa1e8af	499a1468	bd98bfbf	046faa0a	63f441df	c2ebab4c	8c0bbe00	63f441df	21796ad4	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0027	21796ad4	4b03af04	811bea82	2f2d5a84	ad8e5647	8c79d70b	d13d6c42	2c0ebc11	eb612f52	8103aa06	011bea84	eb612f52	dcbbb0cb	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0028	dcbbb0cb	085e5ab5	4b03af04	9776197b	77db065d	525956c4	850023a7	21796ad4	9fe6457a	0b1a1f85	481bba85	9fe6457a	0f511fd8	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0029	0f511fd8	f72eec32	085e5ab5	ea23fb01	f23f9c3e	d003d2ab	6eda0461	dcbbb0cb	f021a95f	070e4c35	0f5e5eb0	f021a95f	dc63973f	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002a	dc63973f	03d447f6	f72eec32	8c72e7fb	c0257c0a	77385f16	61fcf5a0	0f511fd8	28993cfb	234c6f36	d766c736	28993cfb	4c986405	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002b	4c986405	f718e5cf	03d447f6	930c80a9	9fd19c11	592be1d2	8f1bcbdc	dc63973f	479865c7	475c67f7	479865c7	b854c63c	32de1cba	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002c	32de1cba	53261901	f718e5cf	5bc39746	a0c44799	92f013d2	ca170d55	4c986405	731e1d8b	d706f945	731e1d8b	96e0e074	fc87dedf	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002d	fc87dedf	8cb7872e	53261901	90fbdbff	060e315d	c12ff324	18a9c1c1	32de1cba	dca79f0f	8fa7870e	dca79f0f	231640f0	970a0d5c	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002e	970a0d5c	ff21f7b7	8cb7872e	e141ab92	9dd79233	6bcfdac2	71d5f907	fc87dedf	9f23873e	9fb58736	9f23873e	e49c7dc5	7f193dc5	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
002f	7f193dc5	25c28357	ff21f7b7	e327b8af	0af36200	fe8d8035	8f1c1d9c	970a0d5c	7f01b7d7	a520c377	7f01b7d7	a5fa4925	ee1b1aaf	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0030	ee1b1aaf	5fc64f71	25c28357	c36355fd	7d8f380c	8e3e1553	9455f4a9	7f193dc5	6fc20b77	4fc28b71	6fc20b77	941fd689	40f28e09	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0031	40f28e09	fb86c6ab	5fc64f71	1e51c128	fe0020ca	ba187800	03614223	ee1b1aaf	5bc6ce29	5f86c779	5bc6ce29	e4b207d3	1c51e1f2	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0032	1c51e1f2	503ca382	fb86c6ab	8a3c3e43	15df4629	63279194	69afd2c9	40f28e09	5814e3a2	f396a78b	5814e3a2	b7eb84db	a01b846c	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0033	a01b846c	8714787c	503ca382	03708d94	bb3c7536	65369974	b553c6f2	1c51e1f2	801ca06c	d03423ee	801ca06c	77335f92	bead02ca	67452301	efcdab89	98badcfe	10325476	c3d2e1f0
0034	bead02ca	2806e11b	8714787c	d5a05957	e55339e0	05906a74	f17f407d	a01b846c	ae04605a	2914783e	ae04605a	11bf9bad	baf39337	67452301	efcdab89	98badcfe	10325476	c3d2e1f0

```
0035 baf39337 afab40b2 2806e11b 5e7266f7 b394cace 7893b8f9 dddb11ba bead02ca aaa3c133 aaa7603a aaa3c133 3d5e329e 120731c5 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0036 120731c5 eebce4cd afab40b2 40e638a2 23377a2c 05e1f2d5 c7517127 baf39337 aeaf60c5 afac60f7 aeaf60c5 531095ba 641db2ce 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0037 641db2ce 4481cc71 eebce4cd 83b659cc b491539a 76fcb1d9 8f1cb2dc 120731c5 649de4cd cea1c441 649de4cd ce209a72 3847ad66 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0038 3847ad66 99076cb3 4481cc71 08f5acc7 db9a96a6 7dd997a9 ada0847f 641db2ce 1807ec73 5c876c33 1807ec73 e5c10da4 e490436d 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0039 e490436d 8e11eb59 99076cb3 92086dbc 95e1841c f22250f0 27fc0a74 3847ad66 8c116b79 9d176fdb 8c116b79 f386c487 27e9f1d8 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003a 27e9f1d8 792410db 8e11eb59 fd3e3b04 7e33bc69 c1037727 f438d37c e490436d 2f21f1d9 a9301ad9 2f21f1d9 d0dc0a5a 7b71f76d 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003b 7b71f76d 09fa7c76 792410db 6e3eedaf f0256900 824abed5 f181497d 27e9f1d8 7970747f 097474f6 7970747f 0baf9bc0 5e6456af 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003c 5e6456af 5edc7ddb 09fa7c76 cc8ad5eb fbbb3354 6aa55a58 d4a101b2 7b71f76d 5efc7cff 5fde7cdb 5efc7cff 09425702 c846093f 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003d c846093f d79915ab 5edc7ddb 08c127f9 c9a1d757 de9b7e28 d3740993 5e6456af dedc1dbb d69875eb dedc1dbb 4103614f d262ff50 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003e d262ff50 f211824f d79915ab 4c5fea1a bd779be3 3250876e 460327ef c846093f d211974b d79982eb d211974b f7ea68b4 09d785fd 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
003f 09d785fd 3498bfd4 f211824f 3af0bfa1 04621eb9 1d9c3d9a 2de37078 d262ff50 cf5eb866 f29087d6 309187dd cf5eb866 3f52de5a 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0040 3f52de5a 4275e17f 3498bfd4 ea5bcb47 ecfaf600 1ff4f2c7 d548143f 09d785fd 49bf80f1 02d8e1de 3650ff5e 49bf80f1 d756c147 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0041 d756c147 8fd4b796 4275e17f ead828fa 69b473b8 09e0d413 2cde0b77 3f52de5a 1af797ae 8775a13e c754e157 1af797ae 548c9cb2 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0042 548c9cb2 f5d5b051 8fd4b796 9193964a 24d86bc1 6f53ecf6 47371e73 d756c147 2e8d9b75 dfd4b314 d5d4b492 2e8d9b75 b66c020b 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0043 b66c020b 9523272c f5d5b051 cd804176 9de1886b d70bd609 ca71c1d6 548c9cb2 d69a9576 d5b1b258 b5652209 d69a9576 6b61c9e1 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0044 6b61c9e1 ed9b0082 9523272c 6c393c2d ada66b7f c0477227 c5b33710 b66c020b 13d9ee4f fd03268c ed2301a0 13d9ee4f 19dfa7ac 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0045 19dfa7ac 5ad87278 ed9b0082 3bf4f583 d4216076 5ad65e3c b6ca27be 6b61c9e1 ae9cd556 fcd8222a 59db22a8 ae9cd556 101655f9 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0046 101655f9 0677e9eb 5ad87278 02cabf22 09733392 a4652840 849eedb8 19dfa7ac 4cb9ce6a 4ade63e9 125671f9 4cb9ce6a 0c3df2b4 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0047 0c3df2b4 4405957e 0677e9eb 87be5681 f11ef6aa df776030 cac381d6 101655f9 4e4f8e21 0647997f 0435f1fe 4e4f8e21 78dd4d2b 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0048 78dd4d2b 030f7cad 4405957e 1ba9a56f 2dc6ee51 d13b6bc1 049a8edb 0c3df2b4 3fd7a4f8 040ddc7d 400d5d2f 3fd7a4f8 497093c0 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0049 497093c0 de37534a 030f7cad 2e127809 111310b9 48a02459 0fe808ca 78dd4d2b 9448bc27 4a3f7f6d 4b3753c8 9448bc27 3f2588c2 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004a 3f2588c2 125c24f0 de37534a e4b11847 dce8e080 12f78577 82bc5fac 497093c0 f34eff78 d21653c8 1e3500c2 f34eff78 c199f8c7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004b c199f8c7 8fc96230 125c24f0 333f18f8 064684ef 60f3b2f6 026cdbfc 3f2588c2 5c0cbe07 93cd6430 83d960f0 5c0cbe07 39859de7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004c 39859de7 f0667e31 8fc96230 30b3bce7 bd0070fd 14c900ec cc42e3d9 c199f8c7 462a81e6 b64c7e31 b9c57e31 462a81e6 edb42de4 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004d edb42de4 ce616779 f0667e31 b685bc9d 5af382d2 5c0c4609 b22ef62c 39859de7 d3b334ac dc627771 ec646f71 d3b334ac 11793f6f 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004e 11793f6f 3b6d0b79 ce616779 2f27ede2 2fbf7ab5 a295745d b148cd3f edb42de4 e475536f df694b79 1b692f79 e475536f 5ee76897 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
004f 5ee76897 c45e4fdb 3b6d0b79 dced12eb 870ac7cc 7faa34b8 cb58cbd6 11793f6f a1d42c35 654e4bfb 5e6f4bdb a1d42c35 63f7dab7 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0050 63f7dab7 d7b9da25 c45e4fdb 7efb56ec 217e60ed 06c5d74f 21f8b125 5ee76897 70104f49 c7b9df6d c7ffdab7 70104f49 a079b7d9 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0051 a079b7d9 d8fdf6ad d7b9da25 0f36fb34 76d62698 e6570100 4c90ca4f d8fdf6ad af3d9b51 d7f9fead d0f9f6ad af3d9b51 860d21cc 67452301 efcdab89 98badcfe 10325476 c3d2e1f0
0052 860d21cc 681e6df6 d8fdf6ad c1a43990 95949c51 244aa474 9cd0d89d 681e6df6 36eeba97 58fcf7e5 c81d65ec 36eeba97 5738d5e1 67452301 efcdab89 98badcfe 10325476 9cd0d89d
0053 5738d5e1 21834873 681e6df6 e71abc2a 5b395f0b 75cecf4a 7850c26c 21834873 ffffffff 29066877 611a4df3 1ea5f064 42541b35 67452301 efcdab89 98badcfe 7850c26c 9cd0d89d
0054 42541b35 55ce3578 21834873 4a8366a8 75cecf49 e06f3062 ba3e2571 5738d5e1 ffffffff 61c75172 41c61971 3619663e c05235f1 67452301 efcdab89 ba3e2571 7850c26c 9cd0d89d
0055 c05235f1 509506cd 55ce3578 0a46be38 e06f3061 dbc16de4 4706816a 42541b35 ffffffff 559c04c9 50d635f9 c5090644 eab5ee99 67452301 4706816a ba3e2571 7850c26c 9cd0d89d
0056 eab5ee99 70148d7c 509506cd 56bdd33d dbc16de3 9cd4b6e2 a9993e36 c05235f1 ffffffff 70148c5c 70958edd ca346528 327f4120 a9993e36 4706816a ba3e2571 7850c26c 9cd0d89d
```