*) MD5 Algorithm & SHA-1

Works on 128 bit

④ 16 iterations

160 bit

20 rounds

⑤ chaining algo.

⇒ For DS we use SHA-1

⇒ SHA-1 is not attacked till now

(Secured Hashing Algorithm)

MD5

⇒ Padding

⇓

⇒ Convert original message (PT) into 64 bit less than the exact multiple of 512.

PT ⇒ 1000 bit ⇒ 1472 (1536 − 64)

472 padding bit

⇒ [Original message] ④ [Padding]

⇓

[Original message | Padding] ④ [Append]

⇓

[O | P | A]

⇓ Multiple of 512

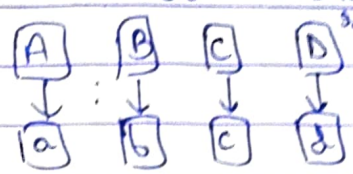
⇒ Divide the message which is to be hashed into a no of blocks of size 512 bit.

Original message (hashed)			
512 bit block	512 bit block	.....	512 bit block

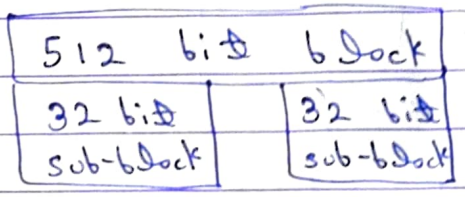
⇒ Initialize the chaining variable

32 bit → A Hex 01 23 45 67
B Hex 89 AB CD EF
C Hex FE DC BA 98
D Hex 76 54 32 10

Copying the chaining variable into small registers

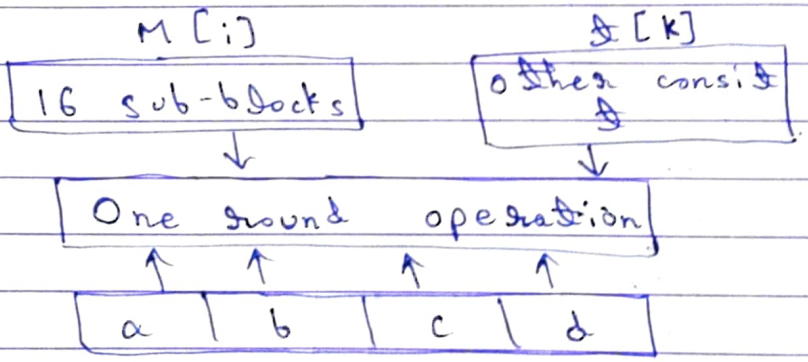


⇒ Divide the 512 bit into 16 sub-blocks of 32 bit each



⇒ Round → 4 rounds

⇒

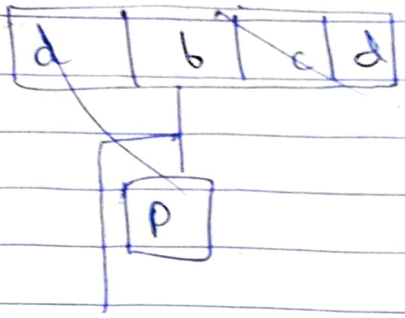


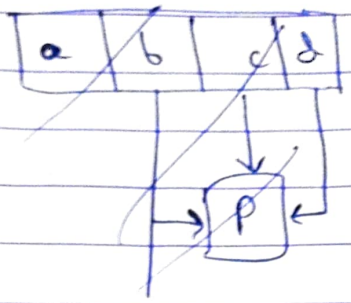
I st round ⇒ $bc + \bar{b}d$ ⇒ (b AND c) OR (NOT b AND d)

II nd round ⇒ $bd + c\bar{d}$

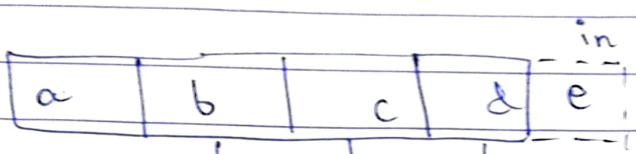
III rd round ⇒ $b \otimes c \otimes d$

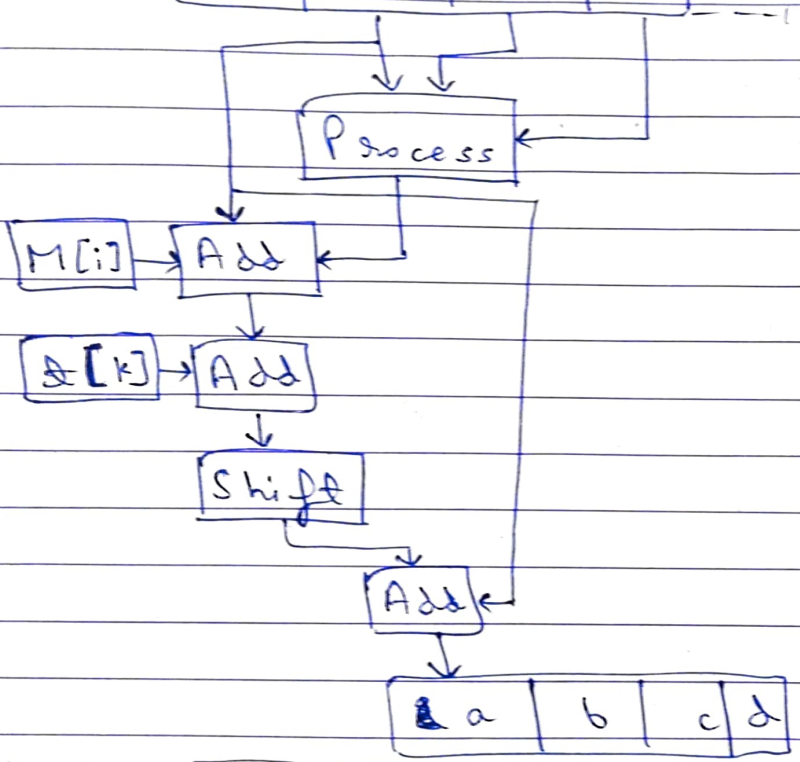
IV th round ⇒ $c \oplus (b + \bar{d})$



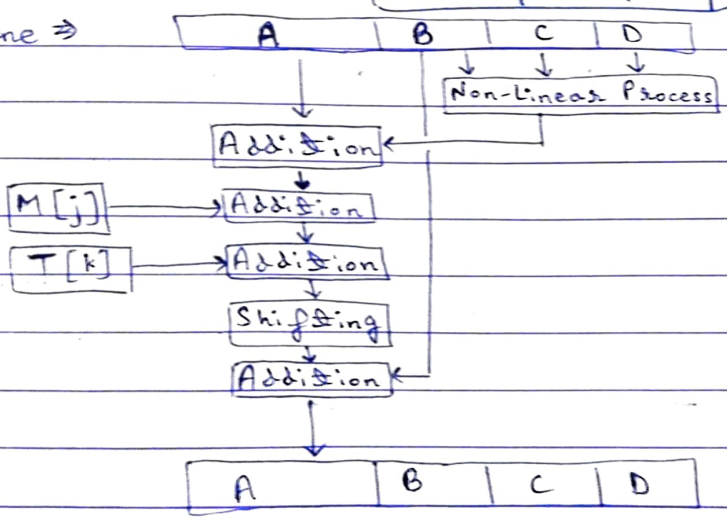


By size ⇒

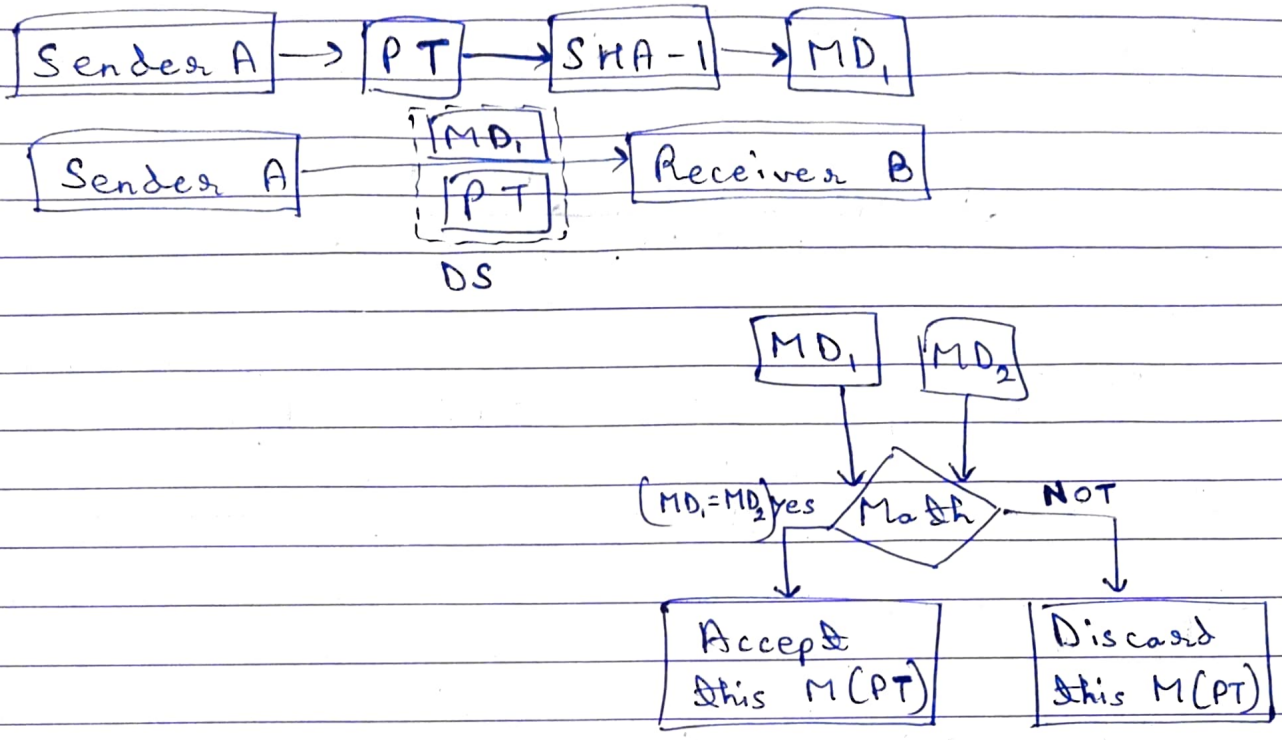




Online ⇒



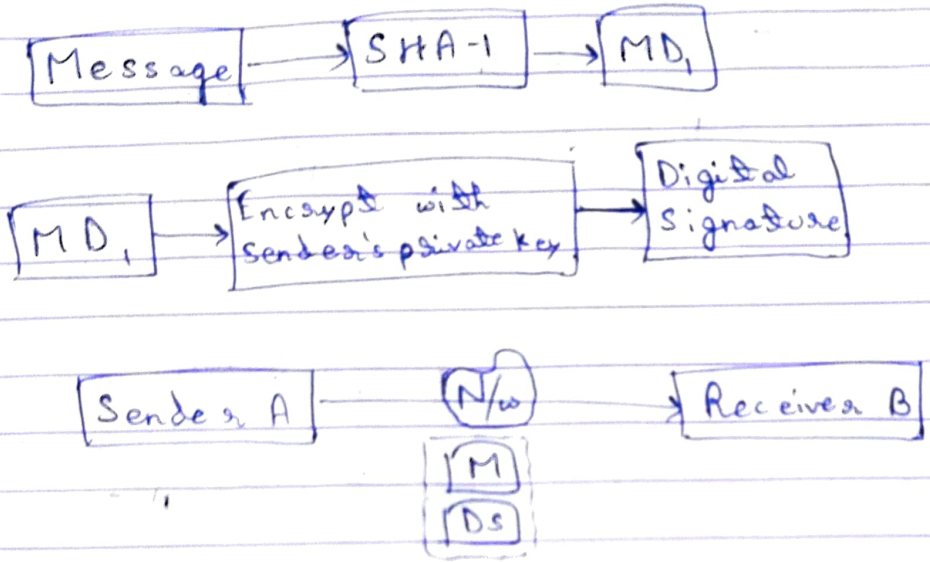
*) Digital Signature with MD (SHA-1)



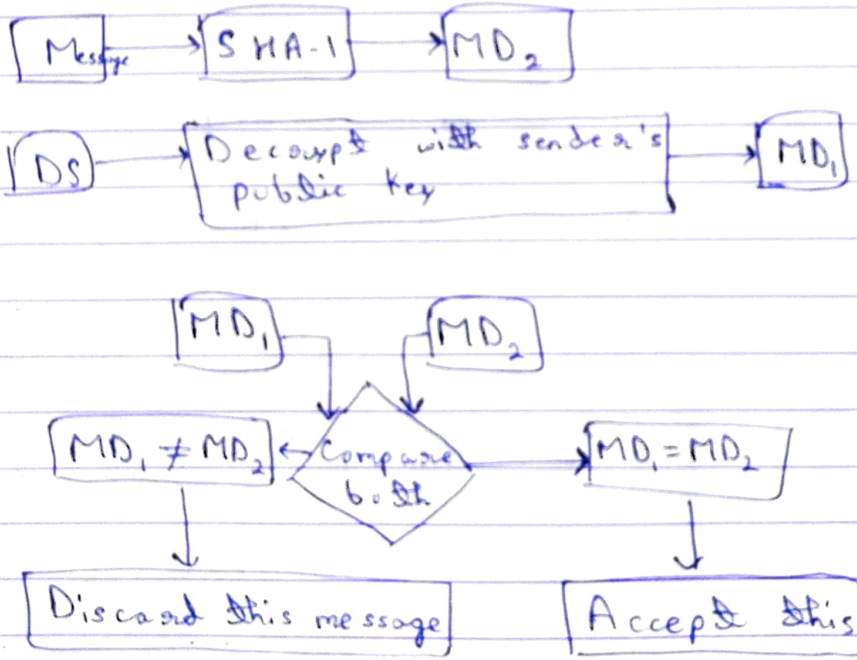
*) Difference between MD_5 & SHA-1

	MD_5	SHA-1
Message Digest Length	128	160
Chaining variables	4	5
Speed	Faster	Slower
Attacked	Yes	No
Iterations	16 (Less)	20 (More)

*) Digital Signature with RSA

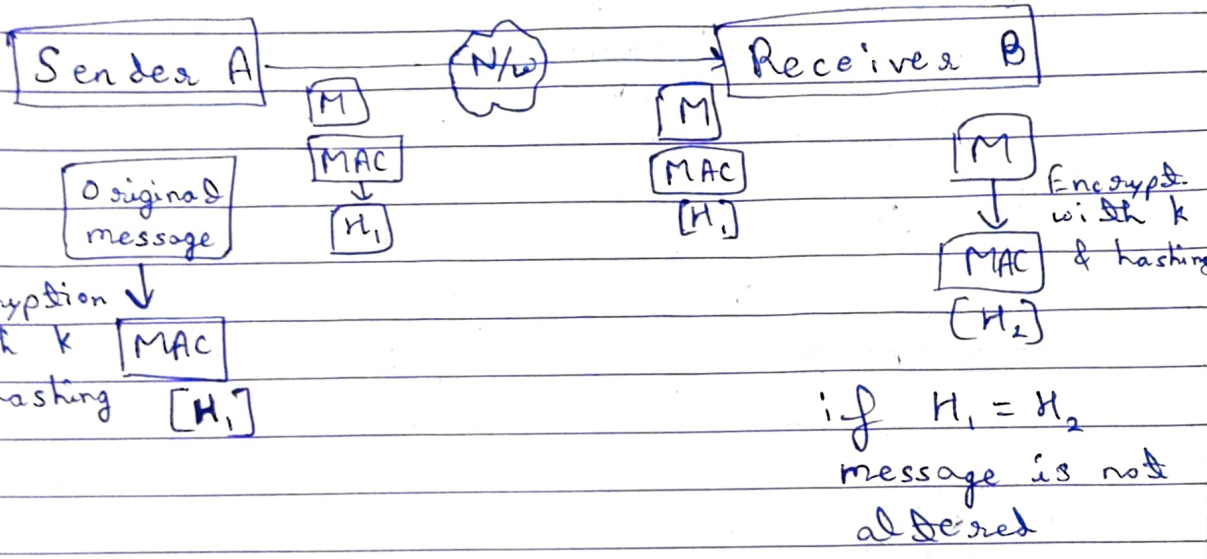


Receiver end



*) Message Authentication Code (MAC)

- Similar to Message Digest, only difference is that symmetric key (k) is used here.



- Attacker has to alter both M & MAC

*) H-MAC

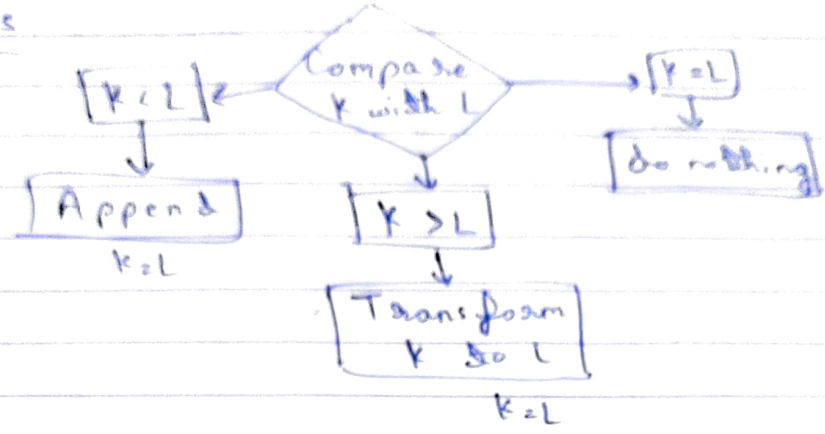
- IP, SSL

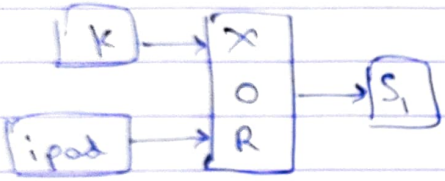
- Symmetric key (k)

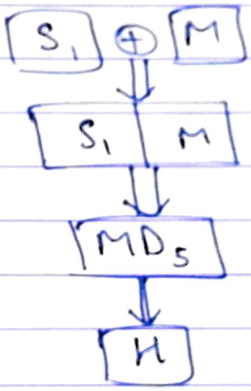
- M → Original message
  L → no. of blocks in original message
  b → no. of bits in a block
  ipad → A string of 0110110 repeated by b/8 time
  [54]

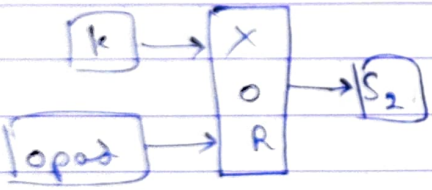
  opad → A string of 01011010 repeated by b/8 times
  [90]

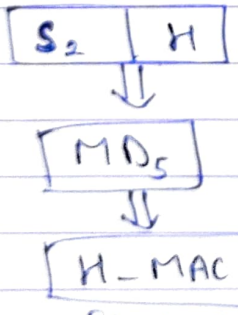
Steps



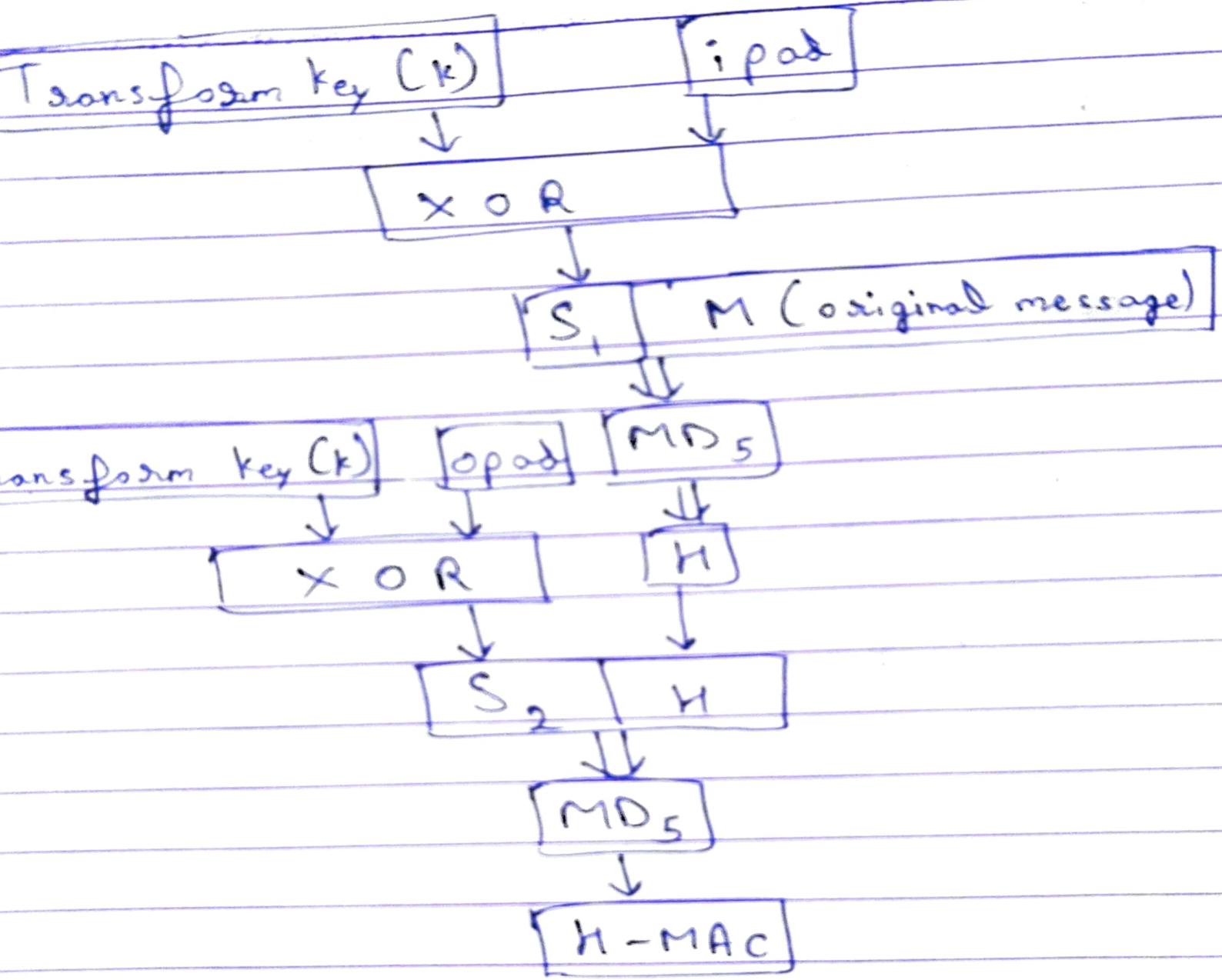








Find MAC


Transform key (K)
ipad
XOR
S1
M (original message)
MD5
ansform key (K)
opad
XOR
H
S2
H
MD5
H-MAC

*) Prime Numbers
Relatively Prime Numbers
Fermat's Theorem
Euler's Totient function
Euler Theorem
Euclidean Theorem

*) Fermat's Theorem

States that if p is a prime no.

$a = 7, p = 19$

$7^{18} \bmod 19 = 1$

$7^2 \bmod 19 = 11$
$7^4 \bmod 19 = 7$
$7^8 \bmod 19 = 11$
$7^{16} \bmod 19 = 7$
$7^{18} \bmod 19 \Rightarrow ((7^{16} \bmod 19) \times (7^2 \bmod 19)) \% 19 \Rightarrow (7 \times 11) \% 19 \Rightarrow 1$

*) Euler's Totient function

$\phi(n)$

↳ less than 'n' & relatively prime to 'n'

Ex ⇒

$\phi(37)$ ⇒ 1, 2, ... 36

⇒ 36 values

$\phi(35)$ ⇒ 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34

⇒ 24 values

$\phi(35) = \phi(5 \times 7)$ ⇒ Factors

⇒ $\phi(5) \times \phi(7)$

⇒ 4×6

⇒ 24

$\{\phi(n) = n-1$ if n is prime$\}$

*) Euler Theorem

~~$\phi(n)$~~

$\boxed{a^{\phi(n)} \equiv 1 \pmod{n}}$ for every a and n that are relatively prime

$a = 3, \; n = 10$

$3^4 \equiv 1 \pmod{10}$ $\quad \phi(10) \Rightarrow \phi(2) \times \phi(5)$

$\Rightarrow 1 \times 4 \Rightarrow 4$ ↩

*) Euclidean Theorem

gcd(a, b)

Algo.

1) Euclid (a, b)
2) A ← a, B ← b
3) If B = 0, return A = gcd(a, b)
4) R = A mod B
5) A ← B
6) B ← R
7) go to step 3

Program (A, B) [a > b]

$A_1 = B_1 \times a_1 + R_1$
$A_2 = B_2 \times a_2 + R_2$
$A_3 = B_3 \times a_3 + R_3$
$A_4 = B_4 \times a_4 + R_4$
⋮ ⋮ ⋮ ⋮

Eg. gcd(1970, 1066)

1970 = 1066 × 1 + 904
1066 = 904 × 1 + 162
904 = 162 × 5 + 94
162 = 94 × 1 + 66
94 = 66 × 1 + 28
66 = 28 × 2 + 10
28 = 10 × 2 + 8
10 = 8 × 1 + 2
8 = 2 × 4 + 0
2 = 0 × 0 + 2

gcd(26835, 32375)

$32375 = 26835 \times 1 + 5540$

$26835 = 5540 \times 4 + 4675$

$5540 = 4675 \times 1 + 865$

$4675 = 865 \times 5 + 350$

$865 = 350 \times 2 + 165$

$350 = 165 * 2 + 20$

$165 = 20 * 8 + 5$

$20 = 5 \times 4 + 0$

$5 = 0 \times 0 + 5$

*) Steganography

*) Chinese Remainder Theorem

$$\begin{cases} x \equiv a_1 \bmod (m_1) \\ x \equiv a_2 \bmod (m_2) \\ x \equiv a_3 \bmod (m_3) \end{cases}$$

Congruency

$M = m_1 \times m_2 \times m_3 \ldots$

$M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$ .....

$Y_1 \equiv M_1^{-1} \bmod (m_1)$, $Y_2 \equiv M_2^{-1} \bmod (m_2)$

$M_1 Y_1 \equiv 1 \bmod (m_1)$

$Y = a_1 Y_1 M_1 + a_2 Y_2 M_2 + \ldots$

$$\boxed{x = Y \bmod (M)}$$

Ex →

$x \equiv 4 \bmod (10)$

$x \equiv 6 \bmod (13)$

$x \equiv 4 \bmod (7)$

$x \equiv 2 \bmod (11)$

$M = 13 \times 7 \times 11 \times 10 = 10010$

$M_1 = \frac{M}{m_1} = \frac{10010}{10} = 1001$

$Y_1 M_1 = 1 \bmod (m_1) \Rightarrow Y_1 = 1$

i	a_i	M_i	Y_i	$Y_i M_i$	$a_i Y_i M_i$
1	4	1001	1	1001	4004
2	6	770	9	6930	41580
3	4	1430	4	5720	22880
4	2	910	7	6370	~~25480~~ 12740
					~~33917~~ 81204

$x = 81204 \bmod 10010$

$$\boxed{x = 1124}$$

P-2

$x \equiv 73 \mod (509)$

$x \equiv 20 \mod (79)$

$x \equiv 123 \mod (211)$

$x = 164 \mod (359)$

Ans = 1600