Unit-2

* **Message authentication:**

Verifying the user identity of Sender and receiver.

* **Approaches of message authentication**

1. protecting the integrity of message
2. validating identity of the originator
3. Non-repudation of origin.

* **Types of authentication:**

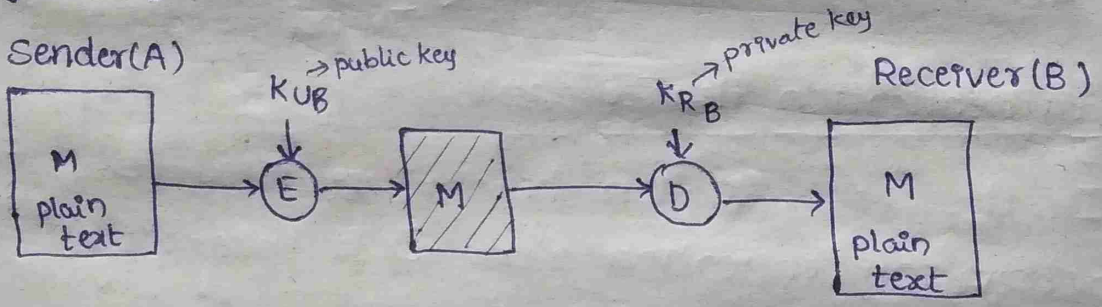
There are three alternative functions used

1. message encryption
2. Message authentication Code (MAC)
3. Hash function (h)

* **Message encryption** (cipher text - authenticator)

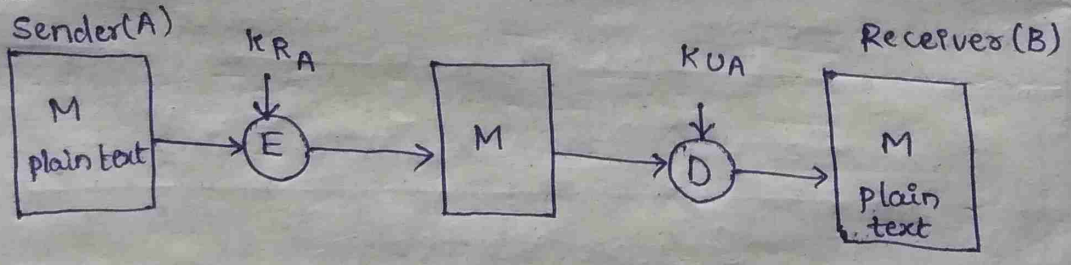
Symmetric

case 1: Sender(A)



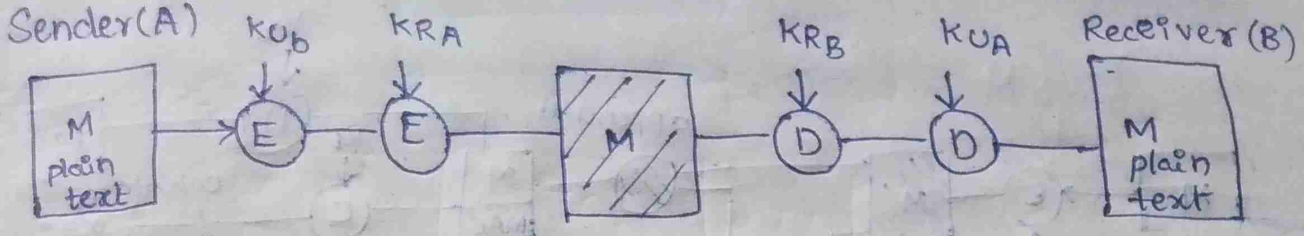
No authentication.

case 2:



No Confidentiality.

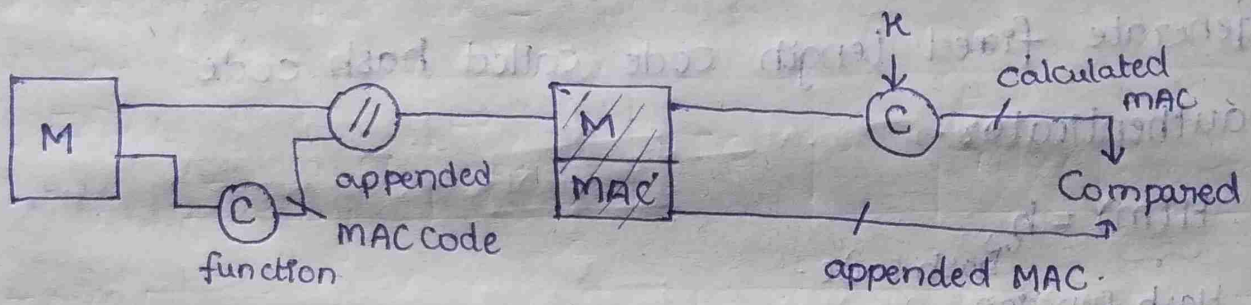
Case-3: Combination of Case 1 and Case 2



We achieved both authentication and confidentiality.

* Imp Message authentication Code (MAC- authenticator)

$C(M, K) = MAC$



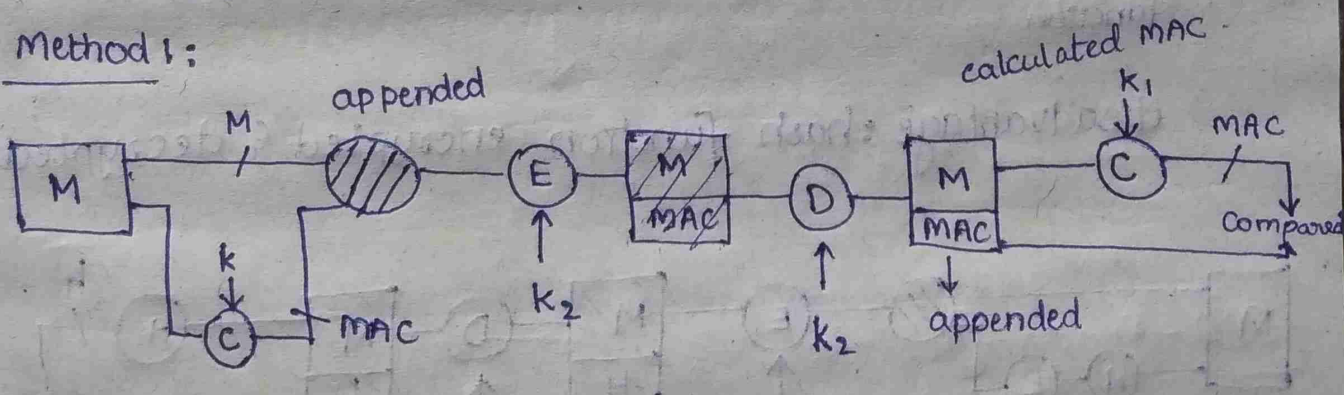
No confidentiality

MAC Code fixed length size code

when we apply a function on message then a code is generated called MAC Code.

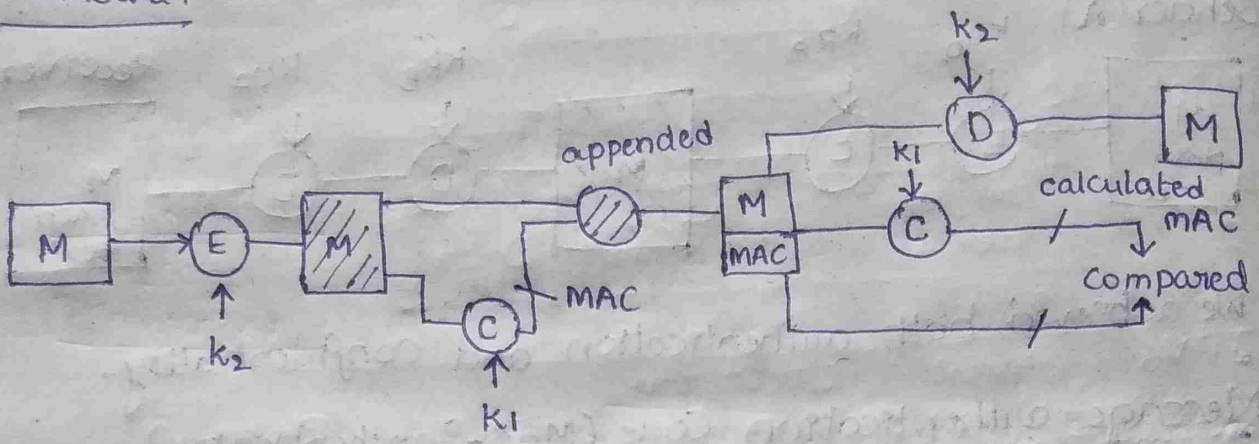
Add confidentiality:

Method 1:



Authentication

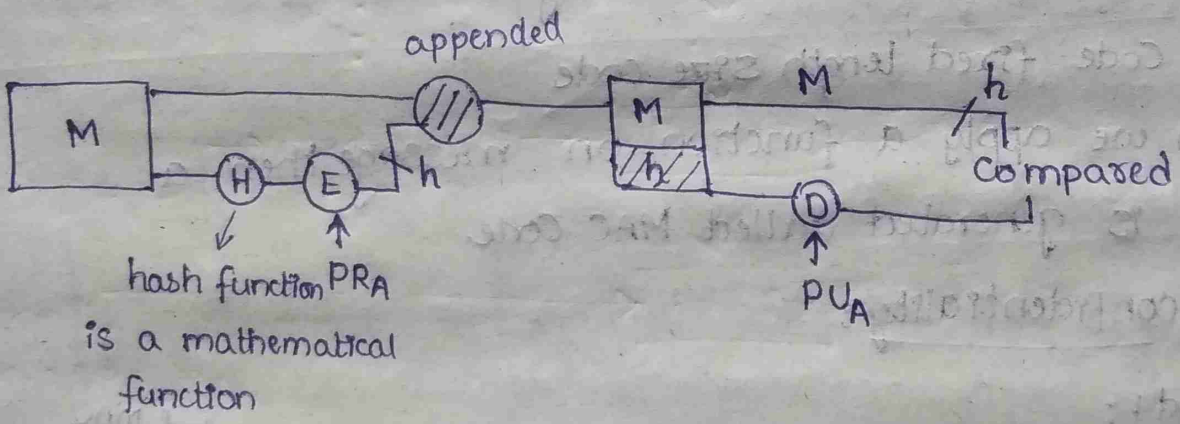
Method 2:



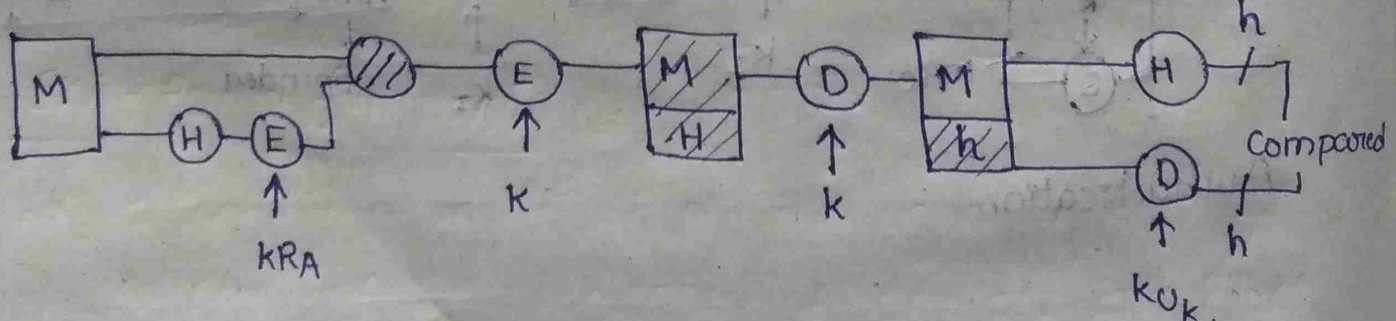
* Hash function:

Generate fixed length code called hash code authenticator.

$\underbrace{H(m)}_{\text{Hash function}} = \underbrace{h}_{\text{hash code}}$



disadvantage: hash function encrypted & decrypted.



* Hash Algorithm (SHA-512):

Secure hash Algorithm (SHA)

Aim: To generate fixed length code depends on hash function.

If output ⟶ 128 bit ------ SHA1
256 bit ------ SHA256
512 bit ------ SHA512 -- 512 bit hash code (output)

plain text Block size = 1024 bits (input after padding)

No. of rounds/steps = 80

Each round "w" (word) = 64 bit (from PT)

Each round use --> constant key

Buffers = 8 (Stores IR results/store o/p)

Each buffer size = 64 bit

o/p of 1st block is i/p to 2nd block.

Steps to be followed:

Step-1: pad the bits 100..and so on. So that length of plain text is multiple of 1024 bits.

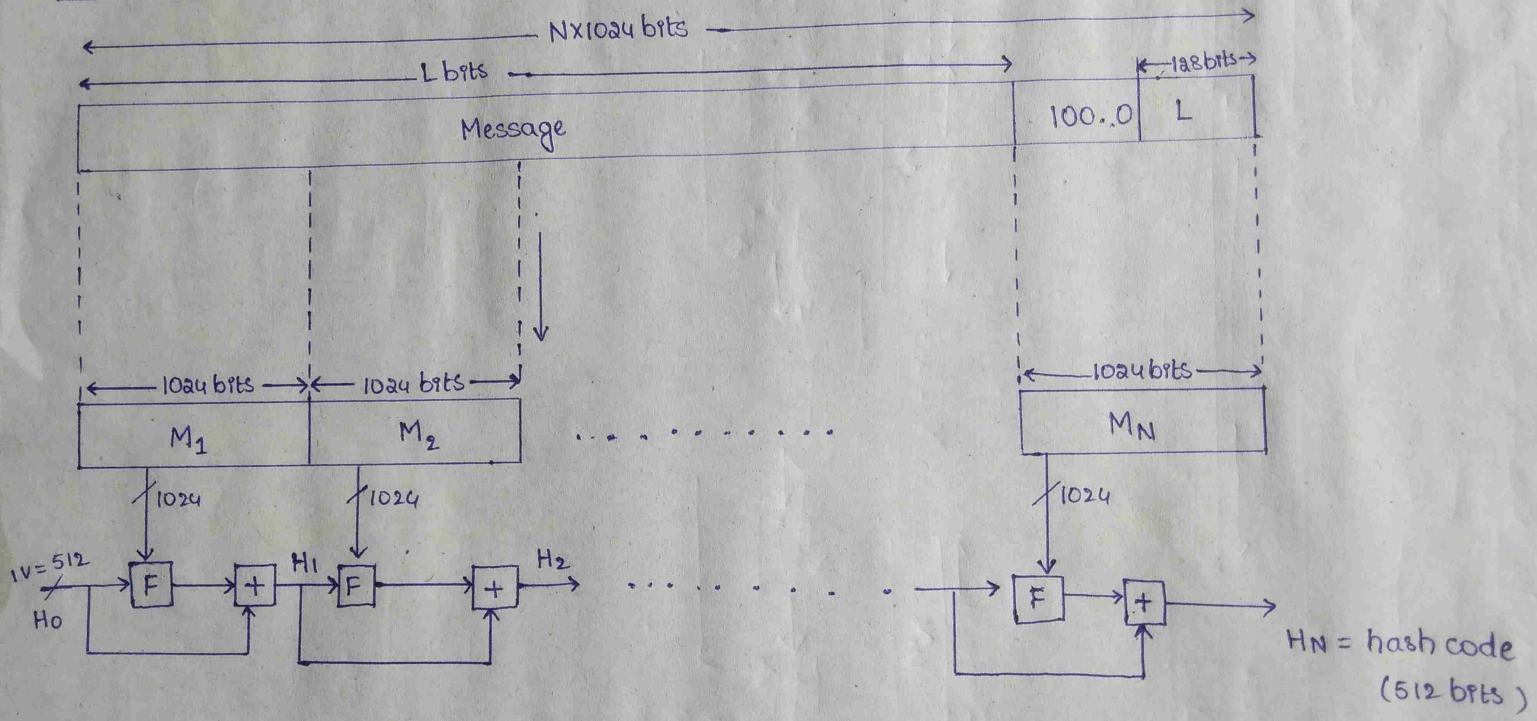
Step-2: Append 128 bit representation of original plain text such that the length of plain text is equal to multiple of 1024 bits.

Step-3: Initialize the buffers (a, b, c, d, e, f, g, h) each of 64 bit in hexadecimal format).

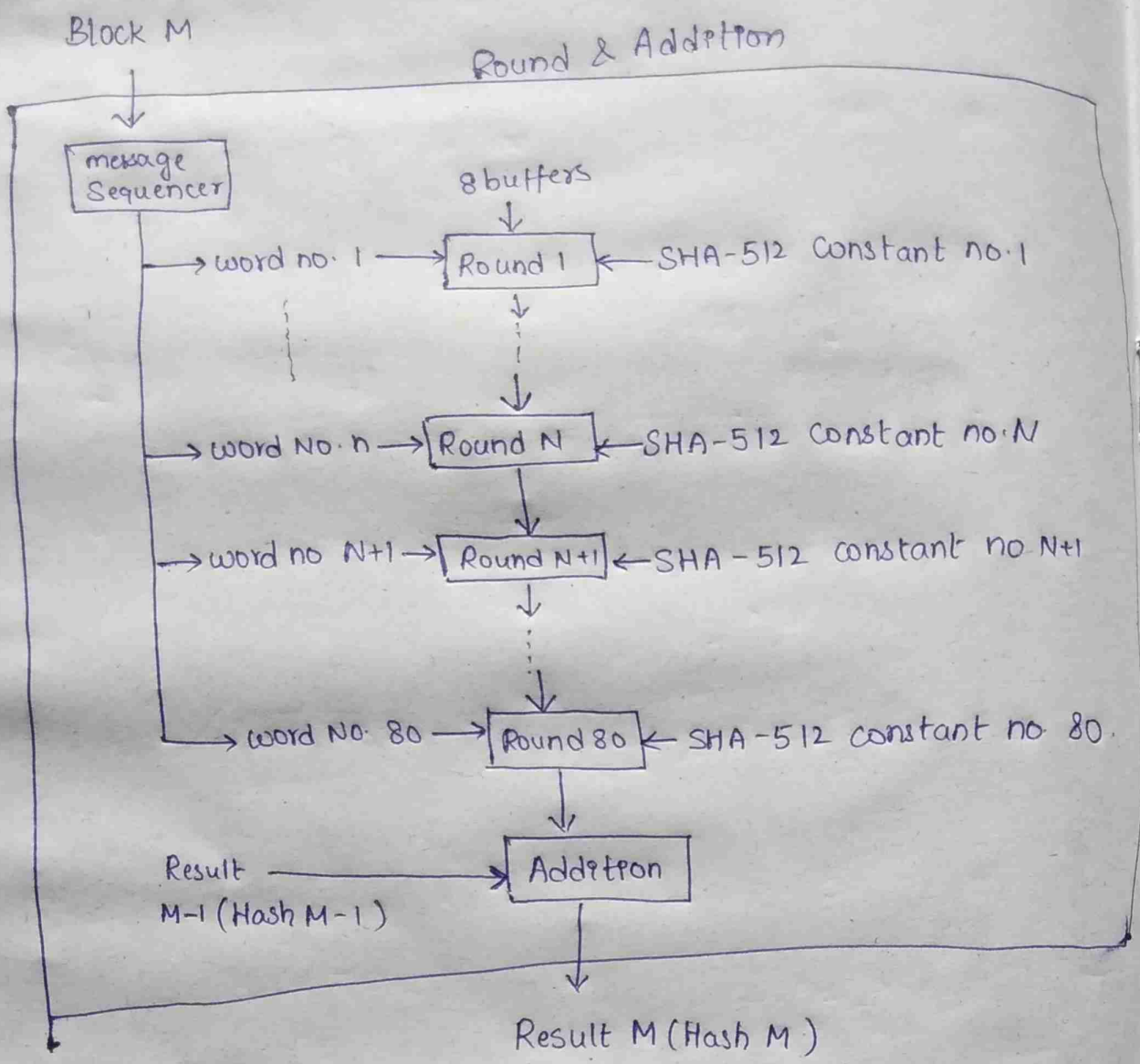
Step-4: process each block of plain text in 80 rounds or steps.

Step-5: Output in buffers is hash code of length 512 bits.

Block diagram:



Initialize the Buffers:



SHA - Round function:

Let us look in more detail at the logic in each of the 80 steps of the processing of one 512-bit block each round is defined by the following set of equations

$$T_1 = h + Ch(e, f, g) + \left(\sum_1^{512} e\right) + w_q + k_i$$

Ch - conditional function

Maj - Majority function.

$T_2 = (\Sigma_0^{512} a) + Maj(a, b, c)$

$a = T_1 + T_2$

$b = a$

$c = b$

$d = c$

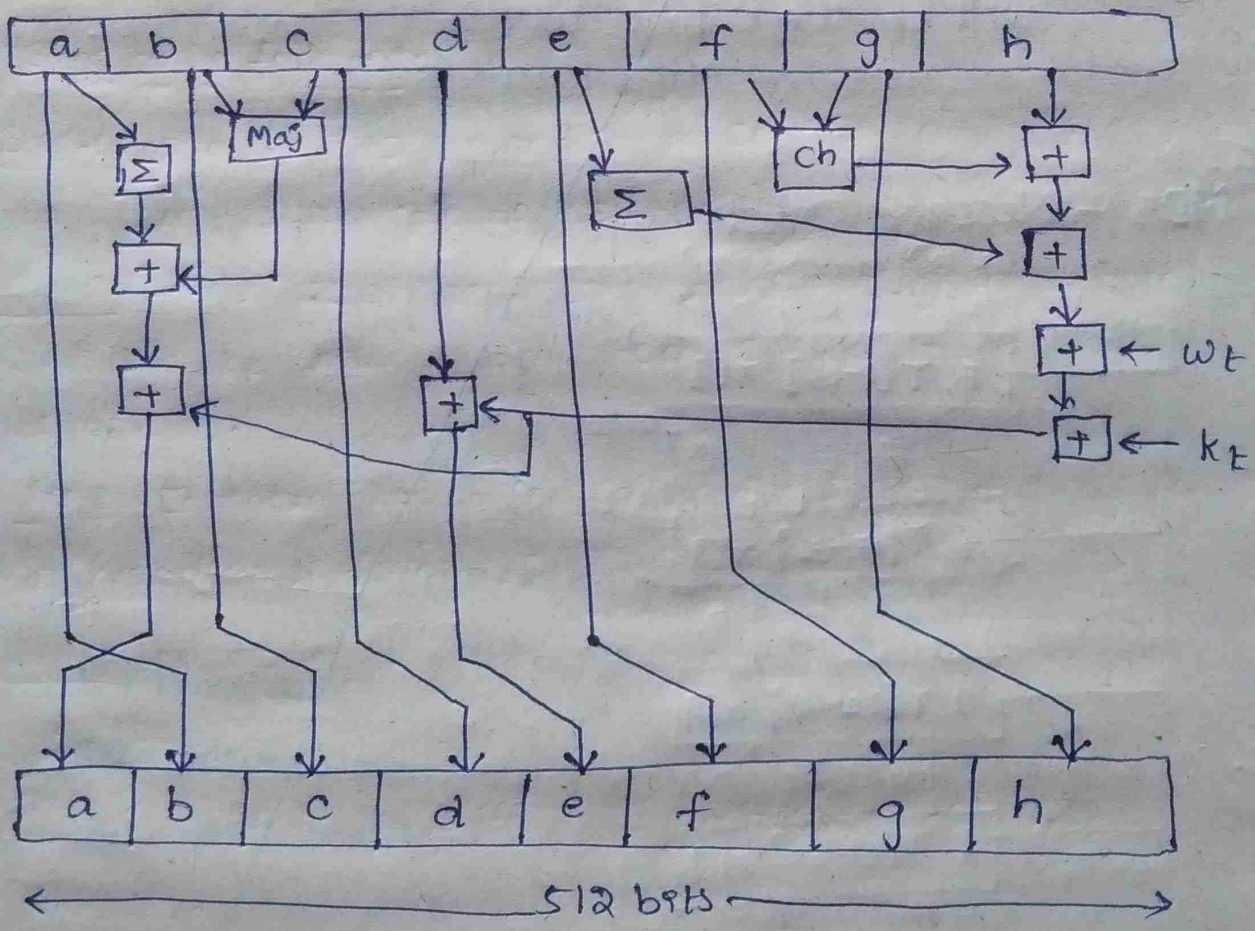
$e = d + T_1$

$f = e$

$g = f$

$h = g$.

Diagramatic Representation



HMAC Algorithm

hash - no key is used

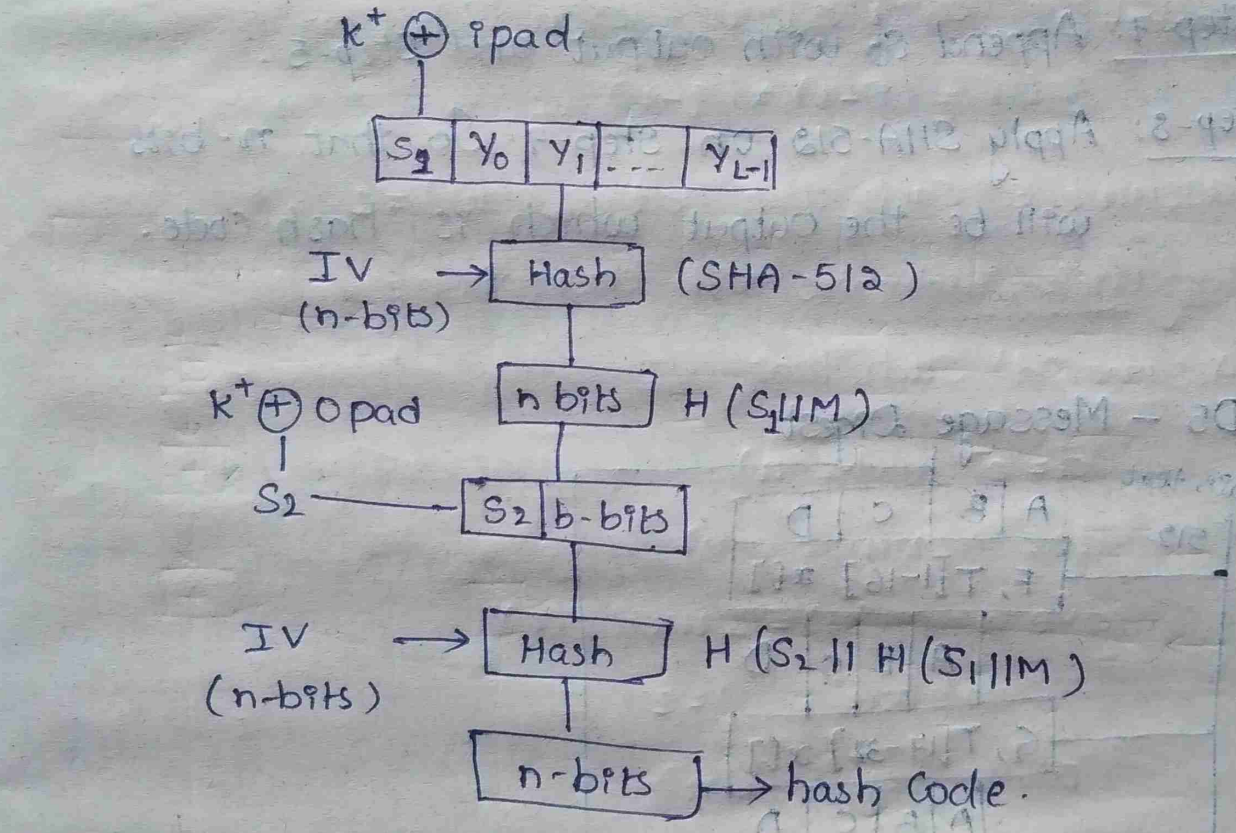
mac - key is used in order to encrypt and decrypt

K → Shared key

K^+ → pad - 0's bit on left side length become 'b' bits.

padding

ipad (00110110) | opad (01011100)



L - Block size

IV - initial vector

S_1 - first result

Y_0... - plain text

K^+ - padded key.

Step-1: Select K if $K < b$ pad zeors on left so that it can be generated with K^+. where

$K^+ = b$.

Step-2: XOR ~~xxxx~~ k^+ with ipad which is equal to b-bits and result is stored in S_1.

Step-3: Append S_1 with M

Step-4: Apply SHA-512 on appended bits.

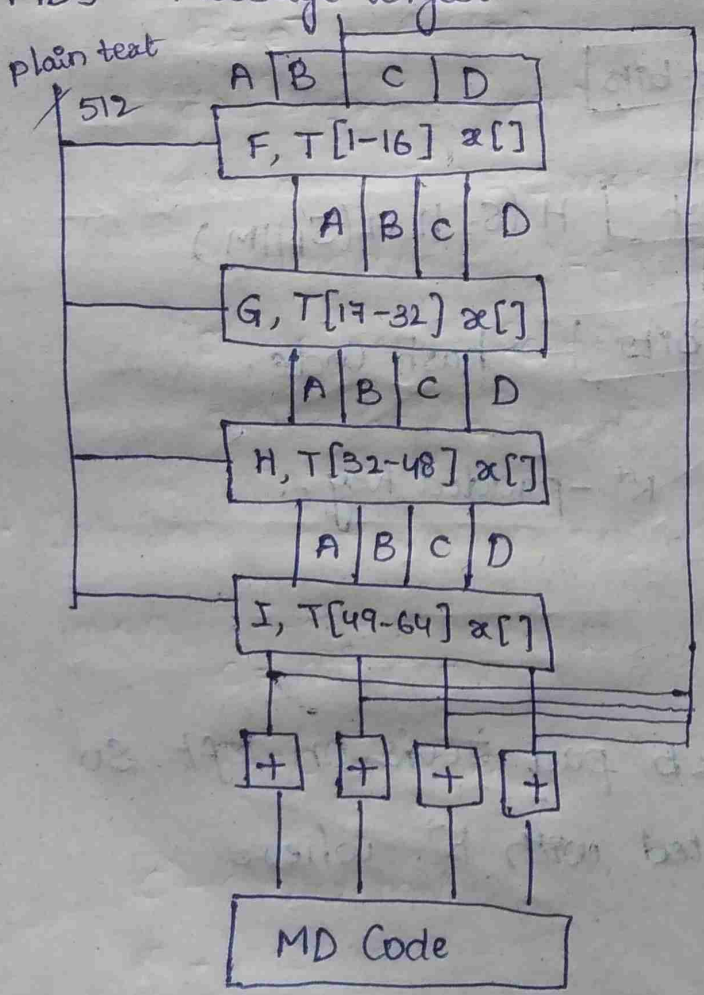
Step-5: pad n-bits until the length is equal to b bits.

Step-6: XOR k^+ with opad which is equal to b-bits and result is stored in S_2.

Step-7: Append S_2 with output and Step-5.

Step-8: Apply SHA-512 on Step-7. So that n-bits will be the output which is hash code.

* MD5 – Message Digest



F, G, H, I - logical function

T - constant

x[] - part of plain text

A, B, C, D - Buffers.

Message digest is a 5 step procedure so it is MD5. the steps are as followed.

Step-1: Append padding bits if plain text is less than 512 bits.

Step-2: Append 64 bit representation.

Step-3: Initialise the buffers. the buffer size is 32 bit and 4 buffers are needed (i.e A, B, C, D).

Step-4: process each block.

Step-5: The output is a MAC code which is an message digest in a buffer.

$F(B,C,D) = (B \wedge C) \vee (\sim B \wedge D)$

$G(B,C,D) = (B \wedge D) \vee (C \wedge \sim D)$

$H(B,C,D) = B \oplus C \oplus D$

$I(B,C,D) = C \oplus (B \cup \sim D)$

$T[1-16] = B \boxplus ((A \boxplus \text{function}(B,C,D) \boxplus x[] \boxplus T[i])$ <<<s)

(16 steps)

→ round function

↓ circular left shift

public key Cryptography

- RSA (Rivest Shameer Anderson)
- Diffie Hellman key exchange.

RSA Algorithm: Steps

1. Consider two large prime numbers as P, Q.
2. calculate $n = P \times Q$.
3. Calculate euler tution ~~fucion~~ function

$$\phi(n) = (P-1) * (q-1)$$

4. assume 'e' such that $\gcd(e, \phi(n)) = 1$.
   where 'e' indicates with encryption.
5. Assume 'd' such that

$$d = e^{-1} \bmod \phi(n)$$

$$d \times e = 1 \times \bmod \phi(n)$$

$$d \times e \bmod \phi(n) = 1 \bmod \phi(n)$$

$$\boxed{d \times e \bmod \phi(n) = 1}$$

public key = {e, n}

private key = {d, n}

6. Calculate encryption and decryption where

$m < n$

$$c = m^e \bmod n$$

$$M = c^d \bmod n$$

C - Cipher text

m - message

Example:

$p=3,\ q=5$

$n = p \times q$

$n = 15$

$\phi(n) = (p-1) \times (q-1)$

$= (3-1) \times (5-1)$

$= 8$

$\gcd(e, \phi(n)) = 1$

assume $e=3,\ d=3$

$\rightarrow \gcd(3,8) = 1$

$d \times e \bmod \phi(n) = 1$

$3 \times 3 \bmod 8$

$\rightarrow = 1$

public key $= \{e, n\} = \{3, 15\}$

private key $= \{d, n\} = \{3, 15\}$

let $m = 13$ because $(m < n)$

$c = m^e \bmod n$

$= (13)^3 \bmod 15$

$= 7$

$m = c^d \bmod n$

$= (7)^3 \bmod 15$

$= 7.$

* Diffie Hellman key exchange:

Step-1: Assume prime number q.

Step-2: Select α such that α is a primitive root of q. ($\alpha < q$).

Step-3: Assume X_a (private key) of user a and $X_a < q$.

Calculate Y_a (public key) of user a

$$Y_a = \alpha^{X_a} \bmod q$$

Step-4: Assume X_b (private key) where $X_b < q$.

calculate Y_b (public key of user b) where

$$Y_b = \alpha^{X_b} \bmod q.$$

* Key Generation:

[A] Sender

$K = (Y_B)^{X_A} \bmod q$

[B] Receiver

$K = (Y_A)^{X_B} \bmod q.$

example:

$q = 11$, $\alpha = 2$.

Let us assume $X_a = 8$ ($X_a < q$)

$$Y_a = \alpha^{X_a} \bmod q.$$

$$= 2^8 \bmod 11$$

$$= 256 \bmod 11$$

$$Y_a = 3$$

Assume $X_b = 4$.

$$y_b = 2^4 \bmod 11$$
$$= 16 \bmod 11$$
$$y_b = 5$$

$$(X_a, Y_a) = \{8, 3\}$$

$$(X_b, Y_b) = \{4, 5\}$$

A-Sender

$$K = (5)^8 \bmod 11$$
$$= 4$$

B- Receiver

$$K = (3)^4 \bmod 11$$
$$= 4.$$