

(a) Public key cryptography is a class of cryptographic is based on algorithms. Public key cryptography uses a pair of keys to encrypt & decrypt data to protect is against unauthorized access on use.

- If other users want to encrypt data, they get the intended recipient's public key from a public directory.
- This key is used to encrypt the message & to send it to the recipient. When the message arrives the recipient decrypts it using a private key, to which no one else has access.
- RSA algo. is the cryptography system that is used for public key, which is commonly used when sending secure, sensitive data over an insecure network like the internet.

(b) AES : — The more popular symmetric encryption algorithm likely to be encountered nowadays is AES [Advanced Encryption Standard].

- Symmetric key symmetric Block cipher.
- 128 bit data, keys.
- Stronger & faster than Triple-DES.
- Provide full specification & design details.
- It is based on 'substitution-permutation networks. It comprises of series of linked operations.

(2)

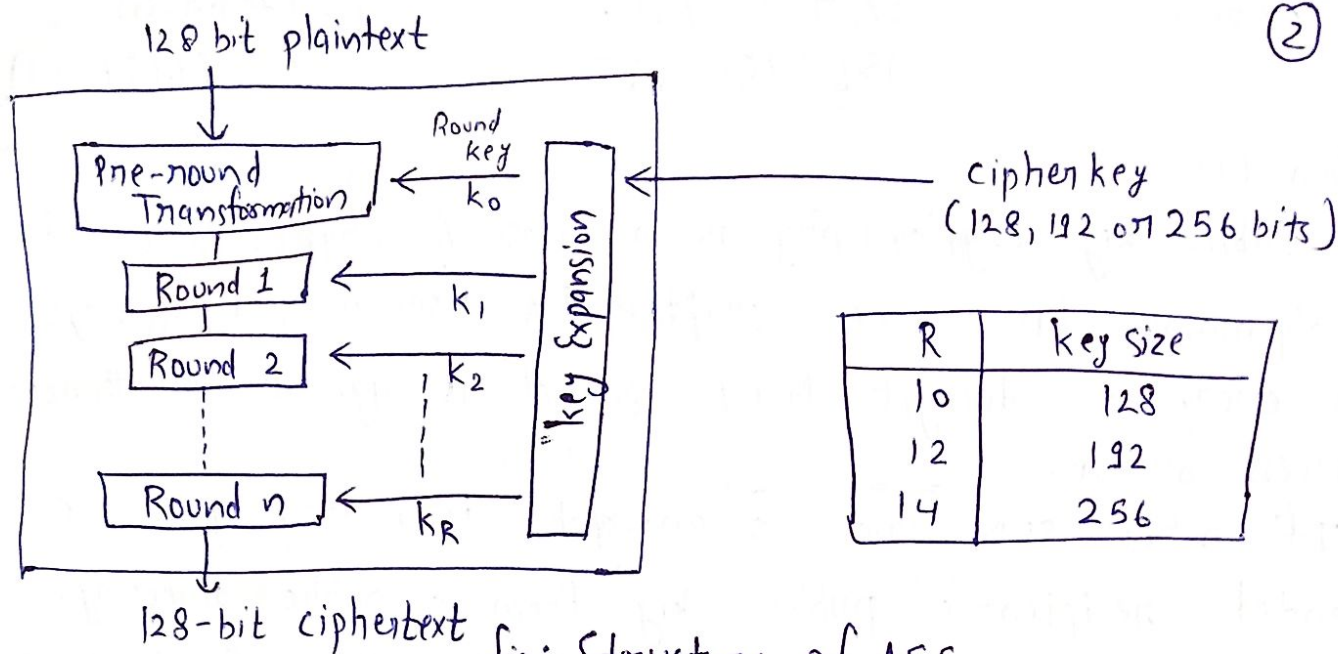


fig: Structure of AES

AES Transformation Function:-

- (i) Substitution
- (ii) Permutation
- (iii) Mixing
- (iv) key Adding

(i) Substitution \Rightarrow AES Uses two invertible transformations SubBytes, GF Field.

(ii) Permutation \Rightarrow Another transformation found in a round is shifting, which permutes the bytes.

(iii) Mixing:- We need an interbyte that changes bits inside a byte, based on bits inside neighboring bytes.

(iv) key Adding:- AddRoundkey Proceeds one column at a time. It adds a round key with each state.

(c) Stream Cipher \Rightarrow It is a symmetric key cipher where plaintexts are combined with a pseudorandom cipher digit stream.

In this, each, plaintext digit is encrypted one at a time with corresponding digit of keystream,

to give a digit of ciphertext stream.

→ The algo. modes which are based in stream cipher are CFB & DFB.

(3)

Block Cipher: - It is an encryption method that applies a deterministic algo. along with symmetric key to encrypt a block of text, rather than encrypting one bit at a time.

Eg- AES encrypts 128 bit Block with key of predetermined length 128, 192 or 256 bits.

(d) Euler's totient Function \Rightarrow It is a multiplicative function, meaning that if two numbers m & n are relatively prime, then

$$\phi(mn) = \phi(m) \phi(n).$$

This function gives order of multiplicative group of integers modulo n . It is also used for defining the RSA Encryption system.

It counts the no. of integers b/w 1 & n inclusive, which are coprime to n . Two no are coprime if their greatest common division equals 1.

$$1 \leq p < \infty \quad \phi(p) = p - 1$$

$$k \geq 1 \quad \phi(p^k) = p^k - p^{k-1}$$

$$\phi(n) = n \cdot \left(1 - \frac{1}{p_1}\right) \left(1 - \frac{1}{p_2}\right) \left(1 - \frac{1}{p_3}\right) \dots \left(1 - \frac{1}{p_k}\right)$$

Fermat's Theorem: - It states that no three positive integers a, b & c satisfy the equation $a^n + b^n = c^n$ for any integer value of n greater than 2.

The cases $n=1$ & $n=2$ have been known since antiquity to have infinitely many solutions. (4)

→ It states if p is a prime number then for any integer ~~multiple of p~~ a , the no. $a^p - a$ is an integer multiple of p .

$$a^p \equiv a \pmod{p}$$

Special case: If a is not divisible by p , Fermat's little theorem is equivalent to statement that $a^{p-1} - 1$ is an integer multiple of p .

• (e) Output Feedback Mode:- OFB is a mode of operation for a block cipher. It has some similarities to ciphertext feedback mode in that it permits encryption of differing block sizes, but has key difference that o/p of encryption block function is the feedback.

→ The bit errors in transmission do not propagate in the encryption.

$$C_j = P_j \otimes E(k, [C_{j-1} \otimes P_j])$$

$$P_j = C_j \otimes E(k, [C_{j-1} \otimes P_j])$$

Counter Mode:- In cryptography, a sophisticated mode of operation. Counter mode uses an arbitrary number that changes with each block of text encrypted. The counter is encrypted with cipher and result is XOR'd into ciphertext.

→ CTR mode is independent of feedback use & thus can be implemented in parallel in this mode.

Key-6 Electronic Code Book :- It is a mode of operation for a block cipher with characteristic that each possible block of plaintext has a defined corresponding ciphertext value & vice-versa. The same plaintext value will always result in the same ciphertext value.

→ It is used when a volume of plaintext is separated into several block of data, each of which is then encrypted independently of other blocks.

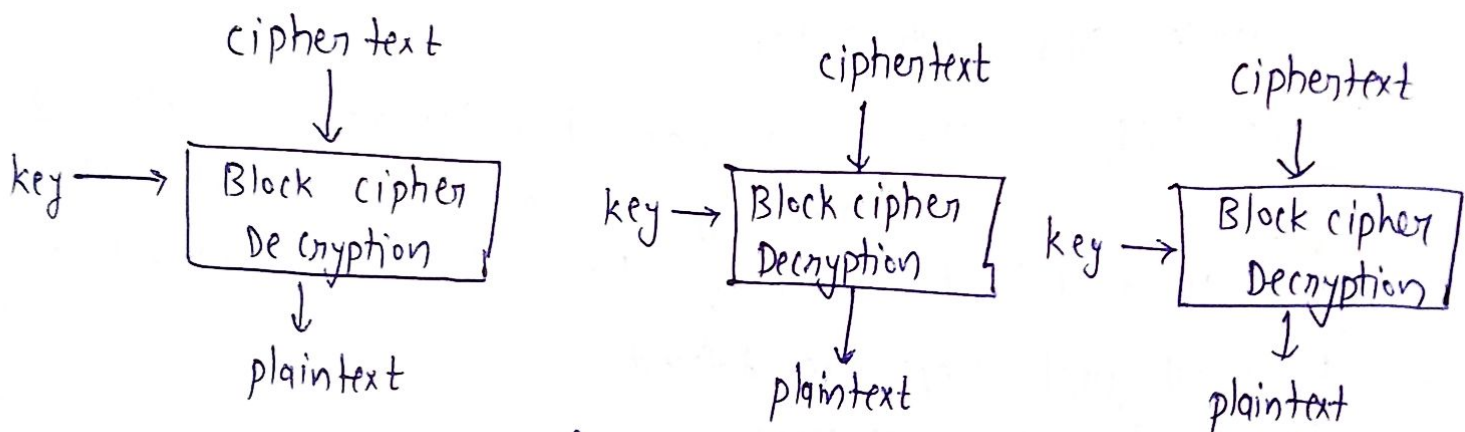


fig:- ECB mode decryption

Cipher Block Chaining (CBC) It is a mode of operation for block cipher and in which a sequence of bits are encrypted as a single unit on block with a cipher key applied to the entire block. CBC uses initialization vector of a certain length by using this along with single encryption key.

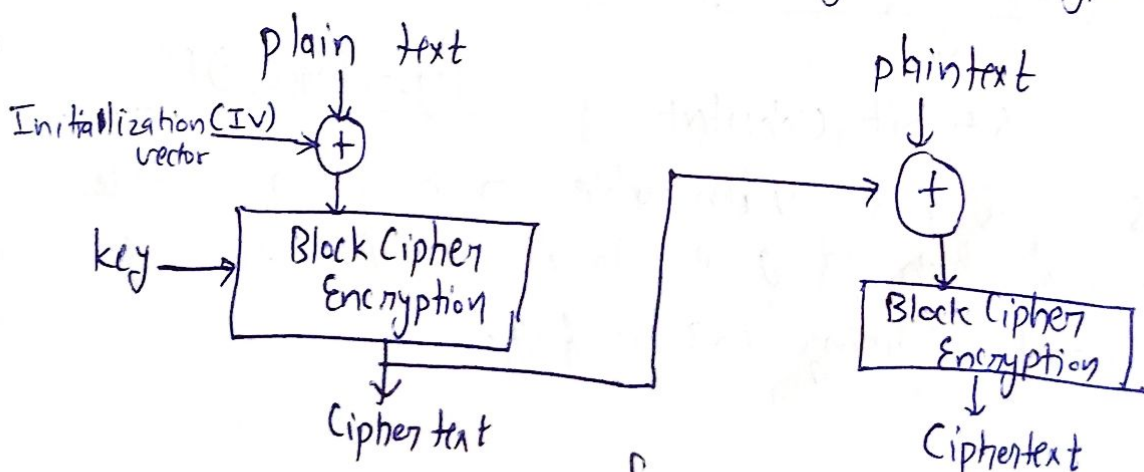


fig:- CBC mode Encryption

Ans-⑤ Multiple Encryption:- It is a technique in which an encryption algo is used multiple times. Plaintext is converted to ciphertext using encryption algo.
→ It is for enhancing effect of cryptographic algo for an application, such as applying a block cipher to a sequence of data blocks or data stream.

Multiple Encryption Techniques:-

- Double DES
- Triple DES with 2 keys
- Triple DES with 3 keys

Triple DES:- It is an encryption technique which uses 3 instance of DES on same plaintext. It uses three different types of keys choosing techniques:-

- First all used keys are different.
- Second 2 keys are same.
- Third all keys are same.

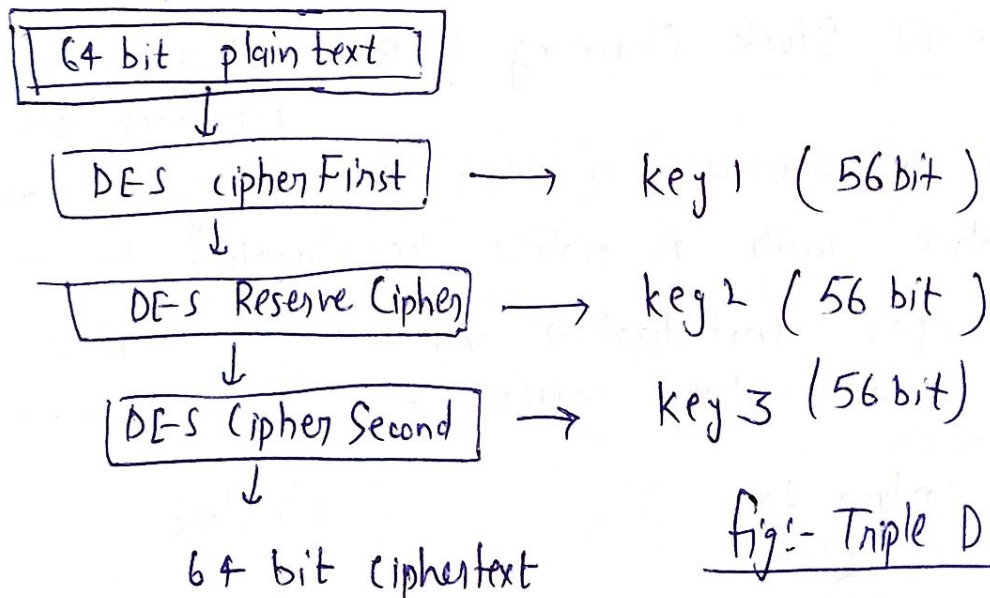


Fig:- Triple DES

→ Triple DES is also vulnerable to meet in middle-attack coz of which it give total security level of 2^{112} instead of using 168 bit of keys.

Ans - (2) RSA algo. is asymmetric cryptography algo. (7)
Asymmetric actually means that it works on 2 different keys i.e. Public & Private key.

→ The public key consists of 2 numbers where one number is multiplication of 2 large prime numbers and private key is also derived from same two prime no. so if somebody can factorize large no., the private key is compromised.

→ The RSA keys can be typically 1024 or 1028 bits long.
Steps to work on RSA algo.:-

Step-① Generate RSA modulus $N = p \cdot q$

Step-② Desired no. (e)

Step-③ Public key (n & e)

Step-④ Private key (d) $\Rightarrow ed = 1 \pmod{(p-1)(q-1)}$

(Encryption) $C = P \pmod n$ | Plaintext = $C \pmod n$ (decryption)

Advantage :-

(a) RSA is stronger than any other symmetric key algo. ~~and~~ and advantage of RSA algo in cryptography are Authenticity and privacy.

Disadvantage:- → It has got too much computation.

→ It is complex.

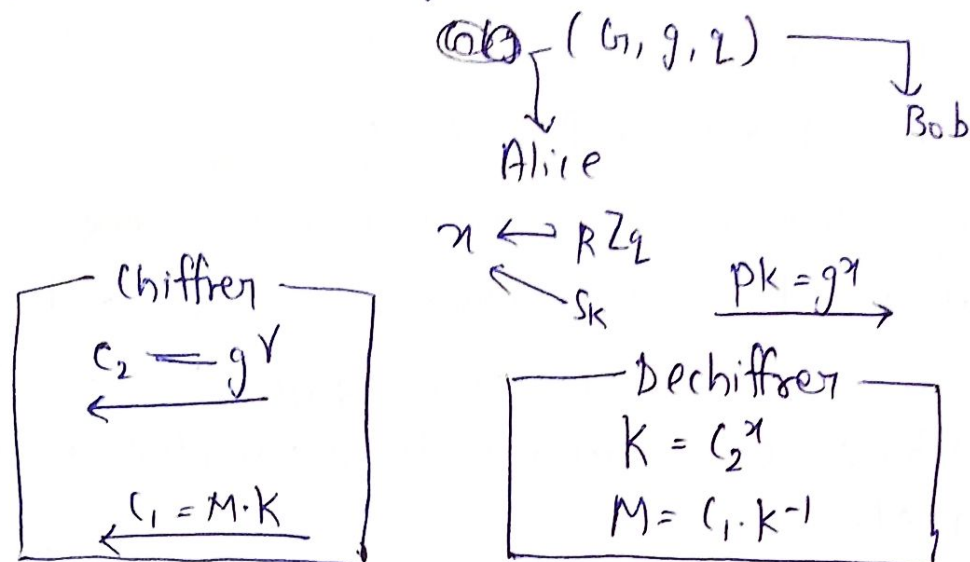
Ans - (4) Elgamal cryptosystem:-

It is an asymmetric key encryption algo. for

public key cryptography which is based on the

Diffie-Hellman key exchange.

(8)



Elliptical Curve Cryptosystem: — It is a public key cryptography system which is based on discrete logarithms structure of elliptical curves over finite fields.

ECC can be used for encryption, secure key exchange and also for authentication & verification of digital signatures.

A) (2) Chinese Remainder theorem \Rightarrow

It states that if one knows the remainders of the Euclidean division of an integer n by several integers, the one can determine uniquely the remainder of the division of n by the product of these integers, under condition that divisions are pairwise coprime.

$$\begin{aligned}
 x \% \text{num}[0] &= \text{rem}[0]; & \text{mod}(\text{num}[0]) \\
 x \% \text{num}[1] &= \text{rem}[1]; & \text{mod}(\text{num}[k-1]) \\
 \vdots & \vdots & \vdots \\
 x \% \text{num}[k-1] &= \text{rem}[k-1] \quad \leftarrow
 \end{aligned}$$

Eg- I/p $\text{num}[] = \{5, 7\}, \text{Rem}[] = \{1, 3\}$
 $O/p = 31$

Q-(a) Public key Cryptosystem \Rightarrow It is an encryption scheme that uses two mathematically related, but not identical, keys. The public key is used to encrypt.

Application:- (i) Digital signatures:- content is digitally signed with an individual's private key & is verified by the individual's public key.

(ii) Encryption:- content is encrypted using an individual's public key & can only be decrypted with the individual's private key.

(b) CHF:- It is a mathematical algo that maps data of arbitrary size to a bit array of a fixed size.

\rightarrow Cryptographic Hash functions have many information-security applications, notably in digital signatures, message authentication codes (MACs) and other forms of authentication.

\rightarrow They can also be used as ordinary hash functions to index data in hash tables.

(c) Digital Signature \Rightarrow It is a cryptographic value that is calculated from the data & a secret key known only by the signer.

In real world, the receiver of message needs assurance that the message belongs to the sender & he should not be able to repudiate the origination of that message.

(2)

Digital signatures provide us with 3 very important properties. These are

- (i) Authentication
- (ii) Integrity
- (iii) Non-repudiation

(d) Key Management \Rightarrow key management refers to managing cryptographic keys within a cryptosystem.

It deals with generating, storing, using & replacing keys as needed at the user level. It will also include key servers, user procedures & protocols, including cryptographic protocol design.

key distribution :- It is done through public key servers. When a person creates a key-pair, they keep one key private & the other known as the public-key.

1e) Public key Infrastructure :- PKI provides assurance of public key. It provides the identification of public keys & (3) their distribution. An anatomy of PKI comprises of the following components.

- Public key Certificate
- Private key tokens
- Certification Authority
- Registration Authority
- Certification Management

Section - (2)

Q - (9) Secure Hash Algorithm \Rightarrow Also known as SHA, are a family of cryptographic functions designed to keep data secured.

It works by transforming the data using a hash function: an algorithm that consists of bitwise operations, modular additions & compression functions.

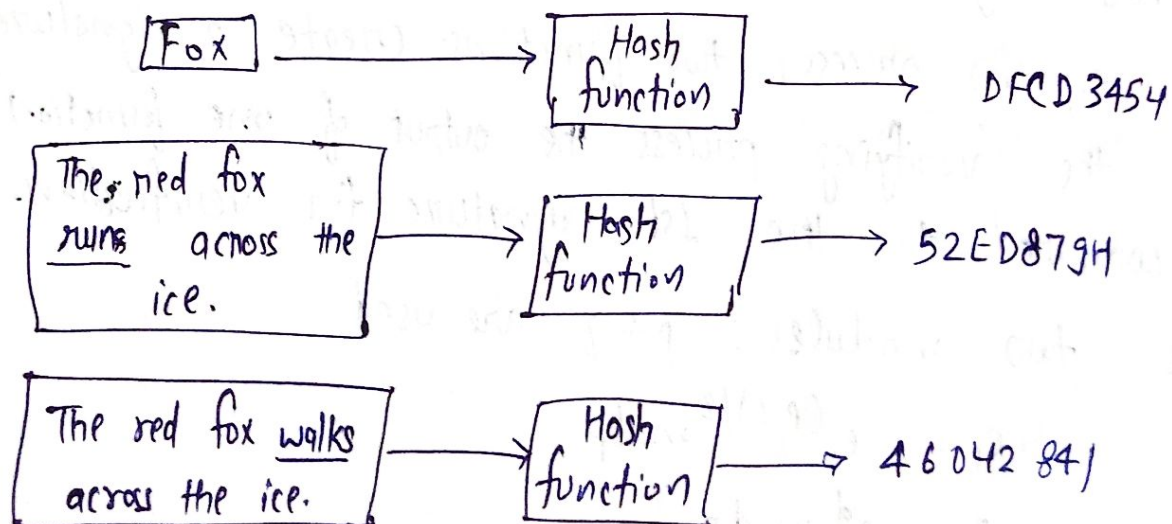


fig:- SHA

Family of SHA comprise of 4 SHA algo:- SHA-0, SHA-1, SHA-2, SHA-3.

(4)

(14) El-Gamal Digital Signature:-

- This scheme used the same keys but a different algo.
- This algo creates two digital signatures, these two signatures, are used in the verification phase.
- The key generation process is the same as that of El-gamal algorithm.
- The public key remains (e_1, e_2, p) & the private key continues to be d .

$$S_1 = e_1^r \text{ mod } p$$

$$S_2 = (M - d \times S_1) \times r^{-1} \text{ mod } (p-1)$$

Schnorr Digital Signature:- It is a digital signature produced by schnorr signature.

- In signing process, two functions create 2 signatures, in the verifying process the output of one function is compared to the 1st signature for verification.

Here two modules: p & q are used

$$e_1 = e_0^{(p-1)/2} \text{ mod } p$$

$$e_2 = e_1^d \text{ mod } p$$

(e) Hash function Based On Cipher Block chaining \Rightarrow

\rightarrow A no. of proposals have been made for hash functions based on using a cipher block chaining technique, but without using secret key. (5)

One of first such proposals was that of Rabin.

Divide a message M into fixed size blocks M_1, M_2, \dots, M_N .

\rightarrow There is no secret key. As with any hash code, this scheme is subject to birthday attack & if the encryption algo is DES & only a 64-bit hash code is produced, then the system is vulnerable.

$$\text{Compute } H_i = E(Q_i, H_{i-1})$$

$$E(X, H_{N-2}) = D(Y, G)$$

$$H_i = E(H_{i-1}, M_i) \oplus M_i$$

(f) MACs based on Hash functions \Rightarrow

for Message Authentication code, the algo. used to generate & verify the MAC is based on the DES.

\rightarrow A keyed Hash MAC is an extension to MAC function to include cryptographic hash function & a secret key is deriving the MAC.

Typically, MD5 & SHA-1 cryptographic hash functions

are used to calculate HMAC value.

→ The type of cryptographic hash used in creating the HMAC is appended to included algo (eg - HMAC-MD5 & HMAC-SHA1)

→ It combines a shared secret key. (6)

→ IPsec uses HMACs. Two parties must pre-share a secret key.

Section (3)

(a) RSA Cryptography :-

RSA algorithm is asymmetric cryptography algorithm.

Asymmetric actually means that it works on 2 different keys public & private.

→ The idea of RSA is based on the fact that it is difficult to factorize a large integer. The public key consists of 2 no where one no. is multiplication of 2 large prime no.

And private key is also derived from the same 2 prime numbers.

→ RSA keys can be typically 1024 & 2048 bits long, but experts believe that 1024 bit keys could be broken in the near future.

$$P=53, Q=59, n=P*Q=3127$$

$$1 < e < \phi(n)$$

$$\phi(n) = (P-1)(Q-1) = 3016$$

$$d = (k * \phi(n) + 1) / e = 2011, k=2$$



Rabin Cryptosystem :- It is an public key cryptosystem.

It uses asymmetric key encryption for commⁿ b/w two parties & encrypting the message.

The security of Rabin - Cny. is related to difficulty of factorization. It has adv. over the others that the problem on which it banks has proved to be hard as integer factorization.

1. $P \neq 2 \rightarrow P \equiv Q \equiv 3 \pmod{4}$

2. for ex:- $P=139, Q=191$
 $n = P * Q$

3. Publish n as public key & save P & Q as private key

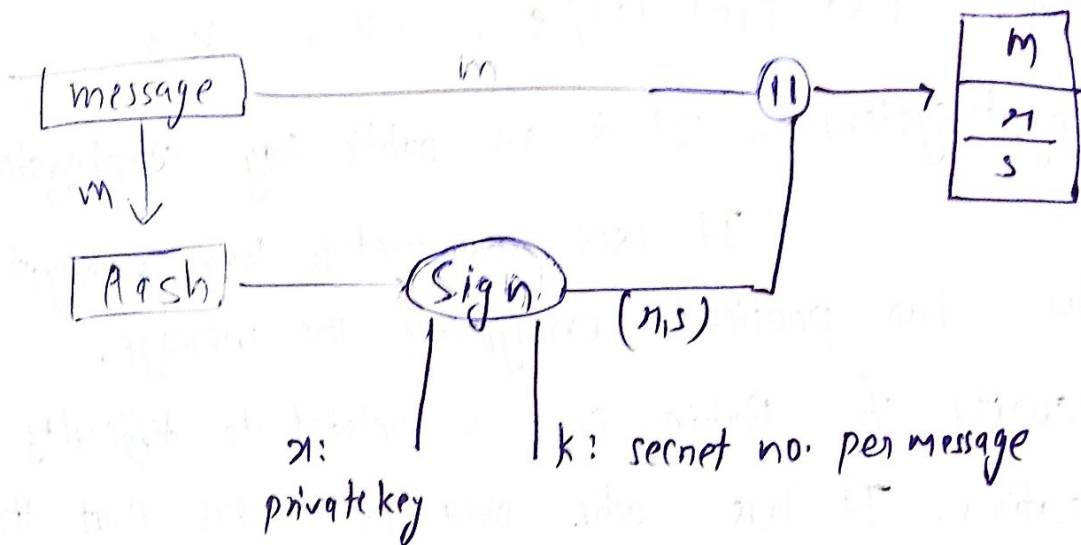
(B) Elgamal Cryptosystem :-

- This scheme used the same keys but a different algo.
- This algorithm creates two digital signatures, these 2 signatures, are used in the verification phase.
- The key generation process is the same as that of el-gamal algorithms
- The public key remains (e, g, p) & the private key continues to be d .

$$S_1 = e_1 V \bmod p$$

$$S_2 = (M - d \cdot S_1) \cdot V^{-1} \bmod (p-1)$$

8



Elliptical Curve Cryptosystem \Rightarrow

It is an approach to public key cryptography based on algebraic structure of elliptic curves over finite fields.

\rightarrow ECC allows smaller keys compared to non-E-C cryptography to provide equivalent security.

