ELGAMAL CRYPTOSYSTEM :-

Global Public Elements

q	prime number
α	$\alpha < q$ and α is a primitive root of q.

Key Generation by Alice

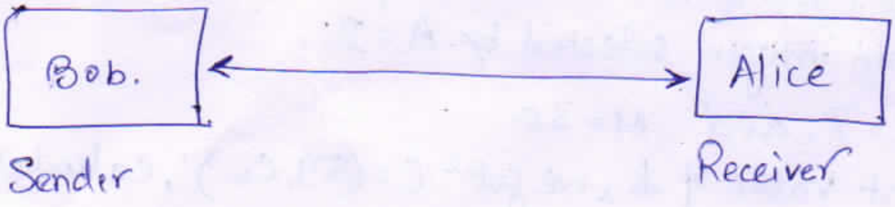
Select Private X_A	$X_A < q-1$
Calculate Y_A	$Y_A = \alpha^{X_A} \bmod q$
Public key	$PU = \{q, \alpha, Y_A\}$
Private key	X_A

Encryption by Bob with Alice's Public key

Plain Text	$M < q$
Select random integer k	$k < q$
Calculate K	$K = (Y_A)^k \bmod q$
Calculate C_1	$C_1 = \alpha^k \bmod q$
Calculate C_2	$C_2 = KM \bmod q$
Cipher Text	(C_1, C_2)

Decryptionby Alice with Alice's Private key.

Cipher Texr	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plain Text	$M = (C_2 K^{-1}) \bmod q$.



Example :- $q = 19$.

Primitive roots of 19 => $\{2, 3, 10, 13, 14, 15\}$

so $\alpha = 10$.

Alice generates a key pair as follows :

i) $X_A = 5$.

ii) $Y_A = \alpha^{X_A} \bmod q = 10^5 \bmod q = 3$.

iii) Public key $PU = \{19, 10, 3\}$.

Private key $= 5$.

Bob wants to send the message with value $M = 17$ then,

i) Bob select $k = 6$.

ii) Calulate $K = (Y_A)^k \bmod q = (3)^6 \bmod 19 = 7$

iii) Calulate C_1 & C_2

$C_1 = \alpha^k \bmod q = 10^6 \bmod 19 = 11$

$C_2 = KM \bmod q = (7 \times 17) \bmod q = 5$

iv) Bob sendscipher text $(11, 5)$.

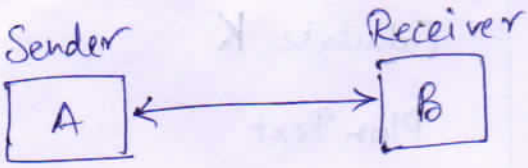
For Decryption :-

i) Alice Calulate $K = (C_1)^{X_A} \bmod q = (11)^5 \bmod 19 = 7$.

ii) $K^{-1} = 7^{-1} \bmod 19 = 11$.

iii) Finally $M = (C_2 K^{-1}) \bmod q = (5 \times 11) \bmod q = 17$.

Example :-



1) $q = 71$, and $\alpha = 7$.

Calculate cipher text for $M = 30$ and
Y_B = public key of $B = 3$. and
k = random integer selected by $A = 2$.

2). $q = 71$, $\alpha = 7$. and $M = 30$.
For different value of k, we got $C = (59, C_2)$, calulate C_2.

MESSAGE AUTHENTICATION :-

→ It is a mechanism used to verify the integrity of a message.

→ It is a procedure to verify that received messages come from the alleged source and have not been altered.

AUTHENTICATION FUNCTIONS :- It is a some sort of function that produces an authenticator: a value to be used to authenticate a message.

3 types of functions that may be used to produce an authenticator.

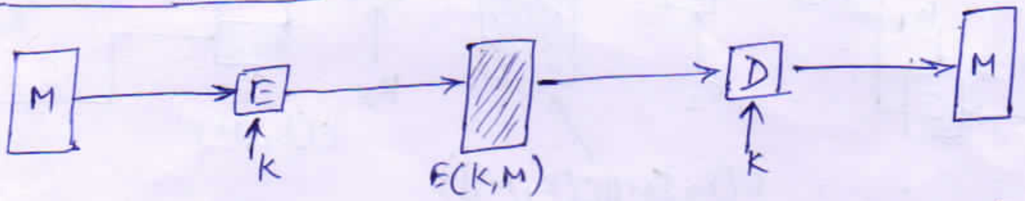
i) Message Encryption :- The cipher text of the entire message serves as its authenticator.

ii) Message Authentication code (MAC) :- A function of the message and a secret key that produces a fixed-length value that serves as the authenticator.

iii) Hash function :- A function that maps a message of any length into a fixed-length hash value, which serves as the authenticator.

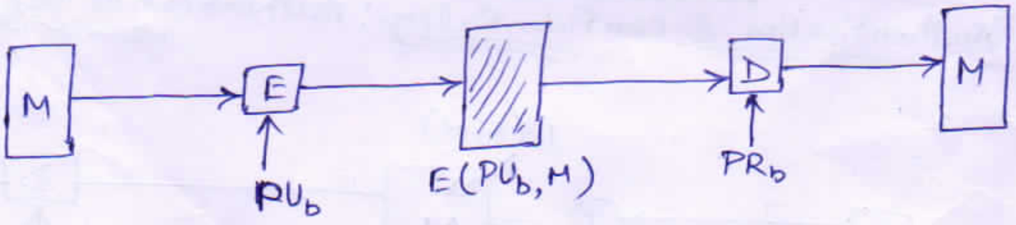
MESSAGE ENCRYPTION :-

(i)



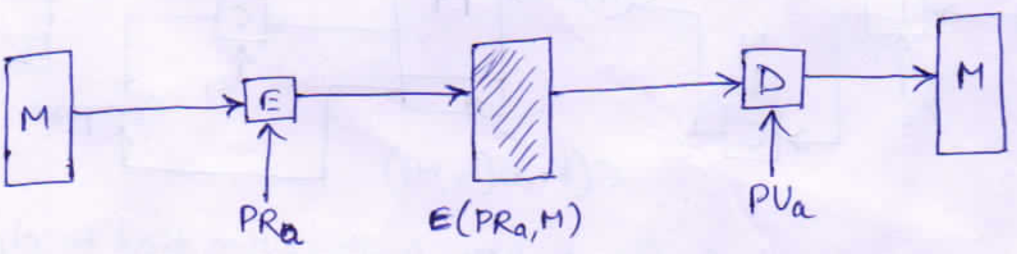
{Symmetric Encryption}

(ii)



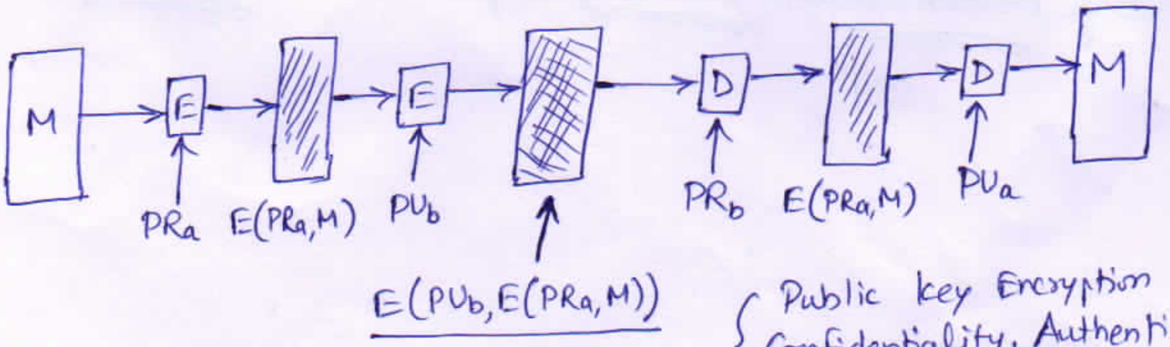
{Public-key Encryption} Confidentiality.

(iii)



{Public-key Encryption Authentication} & Signature

(iv)



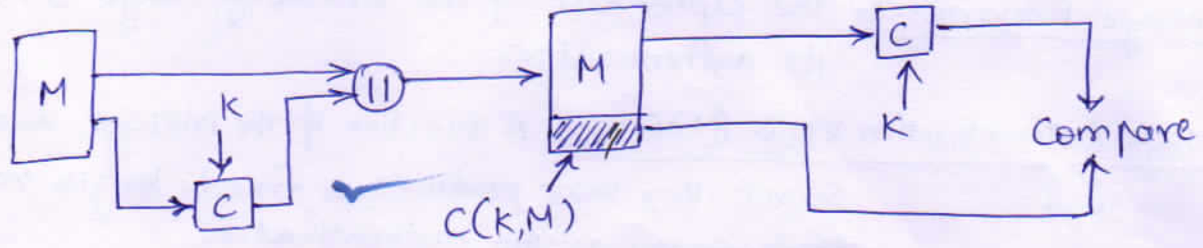
{Public key Encryption Confidentiality, Authentication & Signature}

MESSAGE AUTHENTICATION CODE :-

In this, a secret key is used to generate a small fixed-size block of data, known as a cryptographic checksum or MAC, that is appended to the message.

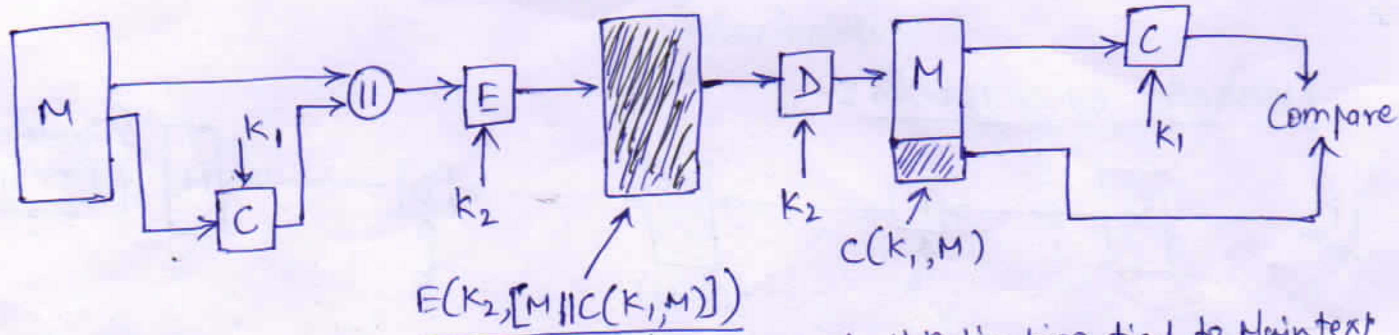
M = input message
C = MAC function
K = shared secret key.
MAC = message authentication code.

(i)



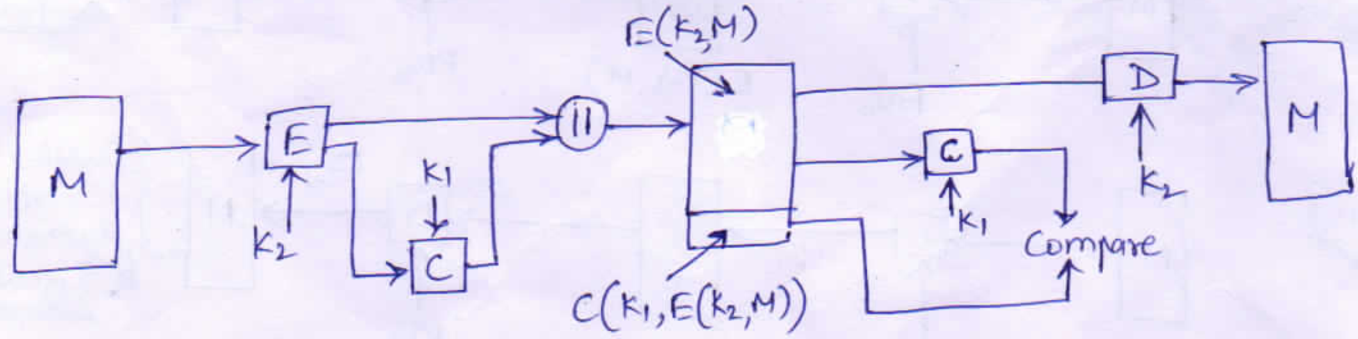
Message Authentication.

(ii)



Message Authentication & Confidentiality : Authentication tied to plaintext

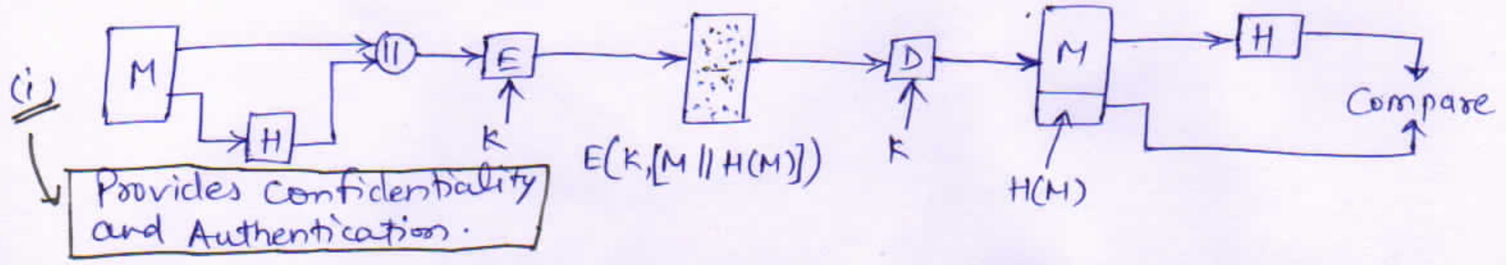
(iii)



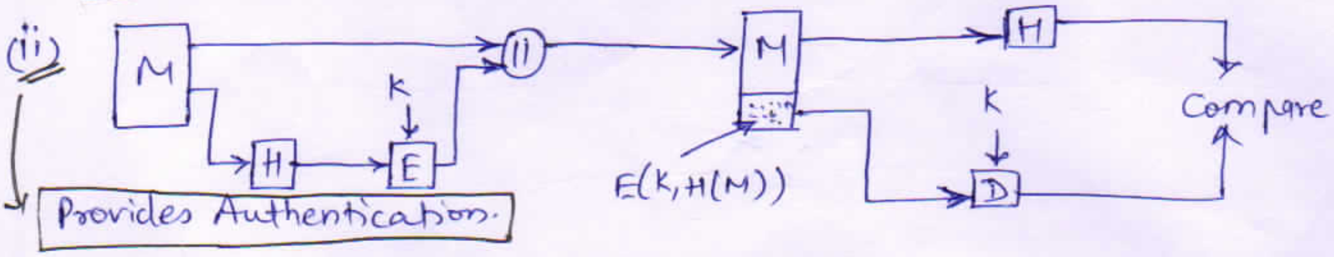
Message Authentication & Confidentiality : Authication tied to ciphertext

HASH FUNCTION:- It accepts a variable size message & produces a fixed-size output, referred to as a Hash code. H(M).

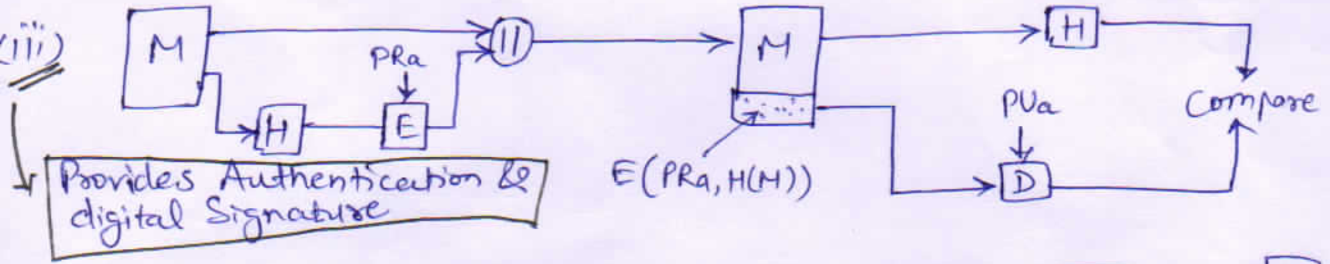
→ Hash code does not use a key but it is a function only of the input message



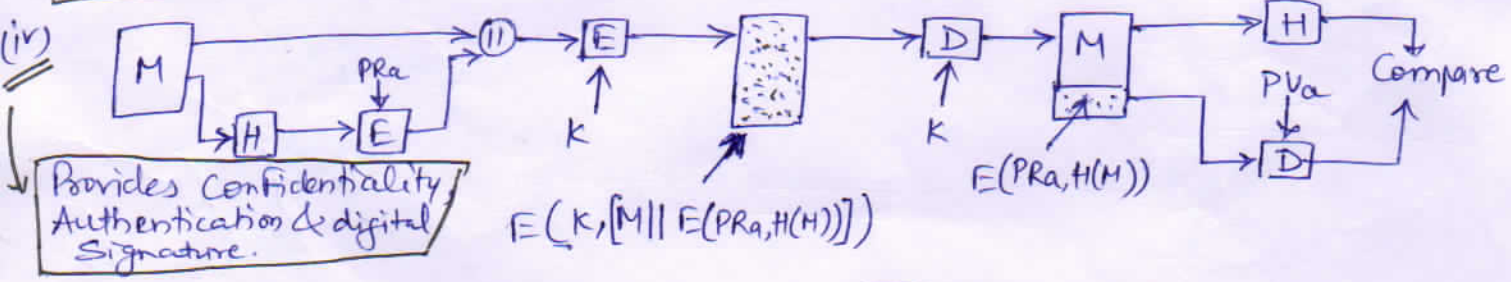
Provides Confidentiality and Authentication.



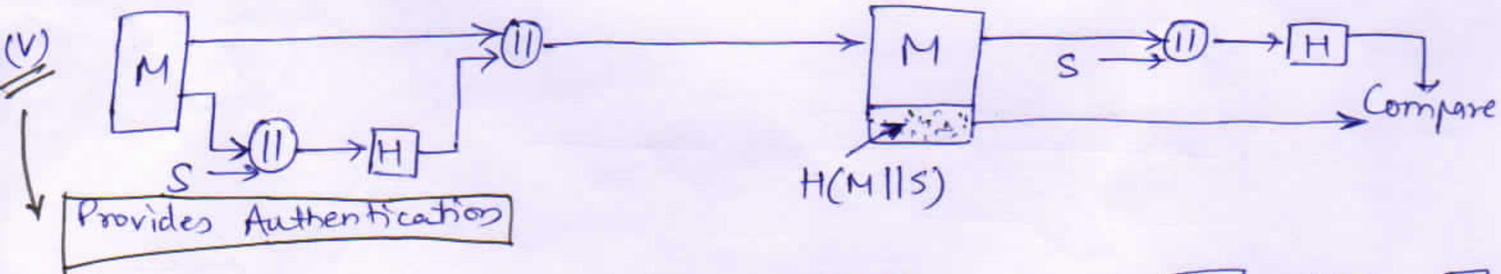
Provides Authentication.



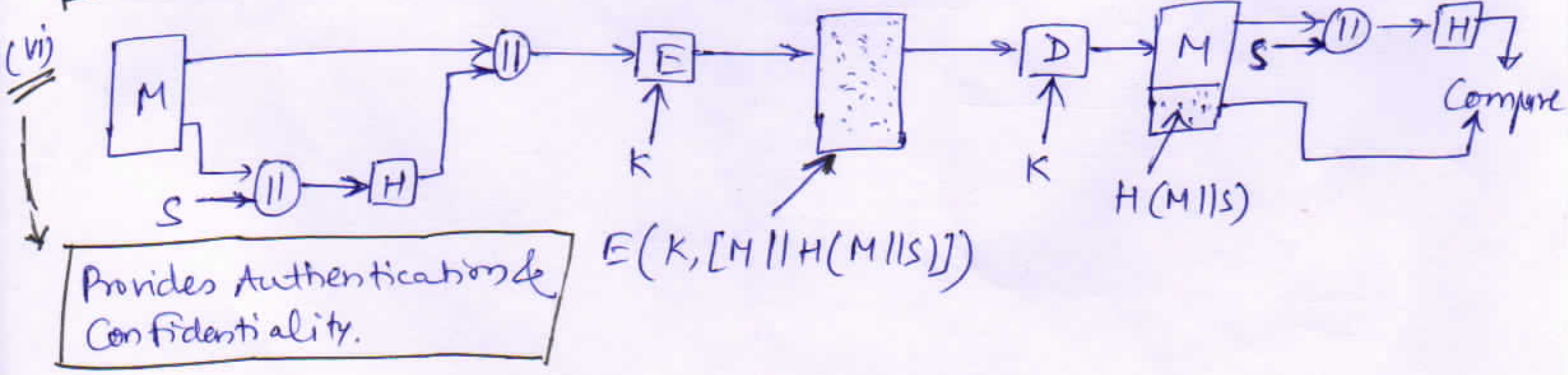
Provides Authentication & digital Signature



Provides Confidentiality Authentication & digital Signature.



Provides Authentication



Provides Authentication & Confidentiality.