Elliptic curve cryptography (ECC)

* uses group of points instead of integers.

* Elliptic curve described by cubic equation.

(weirstrass equation)

$$y^2 + axy + by = x^3 + cx^2 + dx + e$$

a, b, c, d, e are real numbers

* ECC uses special equation. a, b, c = 0

$$y^2 = x^3 + dx + e \Rightarrow y^2 = x^3 + ax + b$$

prime field $\{0, \ldots (p-1)\}$

$$y^2 \bmod p = (x^3 + ax + b) \bmod p$$

prime number

eg!

consider $p = 23$, $a = 1$ $b = 1$

$$y^2 \bmod 23 = (x^3 + x + 1) \bmod 23$$

(or)

$$E_{23}(1,1) \,/\, E_p(a,b)$$

Generating points

(0,0) (1,0) ...... (22,0)

(0,1) (0,2) (00,22)

⋮

(0,22) .... (22,22)

to check if it belongs to curve :

$(0,0) = 0^2 \bmod 23 = (0+0+1) \bmod 23$

x, y

$0 \neq 1$ ×

$(0,1) = 1^2 \bmod 23 = (0+0+1) \bmod 23$

$1 = 1$

$\therefore$ (0,1) belongs to elliptic curve.

My the points belonging to the elliptical curve is

(0,1) (0,22) (1,7) (1,16) (3,10) (3,17)

(4,0) (5,4) (5,19) (6,4) (6,19) (7,11)

(7,12) (9,7) (9,16) (11,3) (11,20) (12,4)

(12,19) (13,7) (13,16) (17,3) (17,20) (18,3)

(18,20) (19,5) (19,18) + $O \rightarrow$ point at infinity

points

Prob

determine the points over $E_{11}(1,6)$

sol

$y^2 \bmod 11 = (x^3 + x + 6) \bmod 11$

0, 0

0, 1

0, 2

0, 3

⋮

0, 10

$(0,0)\ 0 \neq 6$	$(1,0) = 0 \neq 8$	$(2,0) = 0 \neq 5$
$(0,1)\ 1 \neq 6$	$(1,1) = 1 \neq 8$	$(2,1)\ 1 \neq 5$
$(0,2)\ 4 \neq 6$	$(1,2) = 4 \neq 8$	$(2,2)\ 4 \neq 5$
$(0,3)\ 9 \neq 6$	$(1,3)\ 9 \neq 8$	$(2,3)\ 9 \neq 5$
$(0,4)\ 5 \neq 6$	$(1,4)\ 5 \neq 8$	$(2,4)\ 5 = 5$
$(0,5)\ 3 \neq 6$	$(1,5) = 3 \neq 8$	$(2,5)\ 3 \neq 5$
$(0,6)\ 3 \neq 6$	$(1,6)\ 3 \neq 8$	$(2,6)\ 3 \neq 5$
$(0,7)\ 5 \neq 6$	$(1,7)\ 5 \neq 8$	$(2,7)\ 5 = 5$
$(0,8)\ 9 \neq 6$	$(1,8)\ 9 \neq 8$	$(2,8)\ 9 \neq 5$
$(0,9)\ 4 \neq 6$	$(1,9)\ 4 \neq 8$	$(2,9)\ 4 \neq 5$
$(0,10)\ 1 \neq 6$	$(1,10) = 1 \neq 8$	$(2,10)\ 1 \neq 5$

(2,4) (2,7) (3,6) (3,5) (5,2) (5,9) (7,2) (7,9) (8,3) (8,8) (10,2) (10,9) are the points belonging to elliptical curve.

(3,6)

(3,5) $3 \neq 2$

3 =

(2,0) = 0 ≠ 5
(2,1) 1 ≠ 5
(2,2) 4 ≠ 5
(2,3) 9 ≠ 5
(2,4) 5 = 5
(2,5) 3 ≠ 5
(2,6) 3 ≠ 5
(2,7) 5 = 5
(2,8) 9 ≠ 5
(2,9) 4 ≠ 5
(2,10) 1 ≠ 5

(5,9)

points

③ operations

① point addition

② point doubling

③ scalar multiplication

$R = P + Q$

$x_R = (\lambda^2 - x_P - x_Q) \bmod p$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

if $P = Q$ $\quad \lambda = \left(\dfrac{3x_P^2 + a}{2y_P}\right) \bmod p$

if $P \neq Q$ $\quad \lambda = \left(\dfrac{y_Q - y_P}{x_Q - x_P}\right) \bmod p$

prob

$P = (3, 10)$ $\quad Q = (9, 7)$ from $E_{23}(1,1)$

sol

$\because P \neq Q$

$$\lambda = \left(\frac{y_Q - y_P}{x_Q - x_P}\right) \bmod p$$

$$= \left(\frac{7 - 10}{9 - 3}\right) \bmod 23$$

$$= \frac{-3}{6} \bmod 23$$

$23 - \frac{1}{2}$

$$= \frac{-1}{2} \bmod 23 = \frac{22}{2} \bmod 23$$

$$\boxed{\lambda = 11}$$

$x_R = (11^2 - 3 - 9) \bmod 23$

$= (121 - 12) \bmod 23$

$= 109 \bmod 23$

$\boxed{x_R = 17}$

$y_R = (11(3 - 17) - 10) \bmod 23$

$= -154 - 10 \bmod 23$

$= -164 \bmod 23$

$= -3$

$\boxed{y_R = 20}$

$\boxed{R = (17, 20)}$

find R for $P = (3, 10)$ $Q = (3, 10)$ from $E_{23}(1,1)$

$$\lambda = \left(\frac{3(3)^2 + 1}{2(10)}\right) \bmod 23$$

$$= \frac{28}{20} \bmod 23$$

$$= \frac{7}{5} \bmod 23$$

$= 7 \cdot 5^{-1} \bmod 23$

$= 7 \cdot 14 \bmod 23$

$= 98 \mod 23$

$= 6$

$\boxed{\lambda = 6}$

$x_R = (36 - 3 - 3) \mod 23$

$= 30 \mod 23$

$\boxed{x_R = 7}$

$y_R = (6(3-7) - 10) \mod P$

$= -34 \mod 23$

$= -11 + 23$

$\boxed{y_R = 12}$

$R = (7, 12)$

find $P+Q$ from $E_{23}(1,1)$

$P = (9, 16)$ $Q = (18, 3)$

$\lambda = \left(\frac{3-16}{18-9}\right) \mod 23$

$= \left(\frac{-13}{9}\right) \mod 23$

$= -13 \cdot 9^{-1} \mod 23$

$= -13 \cdot 18 \mod 23$

$= 19$

Q	A	B	R	T_1	T_2	T
2	23	9	5	0	1	-2
1	9	5	4	1	-2	3
1	5	4	1	-2	3	-5
4	4	1	0	3	-5	
	1	0		$\boxed{-5}$		

$x_R = (\lambda^2 - x_P - x_Q) \bmod p$

$= (19^2 - 9 - 18) \bmod 23$

$= (361 - 9 - 18) \bmod 23$

$= 12$

$y_R = (\lambda(x_P - x_R) - y_P) \bmod p$

$= (19(9-12) - 16) \bmod 23$

$= (19(-3) - 16) \bmod 23$

$= 19$

$R = (12, 19)$

Diffie - Hellman key exchange based on Elliptic curve cryptography (ECDH):

$G \rightarrow$ Generator point

$\rightarrow$ point on the Elliptic curve whose order is larger value of 'n'.

user A

1. user A selects a random integer n_A, $n_A < n$
2. calculate $\boxed{P_A = n_A * G}$

user B

1. user B selects an random integer n_B, $n_B < n$
2. calculate $\boxed{P_B = n_B * G}$

(A) $\boxed{K_A = n_A * P_B}$ (B) $\boxed{K_B = n_B * P_A}$

How to choose Generator points?

$E_5(1,1) \Rightarrow (0,1)\ (0,4)\ (2,1)\ (2,4)\ (3,1)\ (3,4)$
$(4,2)\ (4,3) + O \rightarrow$ point of infinity.

1. let us take $(0,4)$
2. $2P = (0,4) + (0,4) \Rightarrow \lambda = 2 \Rightarrow (4,3)$
3. $3P = (4,3) + (0,4) \Rightarrow \lambda = 1 \Rightarrow (2,4)$
4. $4P = (2,4) + (0,4) \Rightarrow \lambda = 0 \Rightarrow (3,1)$
5. $5P = (3,1) + (0,4) \Rightarrow \lambda = 4 \rightarrow (3,4)$
6. $6P = (3,4) + (0,4) \Rightarrow \lambda = 0 \Rightarrow (2,1)$
7. $7P = (2,1) + (0,4) \Rightarrow \lambda = 1 \Rightarrow (4,2)$
8. $8P = (4,2) + (0,4) \Rightarrow \lambda = 2 \Rightarrow (0,1)$
9. $9P = (0,1) + (0,4) \Rightarrow \lambda = \infty$

Q: $G = (0,4)$
$n_B = 3 \quad n_A = 2$
find public key of user A and user B also find shared key value

$P_A = n_A * G$
$= 2 * (0,4)$
$P_A = (0,4) + (0,4)$
$\lambda = 2$
$P_A = (4,3)$

$P_B = n_B * G$
$= 3 * G$
$= 3\,(0,4)$
$\lambda = 1$
$P_B = (2,4)$

$k_A = n_A \cdot P_B$

$= 2(2,4)$

$\lambda = \left(\frac{3(4)+1}{2(4)} \right) \text{mod } 5$

$= \frac{13}{8} \text{ mod } 5$

$\lambda = 1$

$R_A = (2,1)$

$k_B = n_B * P_A$

$= 3\ (4,3)$

$= (4,3) + (4,3)$

$\lambda = \left(\frac{3(16)+1}{2(3)} \right) \text{mod } 5$

$\lambda = 49 \cdot 6^{-1} \text{ mod } 5$

$\lambda = 4$

$3P = 2P + P$

$= (3,1) + (4,3)$

$\lambda = 2$

$k_B = (2,1)$

$k_B = k_A = (2,1)$

eg: 2

let

the

Q:

let $a_0 = B4$

$a_1 = 2F$

$a_2 = 12$

$a_3 = 10$ using AES mix column procedure construct the new column value and elaborate the calculations.

$$\begin{pmatrix} 02 & 03 & 01 & 01 \\ 01 & 02 & 03 & 01 \\ 01 & 01 & 02 & 03 \\ 03 & 01 & 01 & 02 \end{pmatrix} \begin{pmatrix} B4 \\ 2F \\ 12 \\ 10 \end{pmatrix} = \begin{pmatrix} 00 \\ EC \\ 8F \\ DA \end{pmatrix}$$

$\Rightarrow (02 * B4) \oplus (03 * 2F) \oplus (01 * 12) \oplus (01 * 10)$

<u>02 * B4</u>

(0000 0010) * (1011 0100)

$\Rightarrow x * (x^7 + x^5 + x^4 + x^2)$

$\Rightarrow x^8 + x^6 + x^5 + x^3 \text{ mod } x^8 + x^4 + x^3 + x + 1$

$= x^6 + x^5 + x^4 + x + 1$

= 0111 0011

= 73

<u>03 * 2F</u>

(0000 0011) * (0010 1111)

$\Rightarrow (x+1) * (x^5 + x^3 + x^2 + x + 1)$

$\Rightarrow x^6 + x^4 + x^3 + x^2 + x + x^5 + x^3 + x^2 + x + 1$

$= x^6 + x^5 + x^4 + 1$

= 0111 0001

= 71

01 * 12

(0000 0001) * (00010010)

$\Rightarrow 1 * (x^4 + x)$

$= x^4 + x$

= 0001 0010

= 12 01 * 10 ⇒ 0001 0000

0111 0011

0111 0001

0001 0010

⊕ 0001 0000

0000 0000 = 00

ECC

Encryp

Decry

exam

sd

en

ECC Encryption / Decryption :

Encryption :

$$C_m = \{ kG , P_m + k P_B \}$$

Decryption :

$$P_M + kP_B - n_B k \cdot G$$

Example :

$G = (0, 4)$ $n_A = 2$ $n_B = 3$ $P_B = 2, 4$

$k = 2$ $P_M = (4, 2)$ for $E_{11}(1, 1)$.

Sol

encryption

$$C_M = \{ kG , P_m + k P_B \}$$

$$= \{ 2(0, 4), (4, 2) + 2(2, 4) \}$$

$= \{(4,3), (4,2) + (0,1)\}$

$= \{(4,3), (3,1)\}$

$\lambda = \left(\frac{1-2}{2-4}\right) \bmod 5$

$= \left(\frac{-1}{-2}\right) \bmod 5$

$= \frac{1}{2} \bmod 5$

$= 1 \cdot 2^{-1} \bmod 5$

Q	A	B	R	T_1	T_2	T
2	5	2	1	0	1	-2
2	2	1	0	1	-2	
-	1	0	-	$\boxed{-2}$		

3 $\quad T_1 - T_2 \times Q$

$\lambda = 3$

$x_R = (9 - 4 - 2) \bmod 5$

$= 3 \bmod 5$

$= 3$

$y_R = (3(4-3) - 2) \bmod 5$

$= 1 \bmod 5$

$= 1$

$R = (3,1)$

$$\boxed{C_m = \{(4,3), (3,1)\}}$$

decryption :

$$\underbrace{P_M + KP_B}_{C_M} - n_B K \cdot G$$

$(2,4) \quad (3,1) - 3(2)(0,4)$

$(2,4) \quad (3,1) - 3(4,3)$

$(2,4) \quad (3,1) - (2,1)$

$(2,4) \quad (3,1) + (2,-1)$

$+_{5(P)}$

$(2,4) \quad (3,1) + (2,4)$

$\lambda = \left(\frac{4-1}{2-3}\right) \bmod 5$

$= \frac{3}{-1} \bmod 5$

$= -3 \mod 5$

$x = 2$

$x_R = (4 - 3 - 2) \mod 5$

$= (-1) \mod 5$

$= 4$

$y_R = (2(3-4) - 1) \mod 5$

$= -3 \mod 5$

$y_R = 2$

$(4, 2)$

$\boxed{P_M = (4, 2)}$

consider the elliptic curve $E_{11}(1, 6)$ and $G = (2, 7)$ B's private key is 3 i.e) $n_B = 3$, find $P_B = ?$ and A choose $k = 3$ encrypt the plaintext $(10, 9)$ and find out cipher text. Show the calculation by which P_M is generated by C_M.

Sol

$G = (2, 7)$ $n_B = 3$ $P_M = (10, 9)$ $k = 3$

$P_B = n_B * G$

$= 3(2, 7)$

$= 2P + P$

$= 2(2, 7)$

$= (2, 7) + (2, 7)$

$q = 1-3\times$ $\quad$ $1-0$

$T_1 - T_2 \times Q$

$\lambda = \left(\dfrac{3(2)^2+1}{2(7)}\right) \bmod 11$

Q	A	B	R	T_1	T_2	T
1	14	11	3	1	0	1
3	11	3	2	0	1	-3
1	3	2	1	1	-3	4
2	2	1	0	-3	4	
-	1	0	-	$\boxed{4}$		

$= \left(\dfrac{13}{14}\right) \bmod 11$

$= 13 \cdot 14^{-1} \bmod 11$

$= 13 \cdot 4 \bmod 11$

$= 52 \bmod 11$

$= 8$

$x_R = (64 - 2 - 2) \bmod 11$

$= 60 \bmod 11$

$= 5$

$Y_R = (8(2-5) - 7) \bmod 11$

$= -31 \bmod 11$

$= -9$

$= 2$

$2P = (5,2)$

$2P + P$

$(5,2) + (2,7)$

$-1-(3\times$

$1-(-1\times 2)$

$0-1$

$T_1 - T_2 \times Q$

$\lambda = \left(\dfrac{7-2}{2-5}\right) \bmod 11$

Q	A	B	R	T_1	T_2	T
1	11	8	3	0	1	-1
2	8	3	2	1	-1	3
1	3	2	1	-1	3	-4
2	2	1	0	3	-4	
-	1	0	-	$\boxed{-4}$		

$= \dfrac{5}{-3} \bmod 11$

$= 5 \cdot -3^{-1} \bmod 11$

$= 5 \cdot 8^{-1} \bmod 11$

$-4 + 11 = 7$

$x = 2$

$x_R = (4 - 5 - 2) \bmod 11$

$= -3 \bmod 11$

$= 8$

$y_R = (2(5-8)-2) \bmod 11$

$= -8 \bmod 11$

$= 3$

$P_B = (8, 3)$

encryption:

$C_M = \{kG, P_m + kP_B\}$

$= \{3(2,7), (10,9) + 3(8,3)\}$

$= \{(8,3), (10,9) + (10,9)\}$

$3(8,3) = 2P + P$

$2P = 2(8,3) + (8,3)$

$\lambda = \left(\frac{3(64)+1}{2(3)}\right) \bmod 11$

$= \frac{193}{6} \bmod 11$

$= 193 \cdot 6^{-1} \bmod 11$

$= 193 \times 2 \bmod 11$

$= 386 \bmod 11$

$= 1$

$T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
1	11	6	5	0	1	-1
1	6	5	1	1	-1	2
5	5	1	0	-1	2	
		1	0		$\boxed{2}$	

$x_R = (1 - 8 - 8) \bmod 11$

$= (-15) \bmod 11$

$= 7$

$y_R = (1(8 - 7) - 3) \bmod 11$

$= -2 \bmod 11$

$= 9$

$(7, 9)$

$2P + P = (7, 9) + (8, 3)$

$\lambda = \left(\dfrac{3 - 9}{8 - 7}\right) \bmod 11$

$= \left(\dfrac{-6}{1}\right) \bmod 11$

$= -6 \bmod 11$

$\lambda = 5$

$x_R = (25 - 7 - 8) \bmod 11$

$= 10 \bmod 11$

$= 10$

$y_R = (5(7 - 10) - 9) \bmod 11$

$= -24 \bmod 11$

$= 9$

$(10, 9)$

$CM = \{(8,3), (10,9) + (10,9)\}$

$\lambda = \left(\dfrac{3(100)+1}{18}\right) \bmod 11$

$= \dfrac{301}{18} \bmod 11$

$= 301 \cdot 18^{-1} \bmod 11$

$= 301 \cdot 8 \bmod 11$

$= 10$

$-1-(2\times1)$
$1-(-1$
$0-11\times$
$1-$
$T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
1	18	11	7	1	0	1
1	11	7	4	0	1	-1
1	7	4	3	1	-1	2
1	4	3	1	-1	2	-3
3	3	1	0	2	-3	
	1	0		$\boxed{-3}$		

$-3+11$

8

$x_R = (100 - 10 - 10) \bmod 11$

$= 80 \bmod 11$

$= 3$

$y_R = (10(10-3) - 9) \bmod 11$

$= 61 \bmod 11$

$= 6 \qquad = (3,6)$

$CM = \{(8,3), (3,6)\}.$

Fermat's Theorem :

If p is prime and a is a positive integer not divisible by p, then,

$$a^{p-1} \equiv 1 \bmod p$$

eg: $p = 19$ $a = 7$

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

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

$$1 = 1$$

Prob : Find $4^{184} \bmod 5 = ?$ ($p-1 = 4$, p)

sol

$$(4^4)^{46} \bmod 5$$

$$(1)^{46} \bmod 5 \quad (\because \text{by fermat's theorem})$$

$$1$$

Prob : Find 3^{121} over $GF(7)$

$3^{121} \bmod 7$ → prime number

$$(3^6) \bmod 7 = 1$$

$$(3^6)^{20} 3^1 \bmod 7 = 1.3 \bmod 7 = 3$$

$6 \overline{)121}$

Euler's Theorem :

Euler's theorem states that for every a & n that are relatively prime ,

$$a^{\phi(n)} \equiv 1 \bmod n$$

eg : ① $n = 10$ $\quad p = 2 \quad q = 5$

$\phi(n) = 1 * 4 = 4$

$\{1, 3, 7, 9\}$

$a = 3$

$3^4 \equiv 1 \bmod 10$

$3^4 \bmod 10 = 1 \bmod 10$

$1 = 1$

② $n = 11$

$\phi(n) = 10$

$\{1, \ldots\ldots 10\}$

$a = 2$

$2^{10} \equiv 1 \bmod 11$

$2^{10} \bmod 11 = 1 \bmod 11$

$1 = 1$

Trapdoor Oneway Function :

$Y = f_K(X)$, easy, if K and X are known.

$X = f_K^{-1}(Y)$, easy, if K and Y are known.

$X = f_K^{-1}(Y)$, infeasible, if Y is known but K is not unknown.

It is easy to calculate in one direction and infeasible to calculate in other direction. unless certain additional information is known.

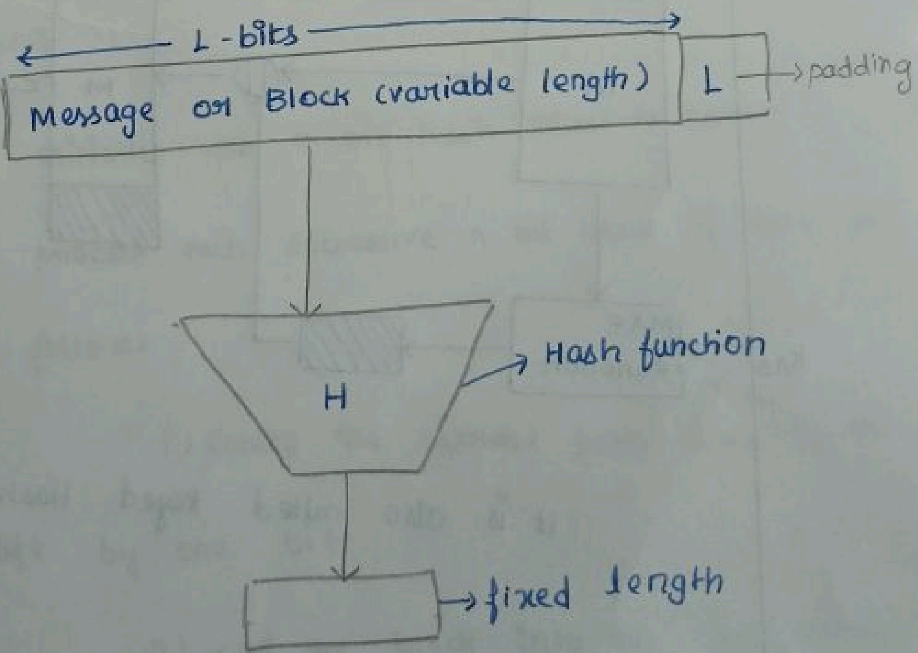
—×—×—

Message Authentication :

① Message Authentication using Hash function.

② Message Authentication using MAC.

③ Digital signature.



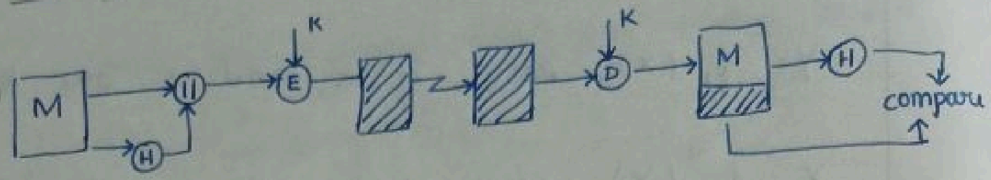
Hash value (h)

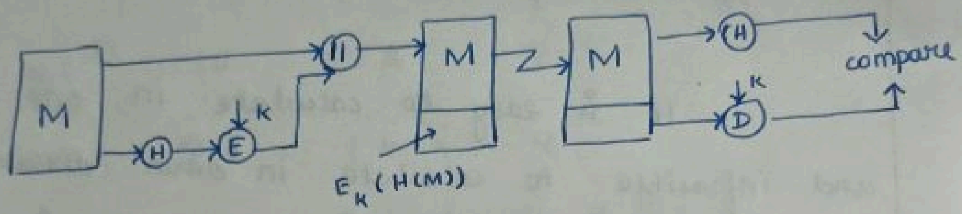
Hash code / Message Digit (MD)

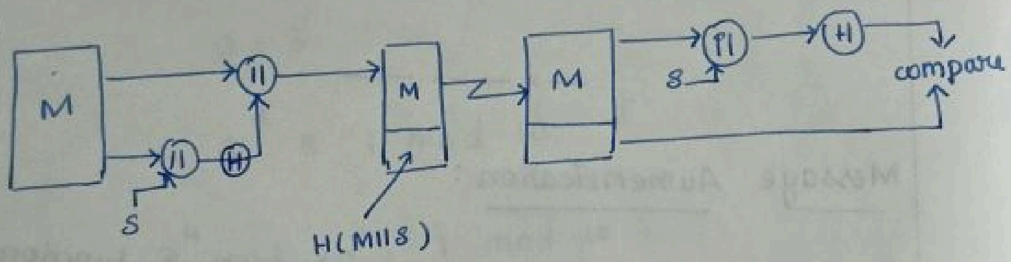
Uses of Hash function in Message Authentication:

|| → concatenation

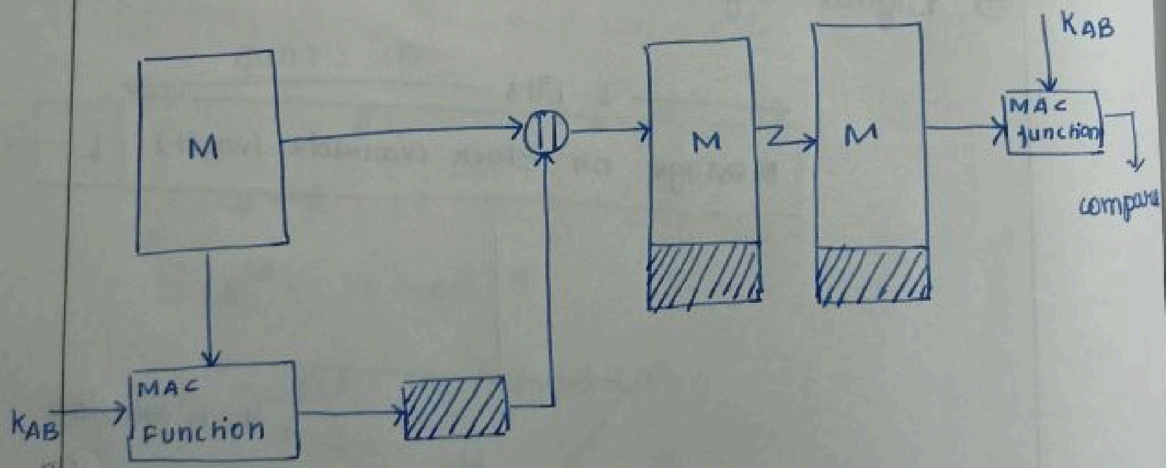
SHA
MD (V4, V5)
RIPEMD



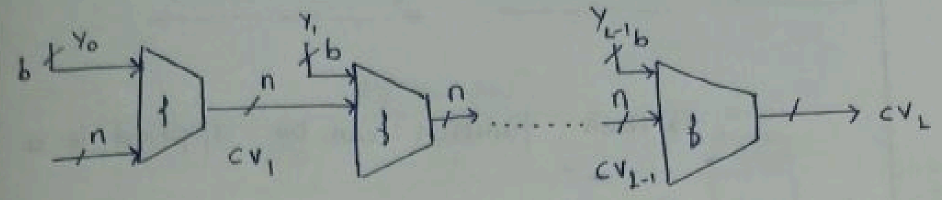




Message Authentication using MAC :- (MAC = Message Authentication code)



It is also called keyed Hash function.



General Structure of Secure Hashcode

$c_i = b_{i1} \oplus b_{i2} \oplus \ldots\ldots \oplus b_{im}$

i^{th} bit, block number

4 bit original message

0011 | 0011 | 0000 | 0101

⇒ converted into 4 bit hash code

$1 \oplus 1 \oplus 1 \oplus 1 \Rightarrow$

$c_i \rightarrow i^{th}$ bit of the hash code

$m \rightarrow$ no. of. n bit blocks in the i/p

$b_{ij} \rightarrow i^{th}$ bit in j^{th} block

Two simple hash function:

① Bit by Bit XOR operation

② Rotated XOR operation

Rotated XOR

step 1: initially set n bit hash values to zero

step 2: process each successive n bit block of data as follows

1) Rotate the current hash value to the left by one bit

2) XOR the block into the hash value.

0001 | 0010 | 0011

H → 0000 | 0010

⊕ 0001 | 0010 (left shift)

0001 | 0000 | 0011

left shift → 0000

0011 → final has value

Properties/ requirements of Hash function :

1) Hash function can be applied to a block of data of any size

2) Hash function produces fixed length o/p

$H(M) = h$

3) Hash function $H(x)$ is relatively easy to compute for any given message x.

4) For any given hash value it is computationally infeasible to find x such that $\boxed{H(x) = h}$ → hash code / hash value

↓

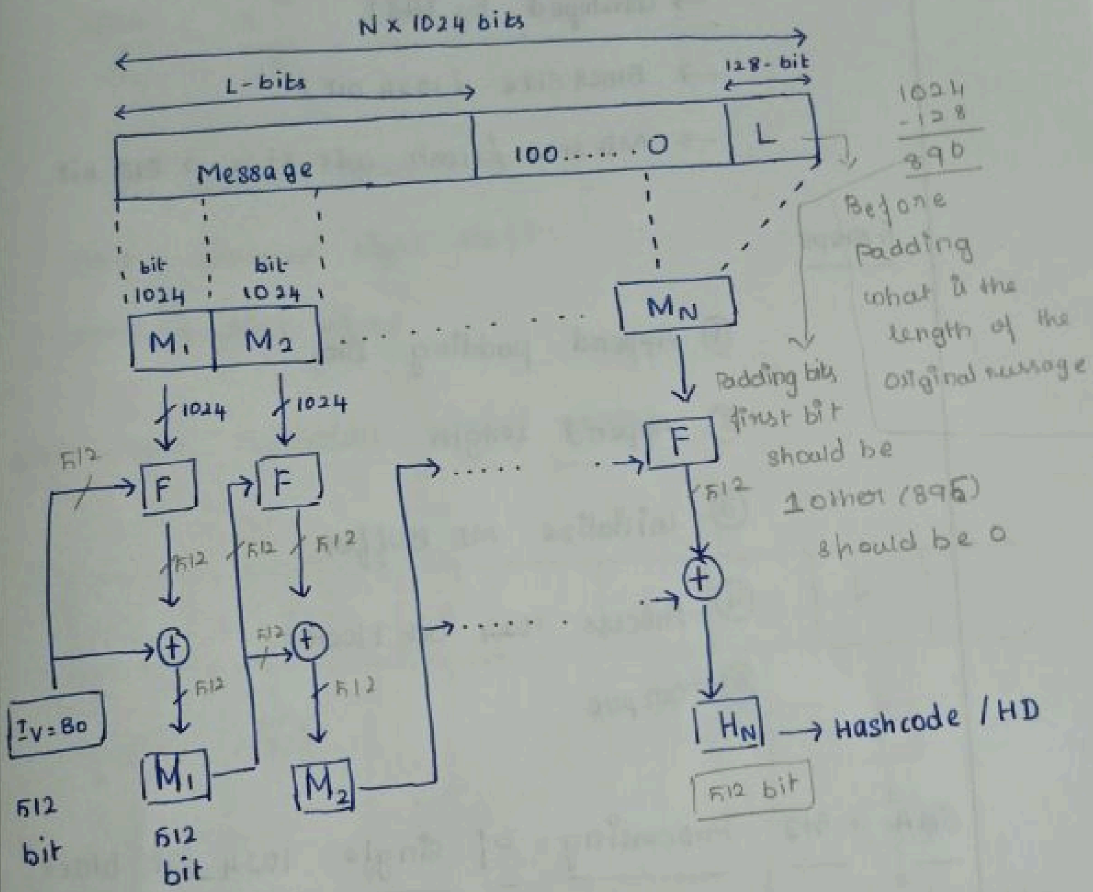
use only for authentication (no reverse process possible)

5) For any given block x it is computationally infeasible to find $y \neq x$ such that $H(y) = H(x)$

6) Strong collision resistance

↳ $H(x) \neq H(y)$

Message Digit Generation using 512- bit SHA :



1024
-128
890

Before padding what is the length of the original message

Suppose we have 1500 bits

then | 1024 | 476 | → make this equival to 1024 bits

476
+ 128 → length of original bit
604
+ 420 → padding bit
1024

first bit should be 1

Secure hash algorithm (SHA)

→ developed by NIST

→ Block size (1024 bit)

→ MD size / Hash code size => 512 bit

5 steps:

① Append padding Bits

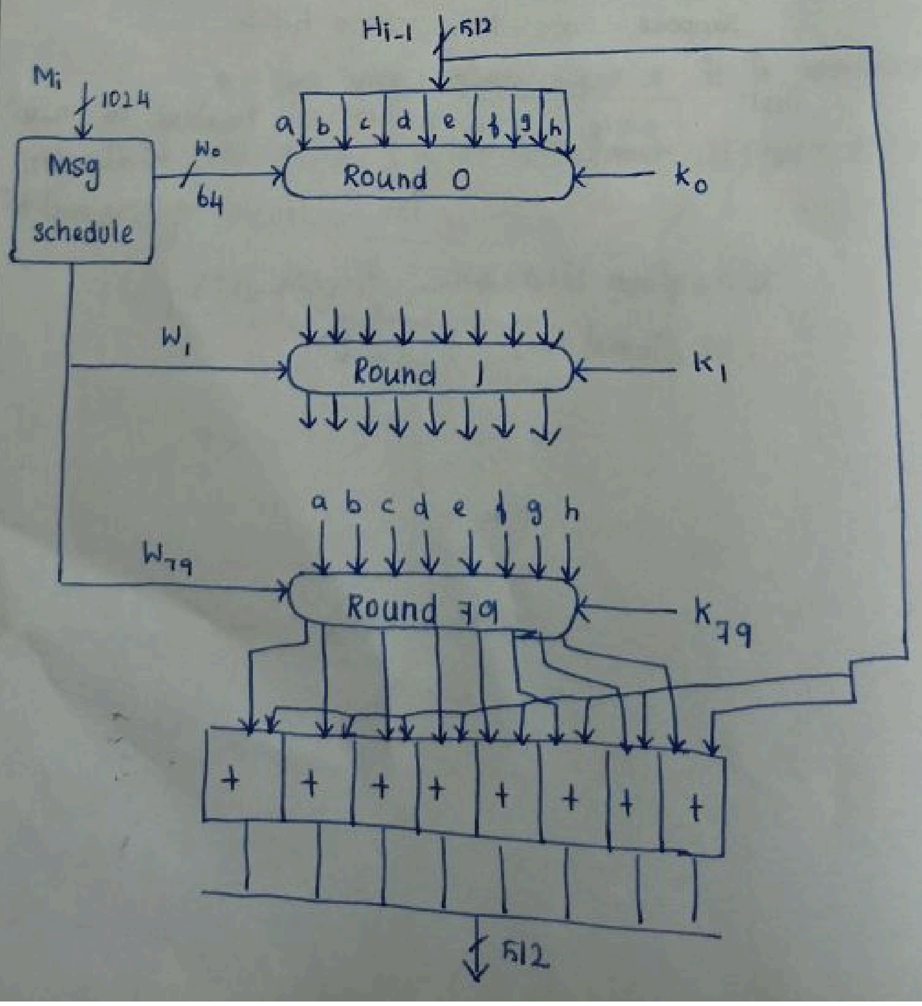
② Append length

③ Initialize MD Buffer

④ Process 1024 bit block

⑤ Output

SHA - 512 Processing of single 1024 bit block:



$\boxed{+}$ - addition modulo (2^{64})

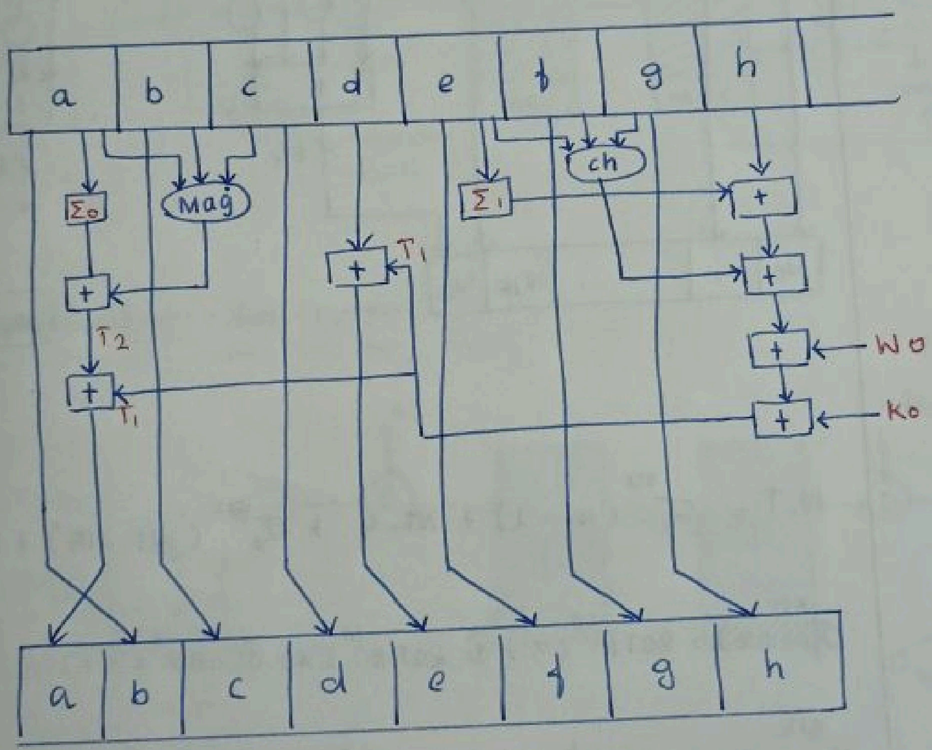
$$\frac{1024}{64} = \frac{2^{10}}{2^{6}} = 2^{4} = 64$$

K - constant value [Given]

ROTR - circular right shift

SHR → shift right

<u>SHA - 512 Operation single round</u> :



$b \leftarrow a$

$c \leftarrow b$

$d \leftarrow c$

$f \leftarrow e$

$g \leftarrow f$

$h \leftarrow g$

$a \leftarrow T_1 + T_2$

$e \leftarrow d + T_1$

$T_1 \leftarrow h + ch(e, f, g) + (\sum_{1}^{512} e) + W_t + K_t$

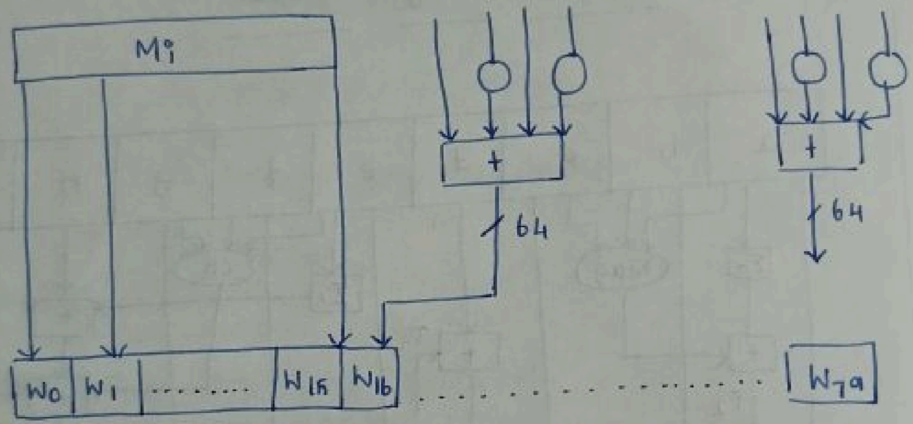
$T_2 \leftarrow (\sum_{0}^{512} a) + Maj(a, b, c)$

$ch(e,f,g) = (e \wedge f) \oplus (\sim e \wedge g)$

$Maj(a,b,c) = (a \wedge b) \oplus (a \wedge c) \oplus (b \wedge c)$

$\left(\sum_0^{512} a\right) = ROTR^{28}(a) \oplus ROTR^{34}(a) \oplus ROTR^{(39)}(a)$

$\left(\sum_1^{512} e\right) = ROTR^{14}(e) \oplus ROTR^{18}(e) \oplus ROTR^{41}(e)$

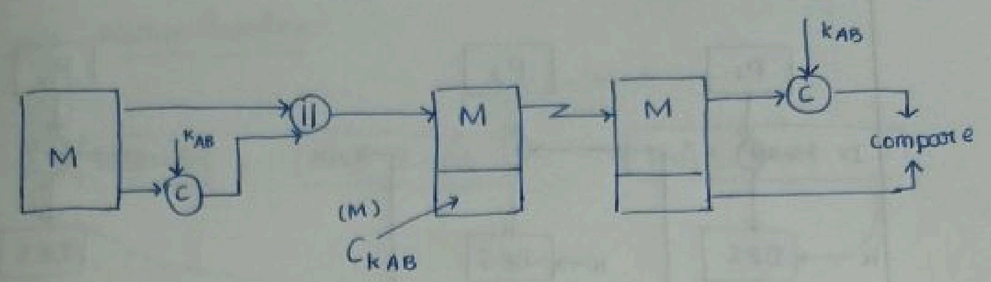


$W.T = \sigma_1^{512}(WT-2) + Wt-4 + \sigma_0^{512}(Wt-15) + WT-16$

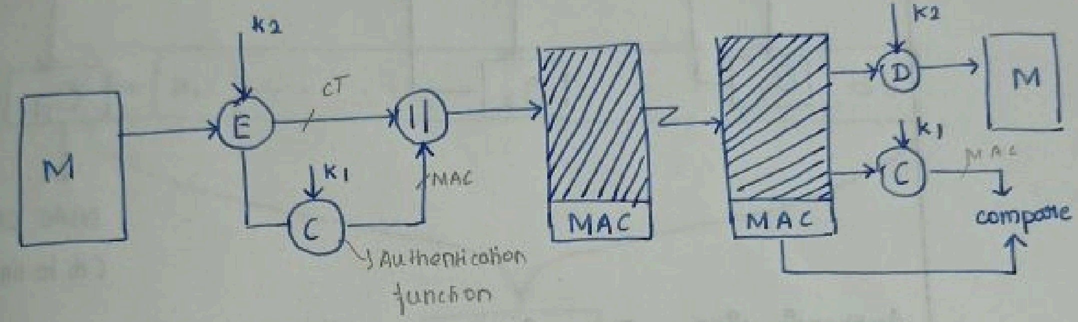
$\sigma_1^{512}(x) = ROTR^{19}(x) \oplus ROTR^{61}(x) \oplus SHR^{6}(x)$

$\sigma_0^{512}(x) = ROTR^{1}(x) \oplus ROTR^{8}(x) \oplus SHR^{7}(x)$

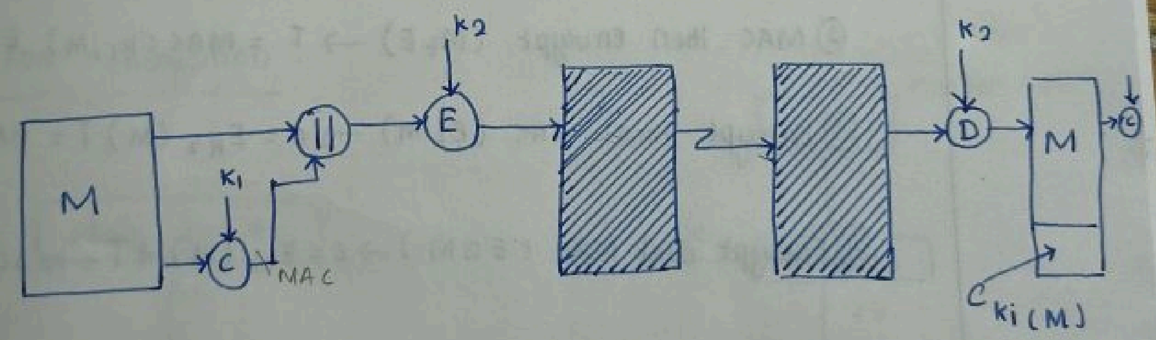
Message Authentication using MAC :



Authentication tied to CT :



Authentication tied to PT :



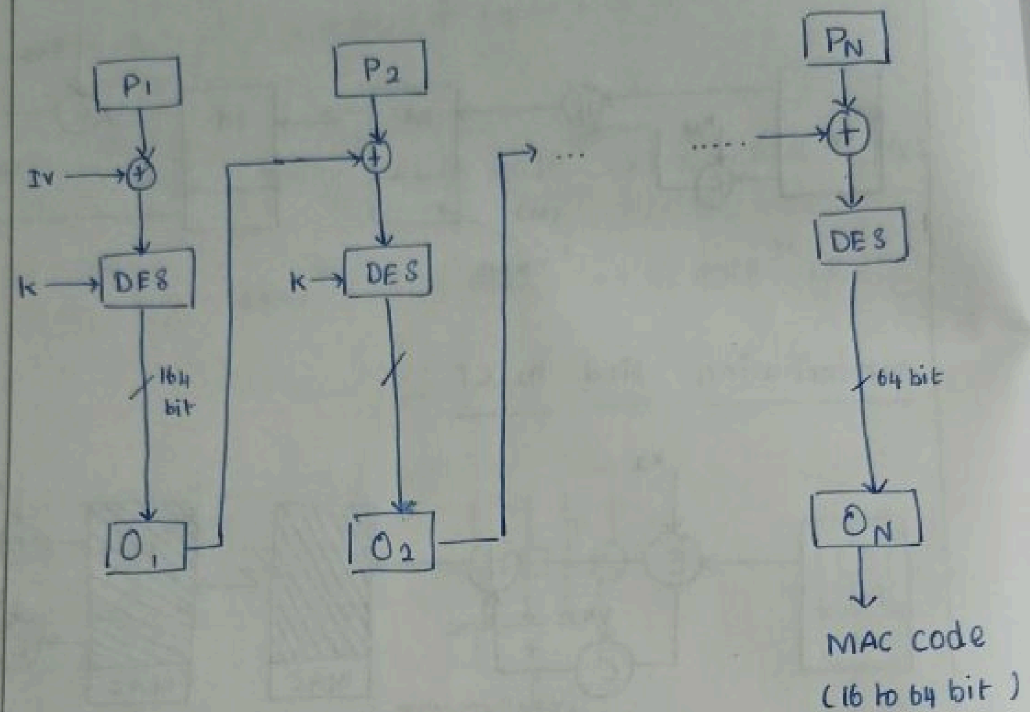
2 Algorithms :

① Data Authentication Algorithm (DAA)

② Cipher based Message Authentication code.

(CMAC)

DAA and CMAC :



Authentication Encryption :

① Hash then Encrypt ($H_t E$) $\rightarrow h = H(M)\ E_k(M \| h)$

② MAC - then Encrypt ($M_t E$) $\rightarrow T = MAC(K_1, M)\ EK_2(M \| T)$

③ Encrypt then MAC ($E_t M$) $\rightarrow c = E_{K2}(M)\ T = HAC(K, c)$

④ Encrypt and MAC ($E \& M$) $\rightarrow c = E_{k2}(M)\ \&\ T = MAC(K_1, M)$

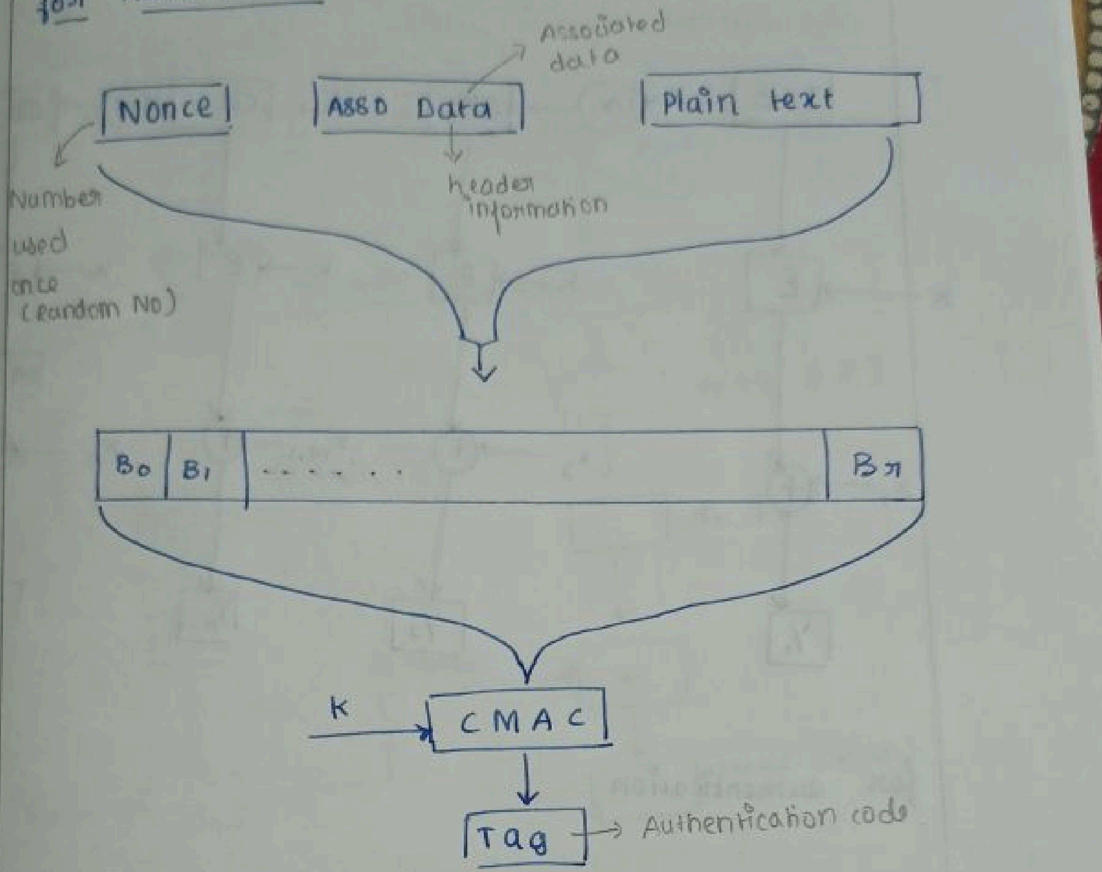
2 Algorithms :

→ counter with cipher block chaining model (CCM)

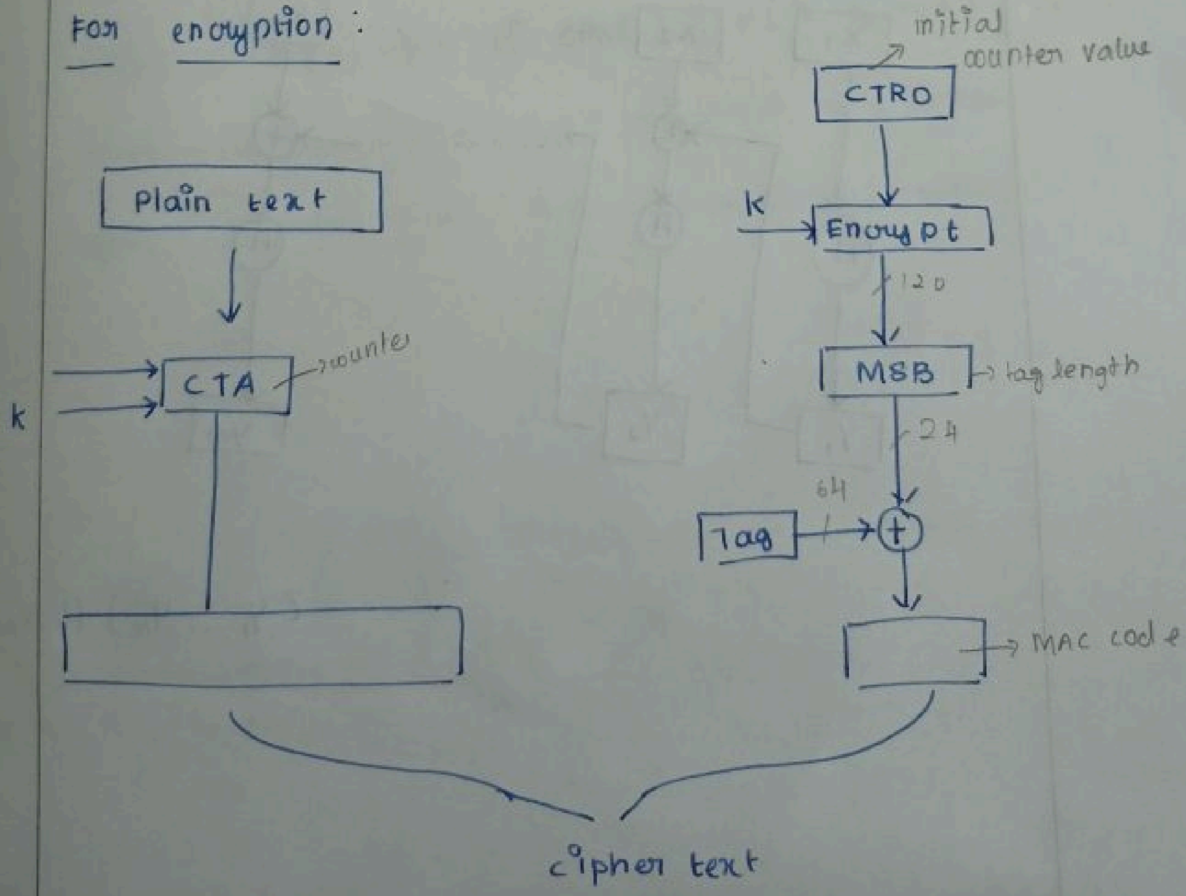
→ Galois counter mode (GCM).

CCM : (counter with cipher block chaining Msg Authentication code)

for Authentication :

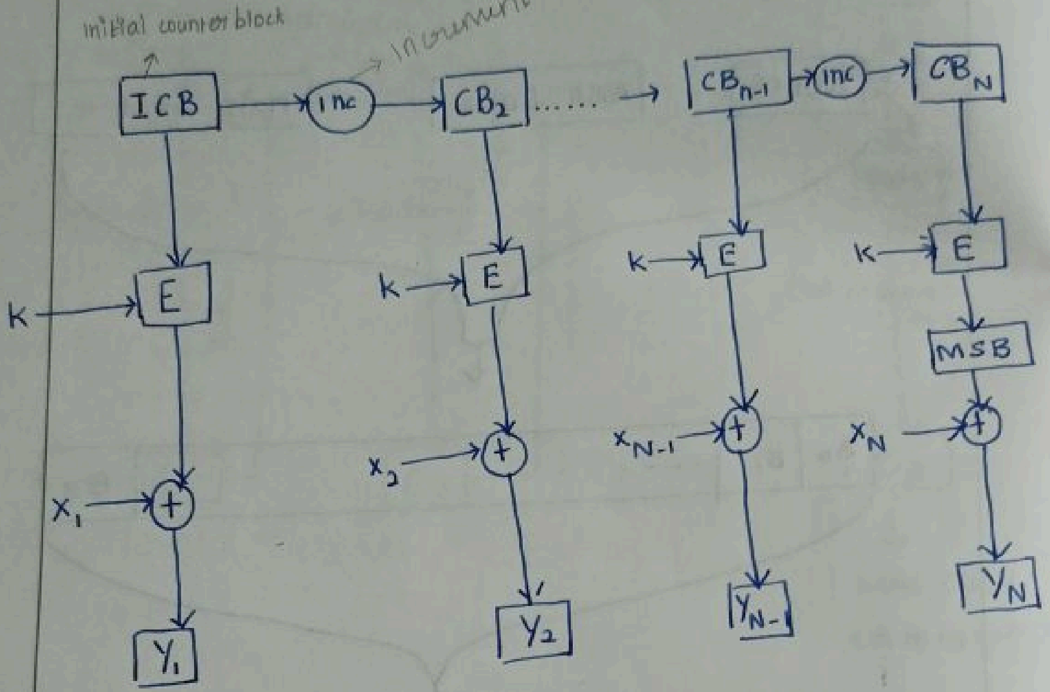


For encryption :

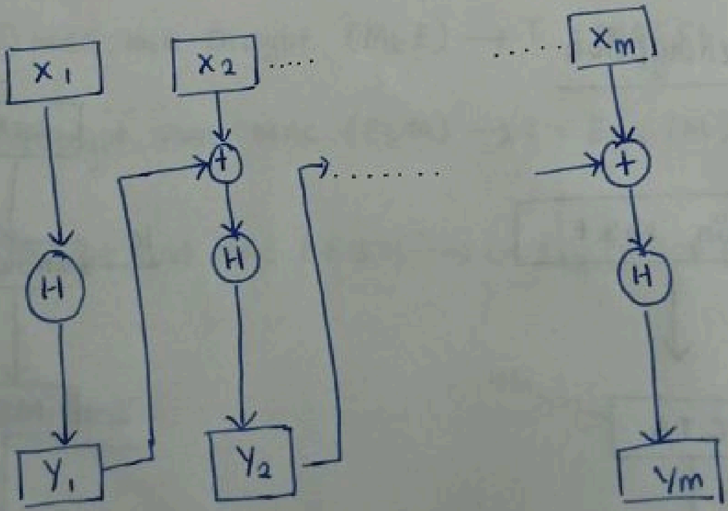


GCM :

for encryption



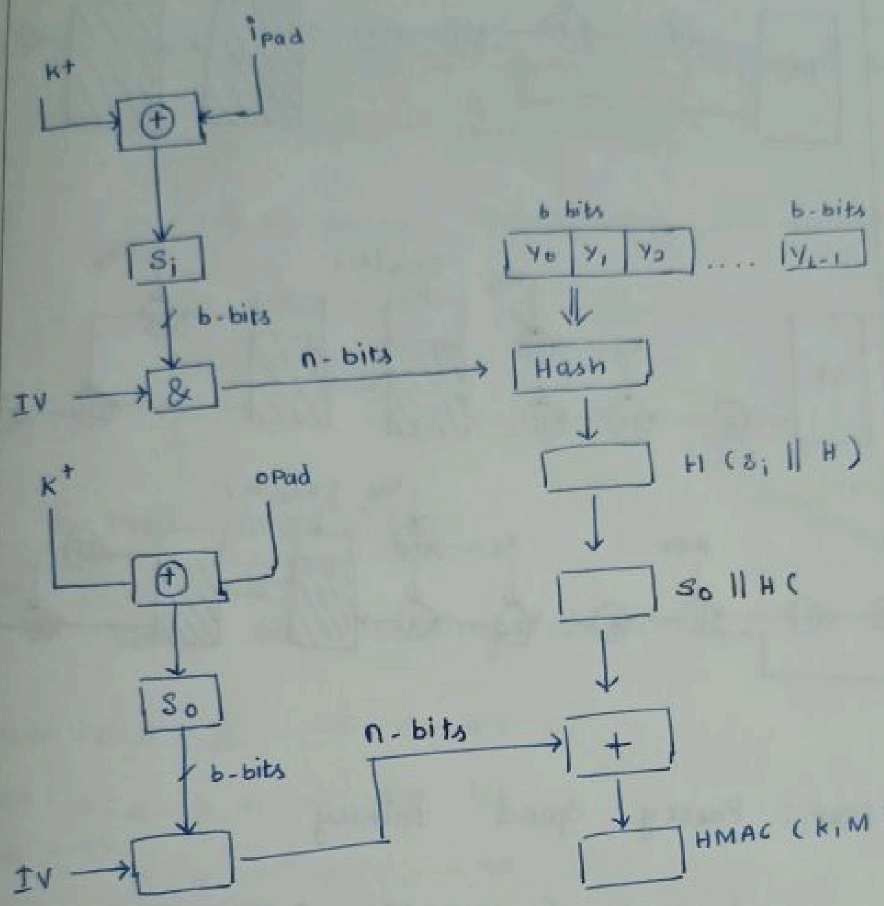
for authentication :



$(Y_1 \dots Y_N) \| Y_M$

C.T A.C

HMAC Structure :



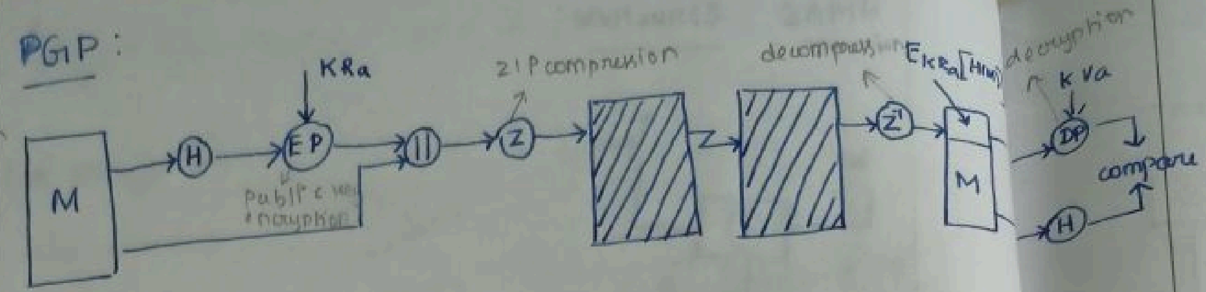
$\text{HMAC}(K, M) = H[(K^+ \oplus \text{OPad}) \| H(K^+ \oplus \text{iPad})]$

iPad ⟶ 0011 0110 (36) repeated b/8 times

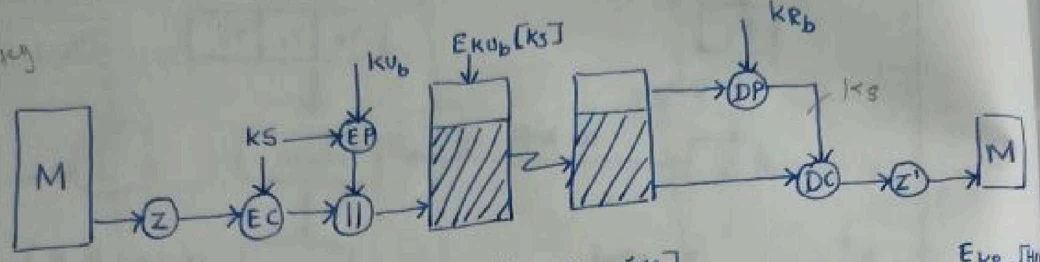
OPad ⟶ 0101 1100 (5C) repeated b/8 times.

PGP :

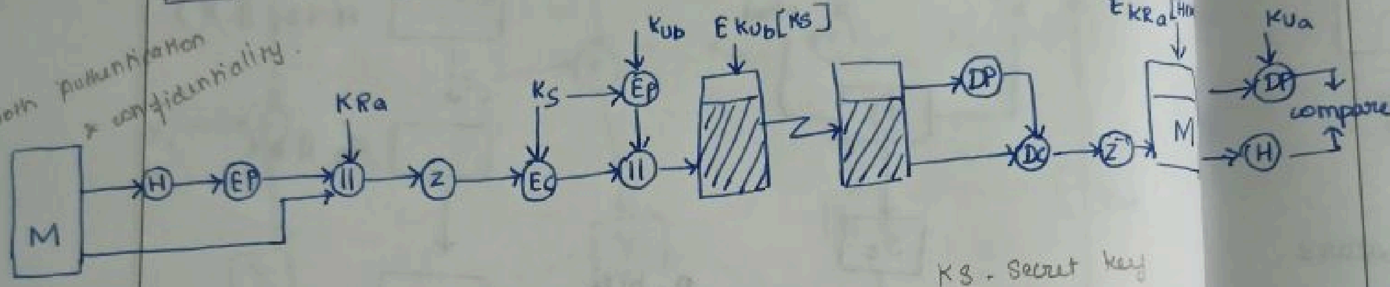
Authentication



confidentiality



Both authentication & confidentiality



KS - Secret key

EC - symmetric key encryption

DC - " " decryption

EP - Public key encryption

DP - " " decryption

Z^{-1} - decompression

Z - compression

PGP : Pretty Good Privacy

↳ developed by phil zimmerman

↳ Email security protocol

Services :

1. Authentication
2. confidentiality & Authentication
3. confidentiality
4. compression
5. Email compatibility
6. segmentation and reassembly.

MTU = max transfer unit

PGP uses

↳ compression done by ZIP compression and ZIP decompression.

↳ to archieve confidentiality and authentication

signature generation ⟶ compression ⟶ encryption.

E-mail compatibility:

Radix 64 Encoding / Decoding

A - Z ⟶ 0 - 25

a - z ⟶ 26 - 51

0 - 9 ⟶ 52 - 61

62 ⟶ +

63 ⟶ /

ABCDEF

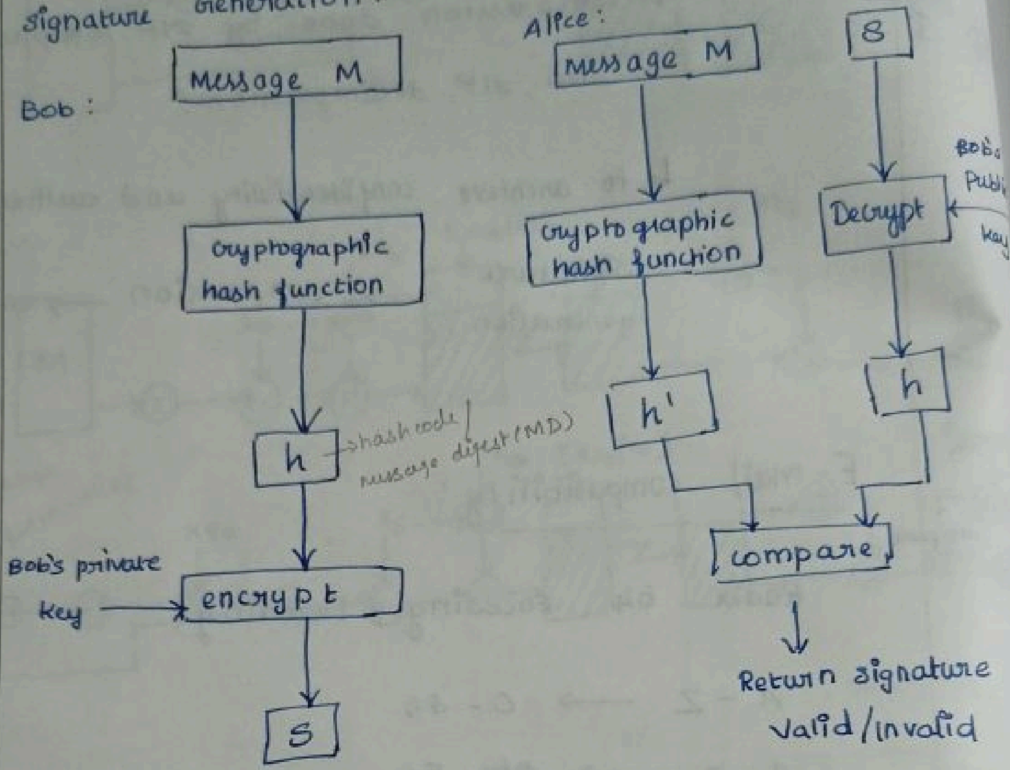
65 66 67

01000001 01000010 01000011

16	20	9	3
↓	↓	↓	↓
Q	U	I	D

Essential elements of DS process :

Signature Generation : signature verification :



3 Algorithm :

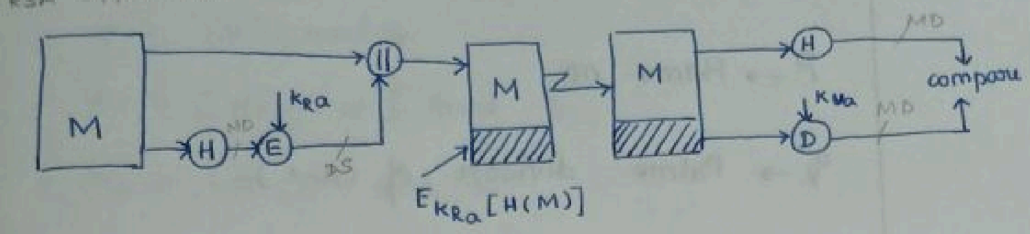
① Digital signature Algorithm / standard (DSA/DSS)

② Elgammal digital dignature

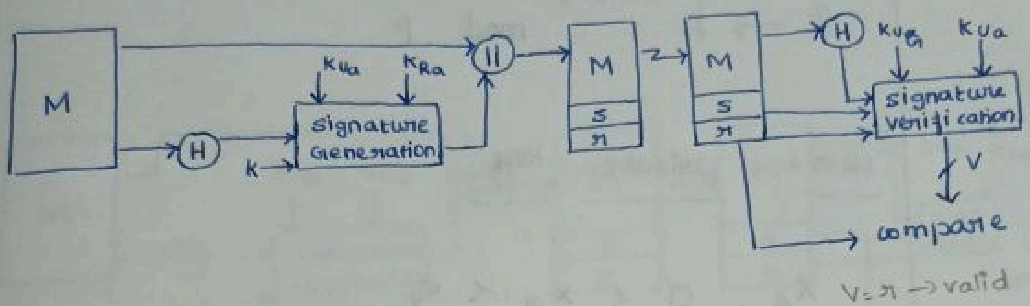
③ schnorr Digital signature .

DSA :

RSA approach



DSS approach



↳ developed by NIST

↳ proposed in 1991

↳ Revised in 1993

↳ Further Revision - 1996

↳ Expanded version 2002

① RSA approach

② DSS approach

Global key components:

$P \rightarrow$ Prime no

$q \rightarrow$ Prime divisor of $(p-1)$

$h \rightarrow 1 < h < (p-1)$

$g \rightarrow h^{(p-1)q} \mod P$

users private key:

$X_A,\ 0 < X_A < q$

user's public key:

$Y_A = g^{X_A} \mod P$

user's per message secret No:

$k,\ 0 < K < q$

Signature Generation:

$r = (g^k \mod p) \mod q$

$s = [K^{-1}(H(M) + X_A \cdot r)] \mod q$

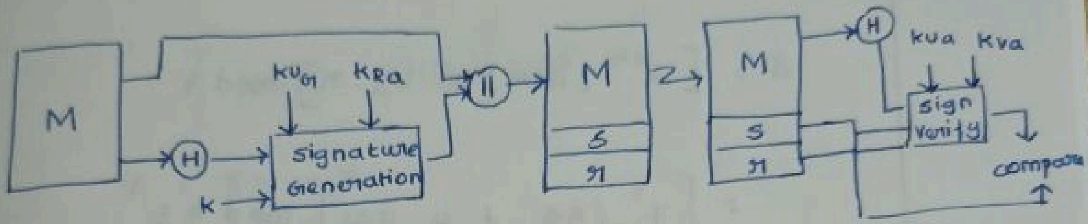
Signature Verification:

$$w = (s^{-1}) \bmod q$$

$$u_1 = [H(M)\, w] \bmod q$$

$$u_2 = (r \cdot w) \bmod q$$

$$v = \left[(g^{u_1} \cdot Y_A^{u_2}) \bmod p \right] \bmod q$$



Problem:

using DSA scheme let $q = 83$, $P = 997$ and $h = 4$ and the private key is 9 (X_A). determine signature value r and s by choosing users per msg secret number is 7 (k), assume $H(M) = 50$.

sol

$$g = h^{(p-1)/q} \bmod P$$

$$= 4^{996/83} \bmod 997$$

$$= 4^{12} \bmod 997$$

$$= 697$$

$$Y_A = g^{X_A} \bmod P$$

$$= 697^{9} \bmod 997$$

$$= 914$$

Signature value:

$r = (g^K \bmod p) \bmod q$

$1 -$
$0 - 1 \times 11$
$T_1 - T_2 \times Q$

$= (697^7 \bmod 997) \bmod 83$

Q	A	B	R	T_1	T_2	T
11	83	7	6	0	1	-1
1	7	6	1	1	-11	12
6	6	1	0	-11	12	
-	1	0	-	12		

$= 993 \bmod 83$

$r = 80$

$s = [K^{-1} . (H(M) + x_A . r)] \bmod q$

$= [7^{1} . (50 + 9 . 80)] \bmod 83$

$= [12 . (50 + 9 . 80)] \bmod 83$

$= [12 . (770)] \bmod 83$

$1 - (-3 \times 13)$
$0 - 1 \times 3$
$T_1 - T_2 \times Q$

$s = 27$

Q	A	B	R	T_1	T_2	T
3	83	27	2	0	1	-3
13	27	2	1	1	-3	40
2	2	1	0	-3	40	
-	1	0	-	40		

$w = s^{-1} \bmod q$

$= 27^{-1} \bmod 83$

$w = 40$

$u_1 = [H(m) w] \bmod q$

$= [50 . 40] \bmod 83$

$= 8$

$u_2 = (r.w) \bmod q$

$= (80 . 40) \bmod 83$

$= 46$

$V = [(g^{u_1} . Y_A^{u_2}) \bmod p] \bmod q$

$= [(697^8 . 914^{46}) \bmod 997] \bmod 83$

$= [(203 . 442)] \bmod 83$

$V = 80 = r$

Elgammal Digital Signature :

X_A - sign's private key

Y_A - sign's public key

(A)

① Generate a Random integer X_A, $1 < X_A < q-1$

② compute $Y_A = \alpha^{X_A} \bmod q$

signing

① choose a random integer K, $1 \le K \le q-1$

② compute $S_1 = \alpha^K \bmod q$

$M = H(M)$

$0 \le M \le q-1$

③ compute $K^{-1} \bmod (q-1)$

④ compute $S_2 = K^{-1}(M - X_A S_1) \bmod (q-1)$

Verification :

$A \xrightarrow{M \,\&\, (S_1, S_2)} B$

① compute $V_1 = \alpha^m \bmod q$

② compute $V_2 = (Y_A^{S_1})(S_1)^{S_2} \bmod q$

Problem :

$\alpha = 10$, $q = 19$, $X_A = 16$, $K = 5$ $\quad m = 14$

sol

$Y_A = \alpha^{X_A} \bmod q$

$= 10^{16} \bmod 19$

$= 4$

Q	A	B	R	T_1	T_2	T
3	18	5	3	0	1	-3
1	5	3	2	1	-3	4
1	3	2	1	-3	4	-7
2	2	1	0	4	-7	
	1	0		-7		

$-3-(4\times1)$

$(-1-3\times1)$

$0-1\times3$

$T_1 - T_2 \times Q$

$S_1 = \alpha^K \bmod q$

$= 10^5 \bmod 19$

$= 3$

$S_2 = K^{-1}(M - X_A S_1) \bmod (q-1)$

$= 11(14 - 16\,3) \bmod 18$

$= -374 \bmod 18$

$= -14$ ~~mod 18~~

$= 4$

verify :

$V_1 = \alpha^m \bmod q$

$= 10^{14} \bmod 19$

$= 16$

$V_2 = (4)^3 (3)^4 \bmod 19$

$= 16$

$\boxed{V_1 = V_2}$ $\therefore$ signature is valid.

Problem :

User A is signing a document using elgammal signature scheme she is using $q = 67$, $\alpha = 17$. She chooses $X_A = 15$ for her private exponent.

(1) What is user A's public key (Y_A)

(2) If user A choose a random integer $k = 5$. Demonstrate how user A signs the document $M = 50$

(3) How does user B verify that signature of user A.

$0 - 1 \times 13$

$T_1 - T_2 \times Q$

Q	A	B	R	T_1	T_2	T
13	66	5	1	0	1	-13
5	5	1	0	1	-13	
		1	0		-13	

sol

(i) $Y_A = \alpha^{X_A} \bmod q$

$= 17^{15} \bmod 67$

$= 59$

(ii) $S_1 = \alpha^{K} \bmod q$

$= 17^{5} \bmod 67$

$= 60$

$S_2 = K^{-1}(M - X_A S_1) \bmod (q-1)$

$= 53\,(50 - 15 \cdot 60) \bmod 66$

$= -38 \quad = 28$

(iii) $V_1 = 17^{50} \bmod 67$

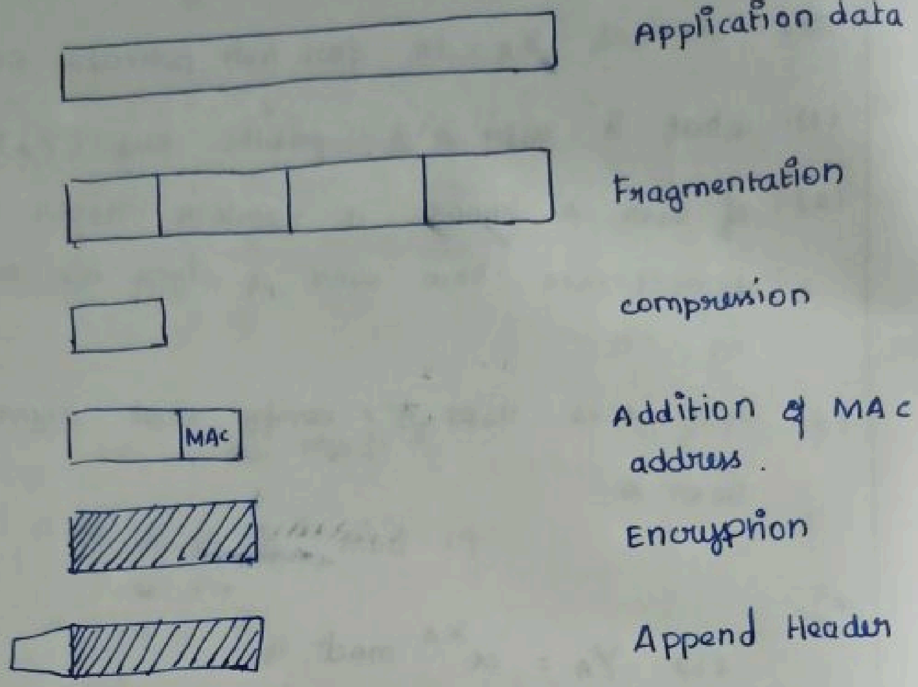
$= 33$

$V_2 = (59)^{60}\,(60)^{28} \bmod 67$

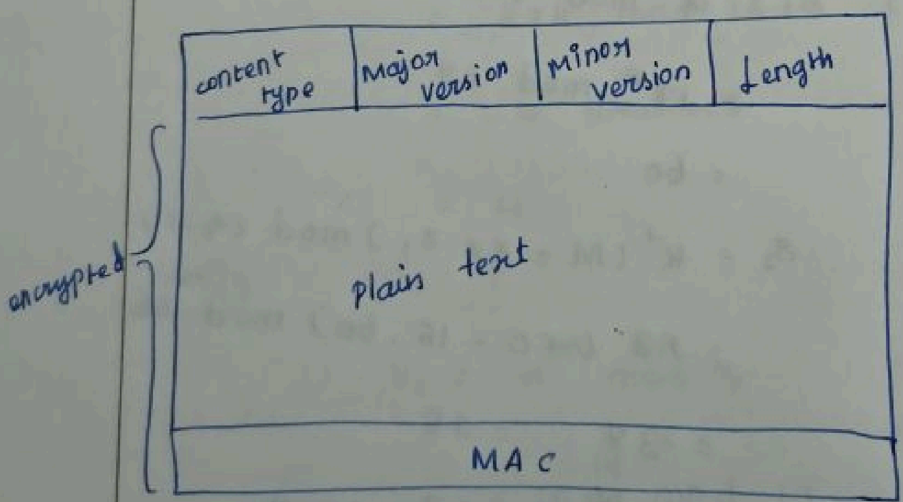
$= 33$

$V_1 = V_2$

Record Protocol :



Find o/p after ssl record Protocol operation :



SSL Provides :

↳ confidentiality

↳ Authentication .

SSL - Handshake Protocol

↳ Record

↳ Alert (2m)

Schnorr Digital Signature:

Key Generation:

① choose prime, P and q → is a prime factor of (p-1)

② choose an integer a, $a^{q} \equiv 1 \mod P$ → Global key

③ choose a random integer S_A, $0 < S_A < q$ → private key

④ calculate $V_A = a^{-s} \mod p$. (V_A → public key)

Signature Generation:

① choose a random integer r, $0 < r < q$ & computer $\boxed{x = a^{r} \mod p.}$

② concatenate the message with x of hash the result to compute e.

$$\boxed{e = H(M \| x)}$$

③ compute $\boxed{y = (r + S_A e) \mod q}$

Verification:

$$Ⓐ \xrightarrow{M \| (y,e)} Ⓑ$$

① compute $x' = a^{y} V_A^{e} \mod P$

② Verify $e' = H(M \| x')$

$$\boxed{H(M \| x) = H(M \| x')}$$

if $e = e'$, then signature is valid.

Problem:

Alice wants to send a message M = 400 along with digital signature to user Bob. she chooses Schnorr DS system with $p = 997$ $q = 83$ $a = 9$ $r = 11$ $S_A = 23$

assume the hash value for the concordinated message and function ie $e = 81$.

find the public key, signature for the message and verify the signature also.

sol

$$V_A = a^{-SA} \bmod P$$

$$= 9^{-23+q} \bmod 997$$

$$= 9^{-23+83} \bmod 997$$

$$= 9^{60} \bmod 997$$

$$V_A = 421$$

$$x = a^r \bmod P$$

$$= 9^{11} \bmod 997$$

$$= 67$$

$$e = H(M \| x)$$

$$= H(400 \| 67)$$

$$= H(40067)$$

$$e = 81$$

$Y = (r + s_A \cdot e) \bmod q$

$= (11 + 23 \cdot 81) \bmod 83$

$= 1874 \bmod 83$

$= 48$

$x' = a^Y V_A^e \bmod P$

$= (9^{48}\ 421^{81}) \bmod 997$

$= (877\ \ 421^{81}) \bmod 997$

$= (887\ \ 257) \bmod 997$

$= 67$

$H(M \| x')$

$H(400 \| 67)$

$H(40067)$

$= 81$

$\therefore\ H(M \| x) = H(M \| x')$