*) Digital Signature with RSA

Message → SHA-1 → MD_1

MD_1 → Encrypt with sender's private key → Digital signature

Sender A → N/w → Receiver B

M

DS

Receiver end

Message → SHA-1 → MD_2

DS → Decrypt with sender's public key → MD_1

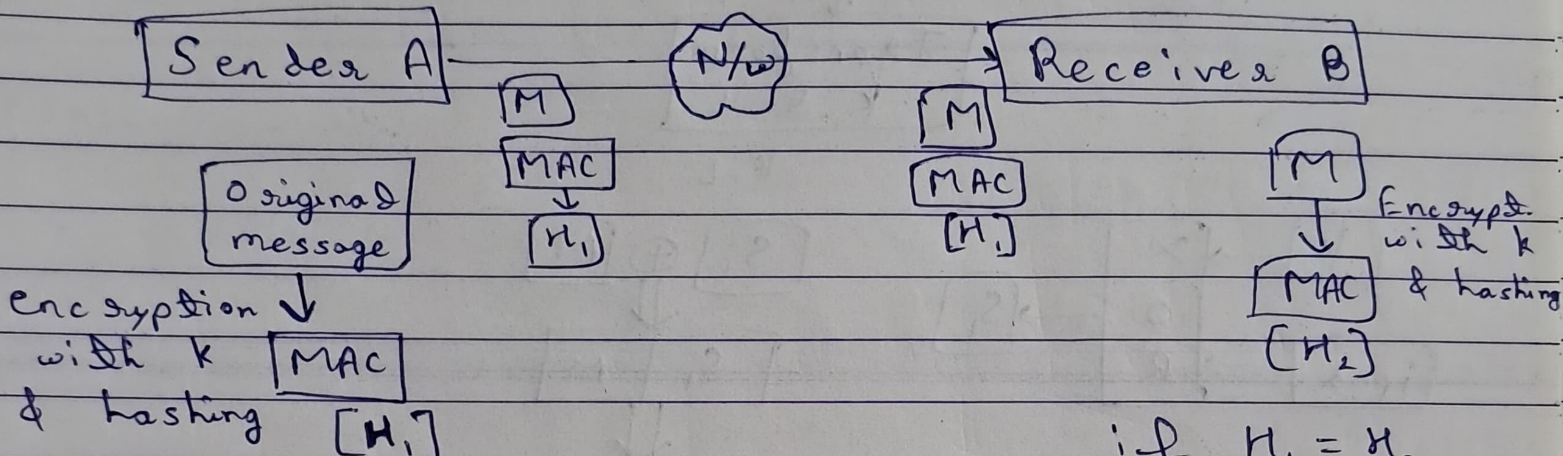
MD_1 → Compare both ← MD_2

Compare both → $MD_1 \neq MD_2$ → Discard this message

Compare both → $MD_1 = MD_2$ → Accept this

*) Message Authentication Code (MAC)

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



if $H_1 = H_2$ message is not altered

- Attacker has to alter both M & MAC

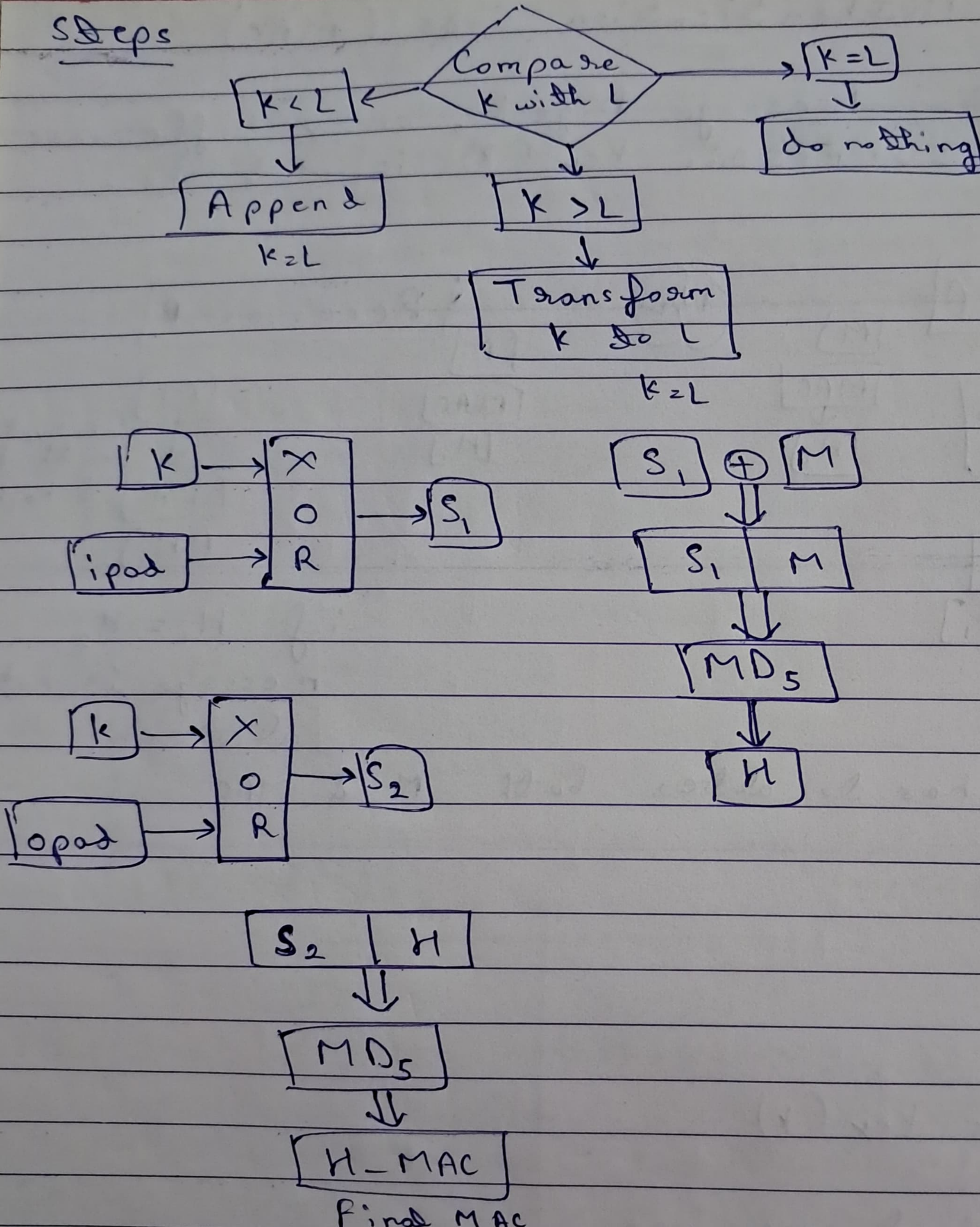
*) H-MAC

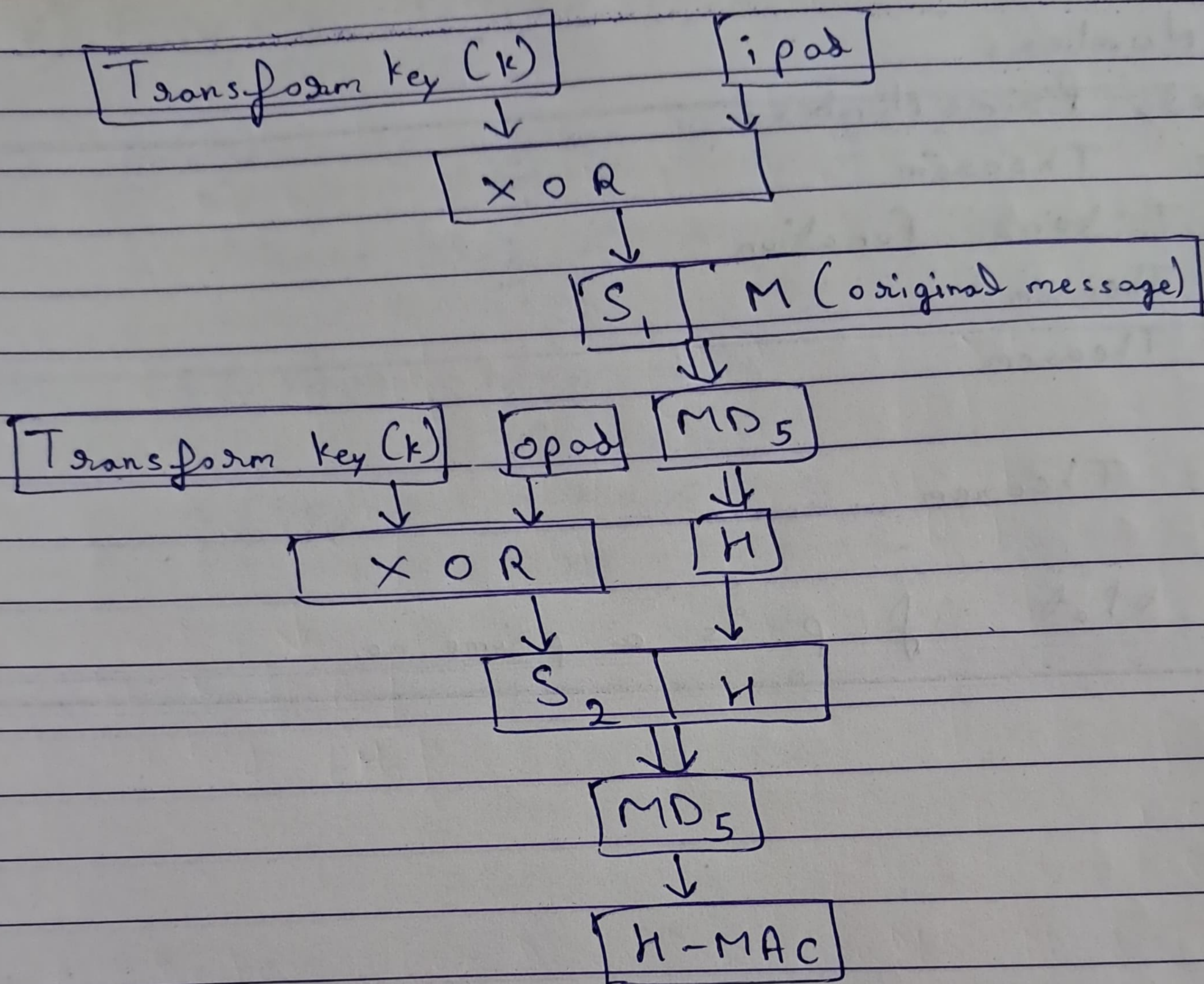
- IP, SSL

- 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
  $\boxed{54}$
  opad → A string of 01011010 repeated by b/8 times
  $\boxed{90}$

Steps


Compare k with L
k<L
Append
k=L
k>L
Transform k to L
k=L
k=L
do nothing
k
ipad
XOR
S1
S1 ⊕ M
S1 | M
MD5
H
k
opad
XOR
S2
S2 | H
MD5
H_MAC
Find MAC


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

*) Prime Numbers
Relatively Prime Numbers
Fermat's Theorem
Euler's Toitent 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 Toitent function

$\phi(n)$

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

Ex ⇒

$\phi(37) \Rightarrow 1, 2, \ldots\ldots 36$

$\Rightarrow 36$ values

$\phi(35) \Rightarrow 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23,$
$24, \cancel{25}, 26, 27, 29, 31, 32, 33, 34$

$\Rightarrow 24$ values

$\phi(35) = \phi(5 \times 7) \Rightarrow$ factors $\left\{ \phi(n) = n - 1 \text{ if } n \text{ is prime} \right\}$

$\Rightarrow \phi(5) \times \phi(7)$

$\Rightarrow 4 \times 6$

$\Rightarrow 24$

*) Euler Theorem

$\cancel{\phi(n)}$

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

$a = 3, n = 10$

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

$\Rightarrow 1 \times 4 \Rightarrow 4$

*) Euclidean Theorem

$gcd(a,b)$

Algo.

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

Program (A_1, B_1) $\boxed{a>b}$

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

Eg. $gcd(1970, 1066)$

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

$gcd(26835, 32375)$

$$32375 = 26835 \times 1 + 5540$$
$$26835 = 5540 \times 4 + 4675$$
$$5540 = 4675 \times 1 + 865$$
$$4675 = 865 \times 5 + 350$$
$$865 = 350 \times 2 + 165$$
$$350 = 165 * 2 + 20$$
$$165 = 20 * 8 + 5$$
$$20 = 5 \times 4 + 0$$
$$5 = 0 \times 0 + 5$$

*) 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

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

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

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

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

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

$$\boxed{x = \sum y \bmod (M)}$$

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
					~~33944~~ 81204

$x = 81204 \bmod 10010$

$$\boxed{x = 1124}$$

P-2

$x \equiv 73 \mod (509)$

$x \equiv 20 \mod (79)$

$x \equiv 123 \mod (211)$

$x \equiv 164 \mod (359)$

$\boxed{Ans = 1600}$