ELGAMAL CRYPTO-SYSTEM :-

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)

Decryption by Alice with Alice's Private key.	
Cipher Text	(C_1, C_2)
Calculate K	$K = (C_1)^{X_A} \bmod q$
Plain Text	$M = (C_2 K^{-1}) \bmod q$.

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.

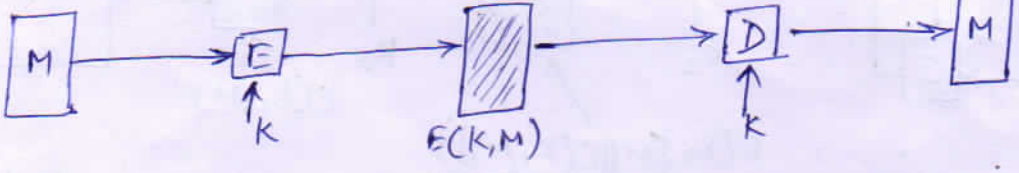
i) **Message Encryption :-** The cipher text of the entire message serves as its authenticator.

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)

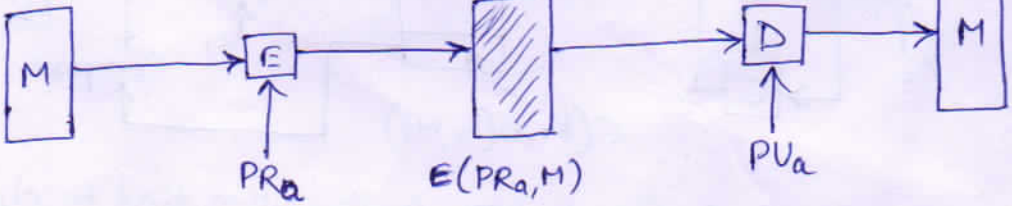


{Symmetric Encryption}

(ii)

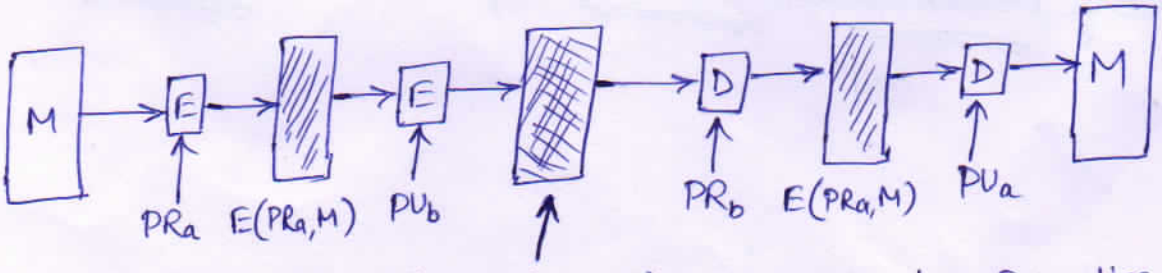
{Public-key Encryption
Confidentiality.}

(iii)



{Public-key Encryption
Authentication & Signature}

(iv)



E(PUb, E(PRa, M))

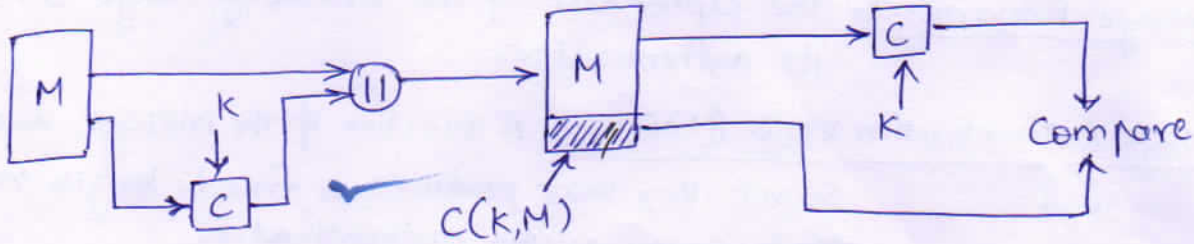
{Public key Encryption
Confidentiality, Authentication & Signature}

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.

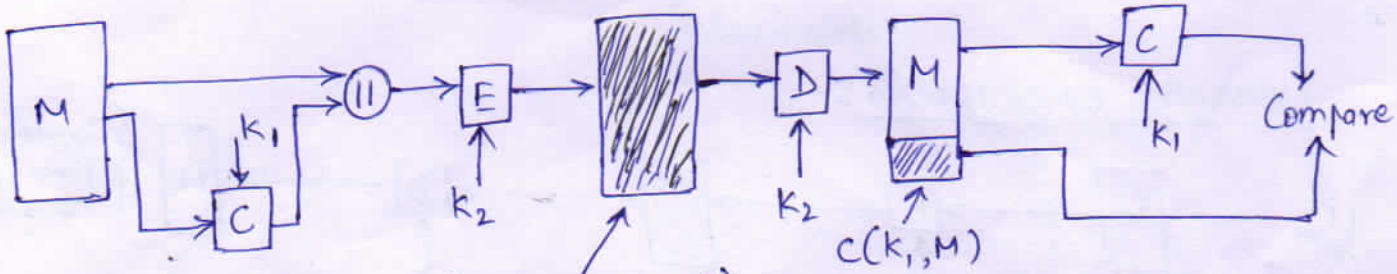
M = input message
C = MAC function
K = shared secret key.
MAC = message authentication code.

(i)



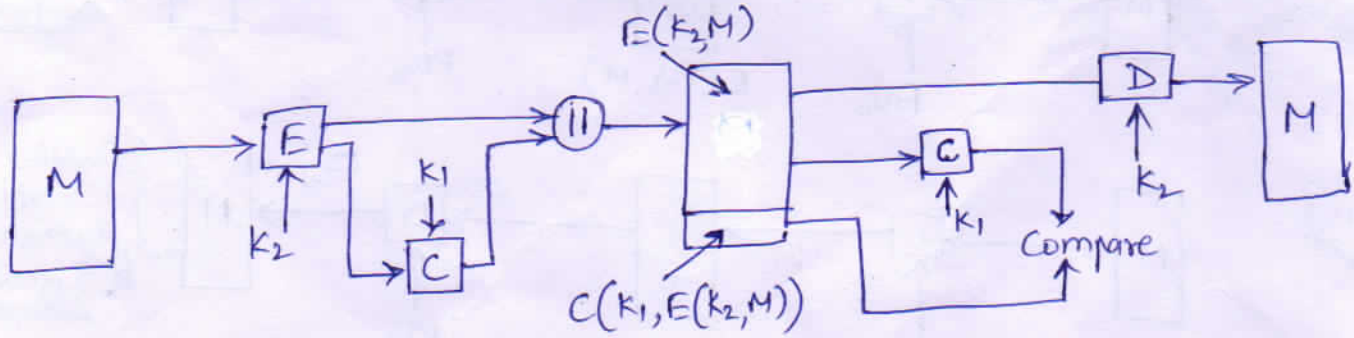
Message Authentication.

(ii)



Message Authentication & confidentiality : Authentication tied to plaintext

(iii)

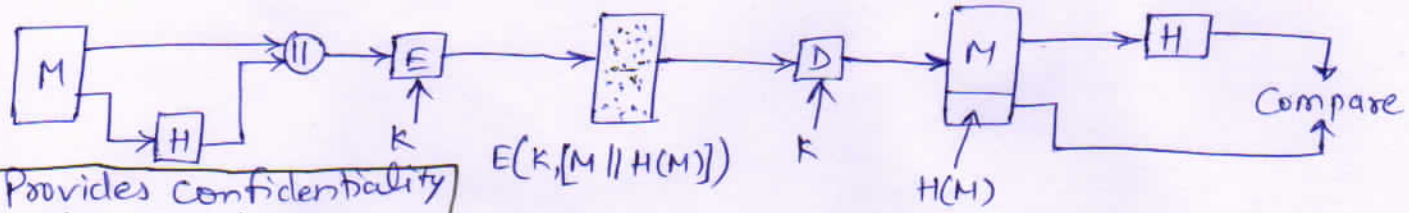


Message Authentication & Confidentiality : Authication tied to ciphertext

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

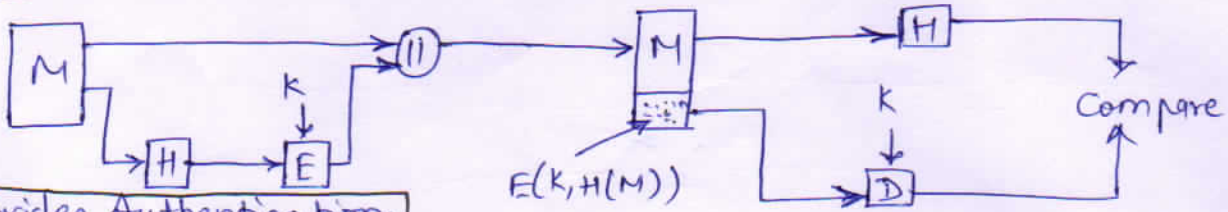
→ Hash code does not use a key but it is a function only of the input-message

(i)



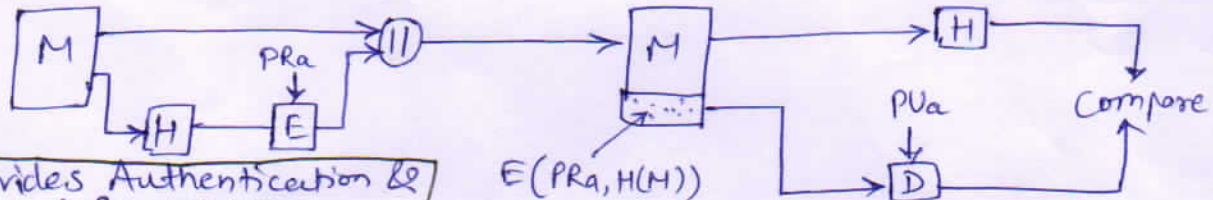
Provides Confidentiality and Authentication.

(ii)



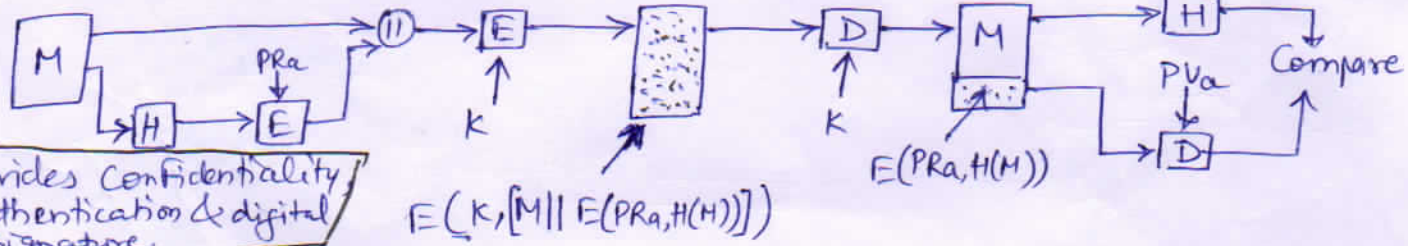
Provides Authentication.

(iii)



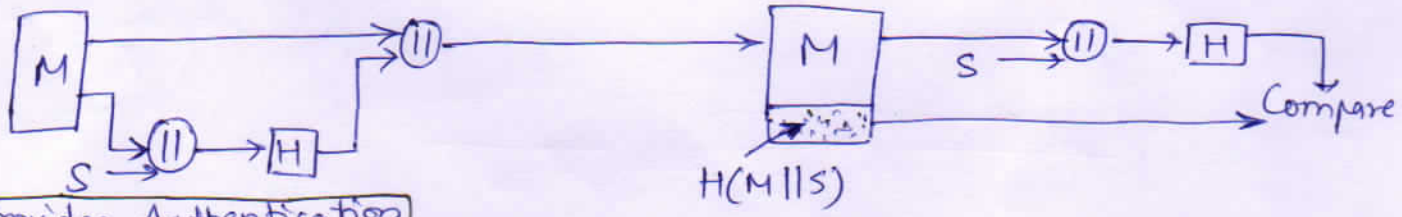
Provides Authentication & digital Signature

(iv)



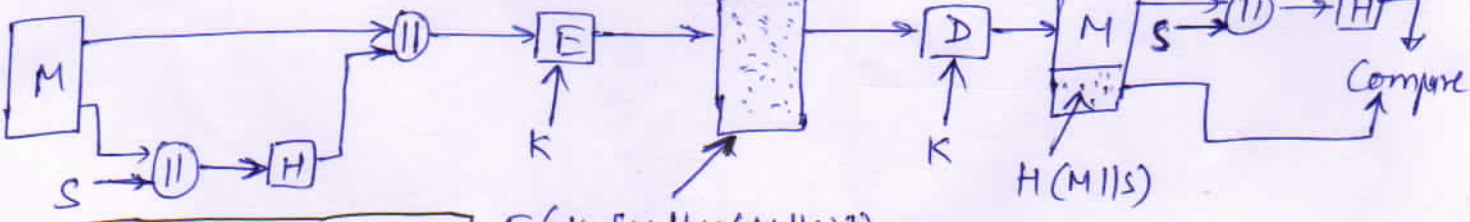
Provides Confidentiality Authentication & digital Signature.

(v)



Provides Authentication

(vi)



Provides Authentication & Confidentiality.