Cyber Security – It is protection of computer systems & networks from attack by malicious actors that may result in unauthorized info disclosure

M T W T F S S YOUVA

Section - I

Introduction to Security :

*key Security Properties / principles of Security

1. Confidentiality :- Unauthorized party cannot gain access
   - Confidentiality means that only authorized individuals / systems can view sensitive or classified information.
   - The data being sent over the network should not be accessed by unauthorized individuals

2. Integrity :— To ensure that info in not altered.
   - Integrity make sure that data has not been modified.
   - corruption of data is failure to maintain data integrity.
   - To check if our data has been modified or not we make use of hash function.
   - ex. of Integrity – When content of msg change after sender sends it before it reaches to receiver we say that integrity of msg is lost.

3. Availability :— Info is accessed by authorized user whenever needed
   - It means that the network should be readily available to its users.
   - This applies to systems and data.
   - To ensure availability, network administrators should maintain hardware, make regular upgrades, have a plan for fail-overs, and bottlenecks in network.

Risk Management :—

Cyber Security risk management is an ongoing process of identifying, analyzing, evaluating and addressing organization's cyber-security threats.

- Understanding Governance

① Policies —

Policies are formal set of rules which is issued by an organization to ensure that the user who are authorized to access company technology and information assets comply with rules and guidlines related to security of information.

② Framework —

CS Frameworks are set of documents describing guidlines, standards, & best practice designed for CS Risk management.

Frame work exist to reduce an organization exposure to weakness and vulnerabilities that hackers and other cyber criminals may exploit.

③ Laws :—

Cyber laws yields legal recognition to electronic documents and structure to support e-filling & e-commerce transactions & also provides a legal structure to reduce, check cyber crimes.

(4) Regulation :-

CS Regulation are laws that govern the types of digital measures an organization must take to protect itself, it's data, and its customers.

(5) ~~Gui~~ Guidlines and Compliance of Cyber Security.

Cyber Security Compliance involves meeting various controls (usually enacted by a regulatory authority, law or industry group) to protect the Confidentiality, integrity, and availability of data.

Risk Based Management :-
(Risk Based Approach)

Risk Based approach is a systematic method that identifies, evaluates, and prioritizes threats facing the organization.

It is customizable method that enables the business to tailor their cybersecurity program to specific organizational needs and operational vulnerabilities.

Cryptography :—

Cryptography is technique of securing information through use of codes so that only those person for whom the information is intended can understand it and process it. Thus preventing unauthorized access to information. The prefix "Crypt" means "hidden" & suffix "graphy" means "writing".

- features of Cryptography :—

1) Confidentiality :-
info can only be accessed by the person for whom it is intended.

2) Integrity : info cannot be modified in storage or transition betn sender & intended receiver without any addition to information being detected

3) Non-repudiation

4) Authentication

- Types of Cryptography

(1) Symmetric key cryptography

(2) Hash Funn

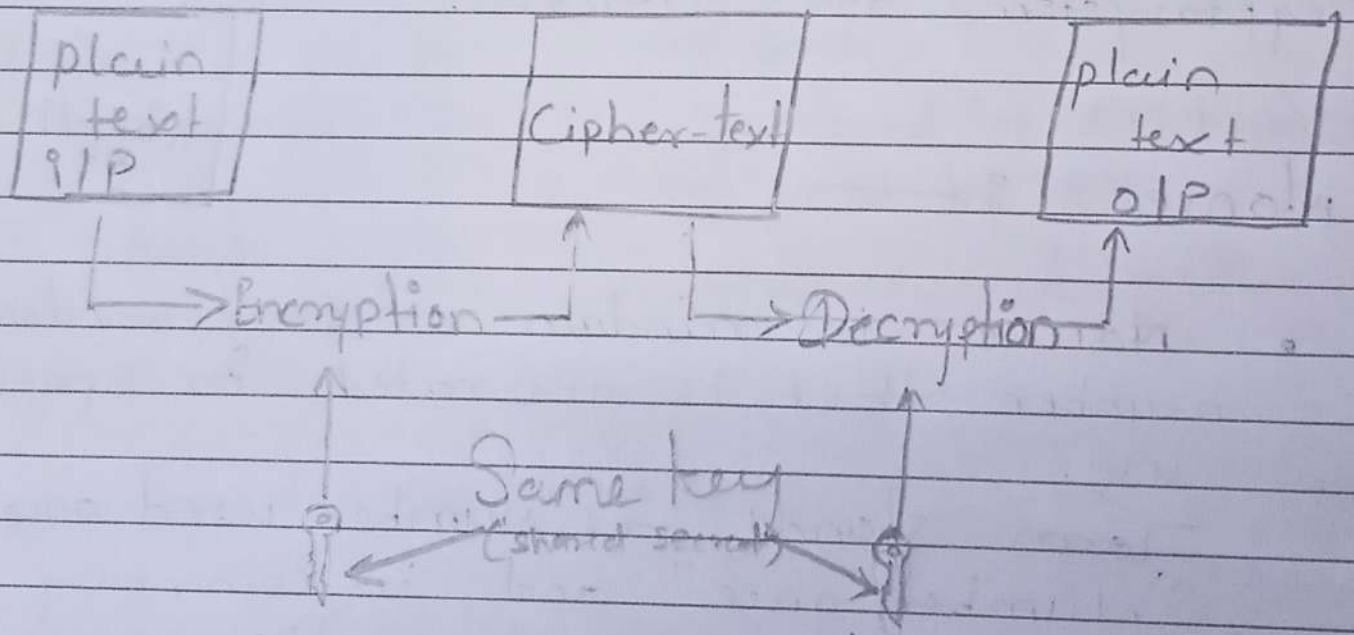
(3) Asymmetric key Cryptography

① Symmetric — / Private key Cryptography

It is best suited for bulk encryption because it is much faster than asymmetric cryptography.

Wit symmetric or private key cryptography

- Both parties share the same key (which is kept secret). Before comm^n begin, both parties must exchange the shared secret key.
- Each pair of comm^n entities requires a unique shared key. The key is not shared with othe comm^n partners.



Symmetric key encryption

* Role of random numbers :—

- Random number is choosen by chance i.e randomly from set of numbers.

Random numbers are imp in digital cryptography & cryptocurrency wallets.

Random numbers are produced with Random number generator. There are two types of RNG.

(1) pseudrandom num generator.
(2) true random num generator.

- In cryptography randomness is found everywhere, from generating key to encryption systems, even the way in which cryptosystems are attacked.

* Nonce :—

- Nonce is random or semi-random number that is generated for specific use.
Term stands as "Number used once" "Number once" and is commonly referred to as cryptographic nounce

- A nonce in cryptography is number to protect private comm" by prev replay attacks

Prime numbers used in Cryptography

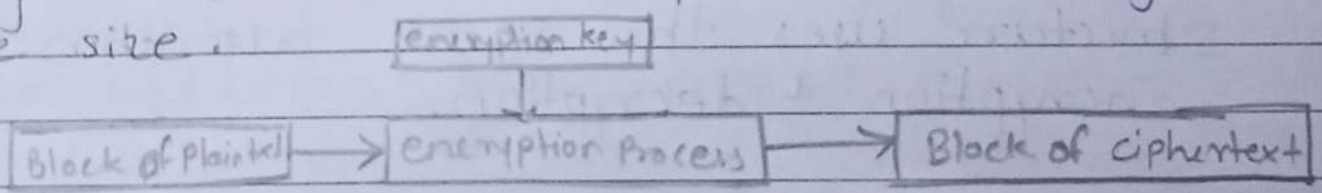
- prime nums are used in cryptography because they are difficult to factorize.
- This means that it is difficult to find the prime factors of composite number without knowing the factors to begin with.
- This makes it difficult for someone to intercept msg & read it without the proper key.

Data Encryption Standard :—

- **Block Cipher**

Block cipher is a method of encrypting data in blocks to produce ciphertext using cryptographic key and algorithm.

Block cipher takes a block of plaintext bits and generates a block of ciphertext bits, generally of same size.



- **Stream Cipher :—**

In stream cipher one byte is encrypted at a time while in block cipher 128 bits are encrypted at a time

DES

- Symmetric block cipher
- 56-bit, 64-bit i/p block, 64-bit o/p block
- Developed in 1977 by NIST, designed by IBM
- Principles used in other cipher-s

1. Stream cipher follows the sequence of pseudorandom num stream.

2. One of the benefits of following stream ciphe is to make cryptanalysis more difficult, so the number of bits chosen in the keystream must be long in order to make cryptanalysis more difficult.

3 By making key more longer it is also safe against brute force attacks.

- Feistel structure :—

Feistel structure is a design [redacted] to develop many block ciphers such as DES. A cryptographic system based on Feistel cipher structure uses the same algorithm for both encryption & decryption.

★ Block Cipher modes of Operation :—

Encryption algorithms are divided into two categories based on the input type, as a block cipher and stream cipher

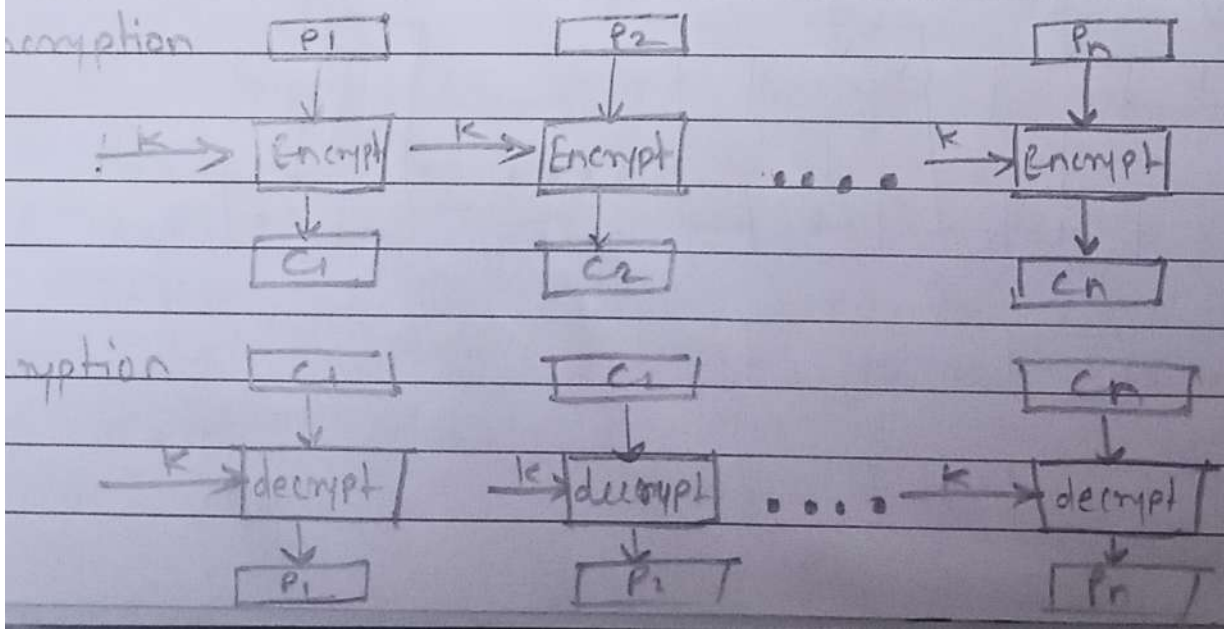
Block cipher is an encryption algorithm that takes a fixed size of input say b bits and produces ciphertext of b bits again.
If the input is larger than b bits it can be divided further.

For different appl^n & uses, there are several modes of operations for a block cipher.

① Electronic Code Book (ECB)

ECB is the easiest block cipher mode of functioning. It is easier because of direct encryption of each block of i/p plaintext & o/p is in form of blocks of encrypted ciphertext.
Generally, if a msg is larger than b bits in size, it can be broken down into a bunch of blocks and the procedure is repeated.

cedure of ECB is as follows :—



Advantages of ECB :—

- Parallel encryption of blocks of bits is possible, thus it is faster way of encryption
- Simple way of block cipher.

disadvantage of ECB :—

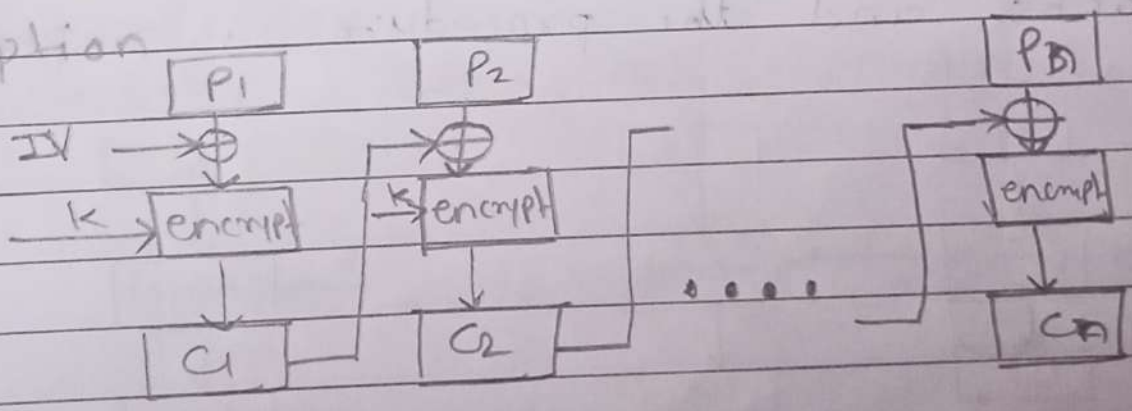
- prone to cryptanalysis since there is a direct relationship betⁿ plaintext and ciphertext

(2) Cipher Block Chaining (CBC)

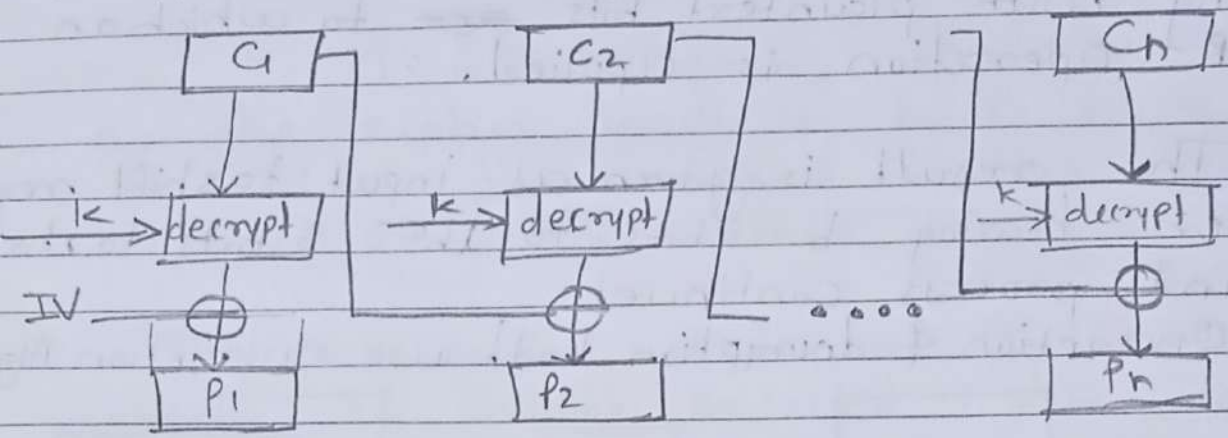
CBC is an advancement on ECB since ECB compromises some security requirements.

In CBC, the previous cipher block is given as input to the next encryption algorith after XOR with the the original plaintext block.

In a nutshell here, cipher block is pro-ced by encrypting an XOR output of the previous cipher block and present pla-t block. Process :—



decryption :-



Advantages of CBC

- CBC works well for i/p greater than b bits.
- CBC is good authentication mechanism.
- Better resistive nature towards cryptanalysis than ECB.

Disadvanteges of CBC -

- Parallel encryption is not possible since every encryption requires a previous cipher.

Cipher Feedback Mode (CFB)

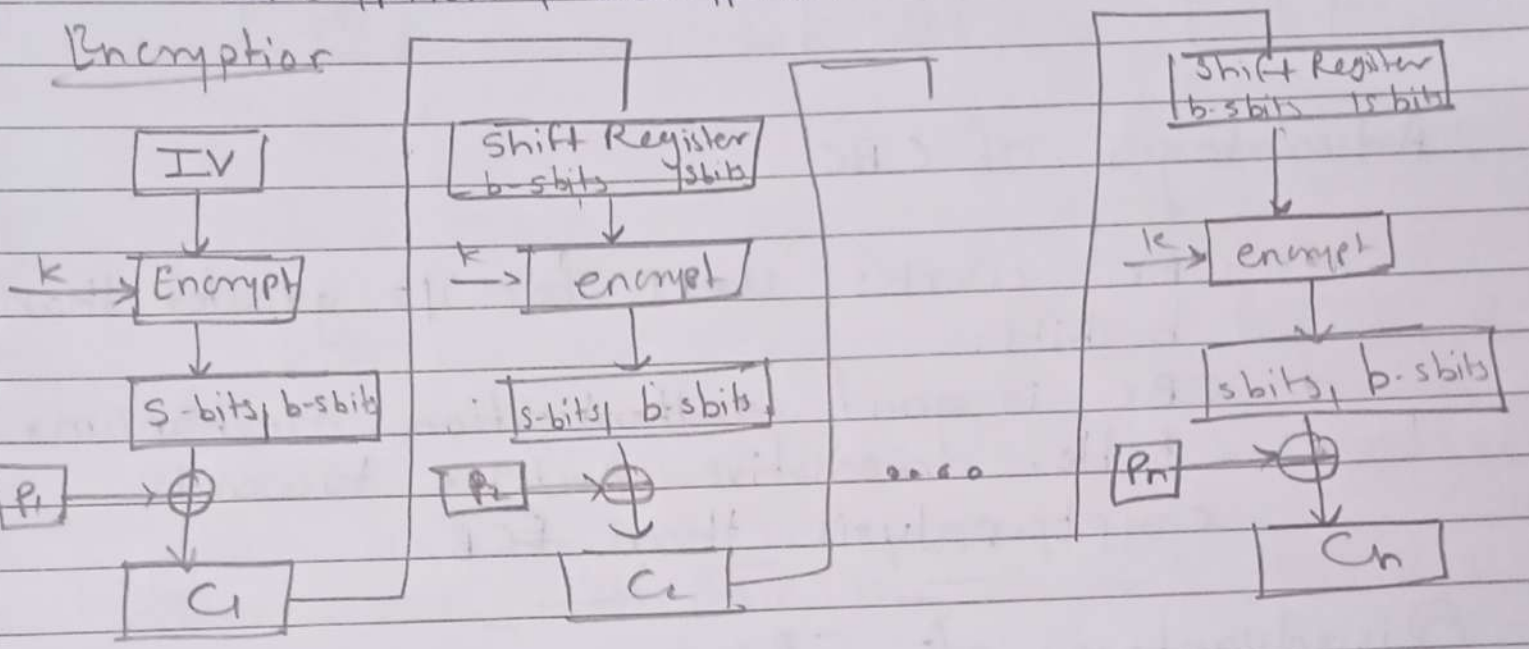
In this mode cipher is given as feedback to the next block of encryption with some new specifications : first, intial vector IV is used for first encryption and o/p bits are divided as set of s & b-s bits.

The left hand side S bits are selected along with plaintext bits ~~are~~ to which an XOR operation is applied.

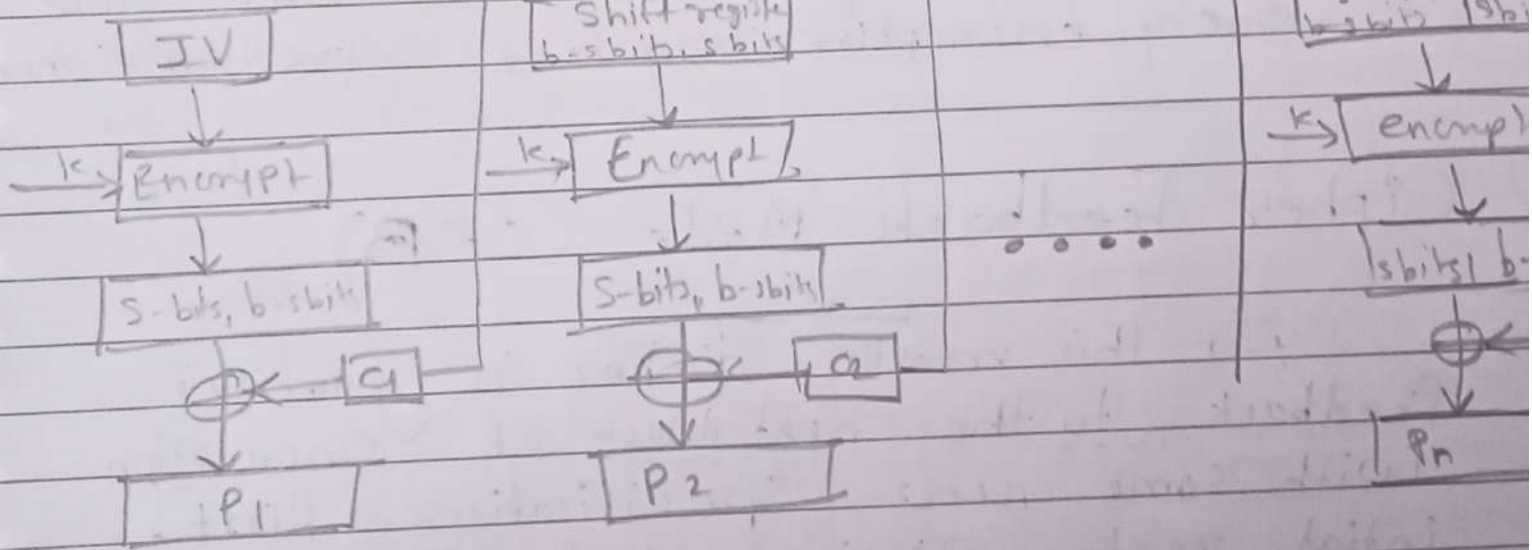
The result is given as input to shift register having b-s bits to lhs, s bits to rhs and process continues.

Encryption & decryption both use encryption Algo

Encryption



decryption



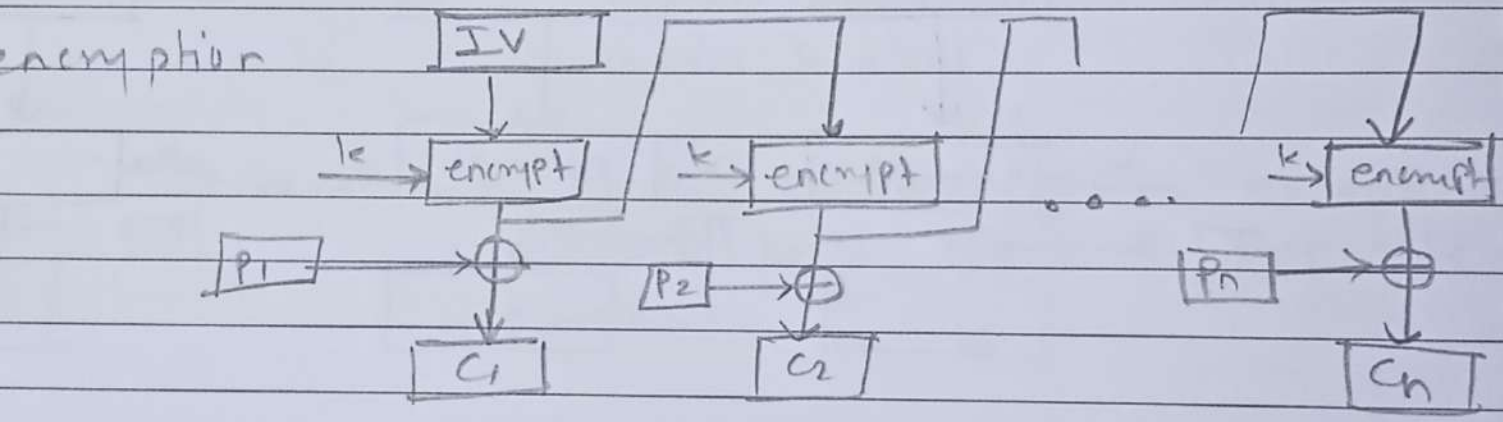
Date

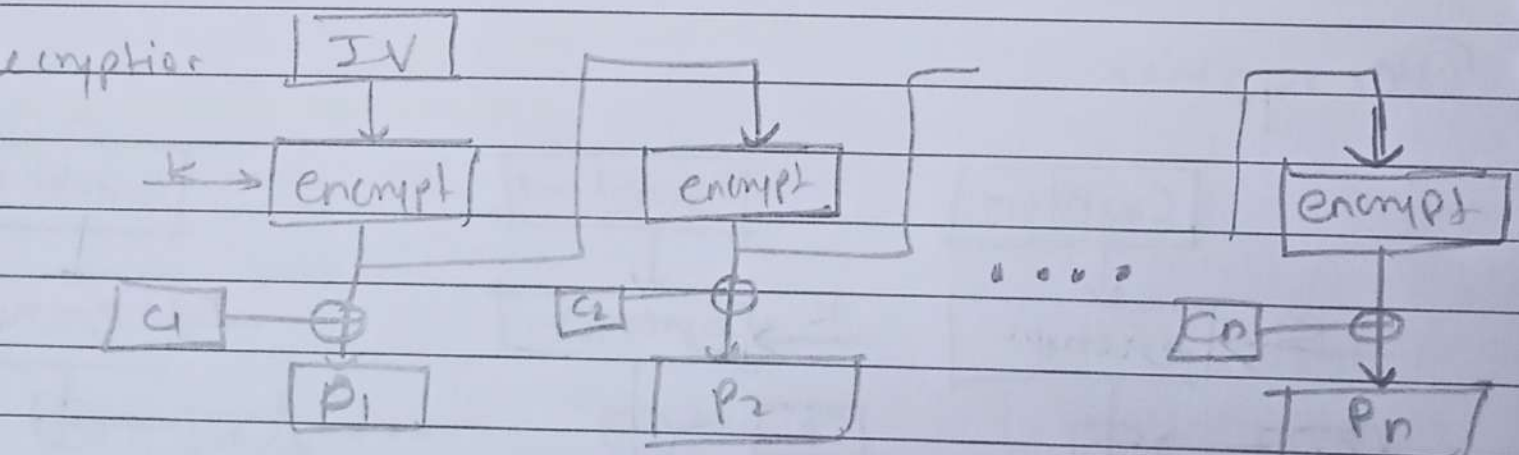
(4) Output Feedback Mode

It follows nearly the same process as the cipher Feedback mode except that it sends the encrypted o/p as feedback instead of actual cipher which is XOR o/p.

In this mode all bits of the block are sent instead of sending selected s bits.

OFM of block cipher holds great resistance towards bit transmission errors. It also decreases the dependency or relationship of the cipher on the plaintext.

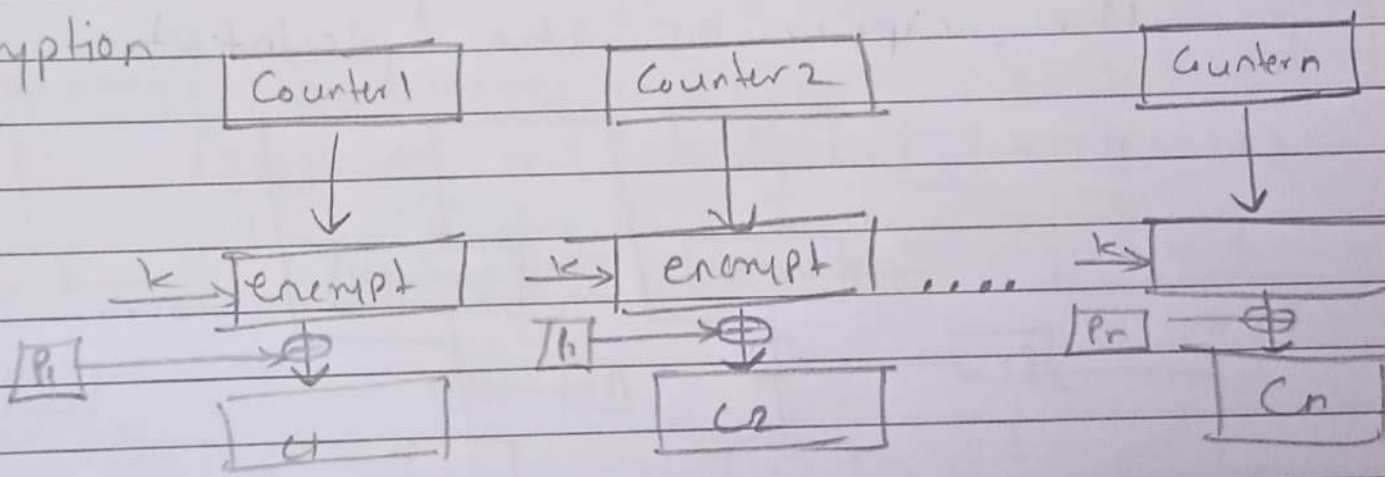




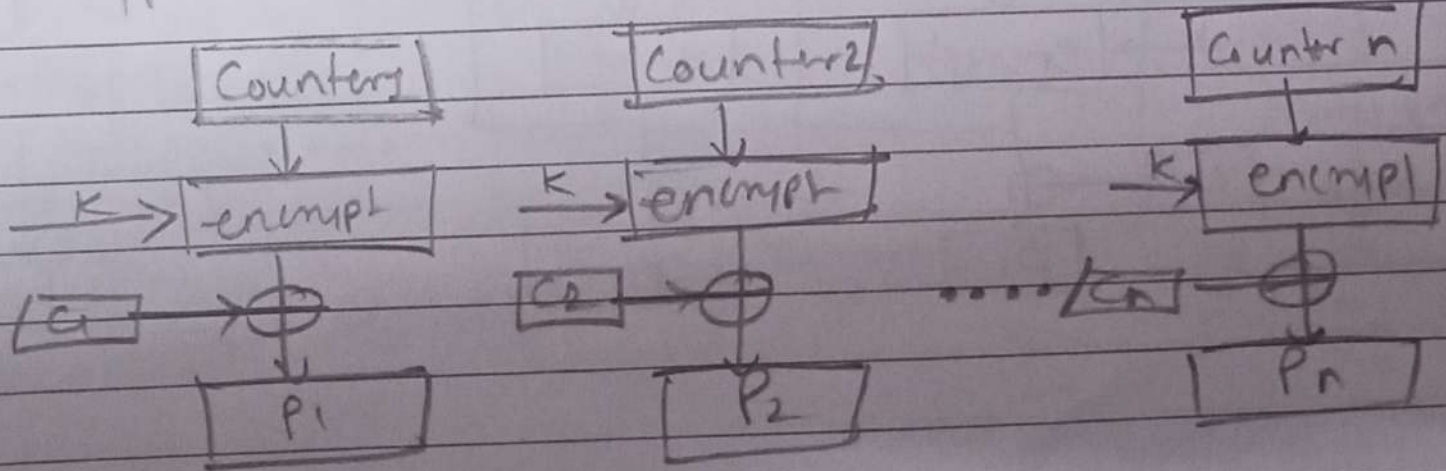
Counter mode :- (CTR)

- It is counter based block cipher implementation.
- Every time a counter-initiated value is encrypted & given as input to XOR with plaintext which results in cipher-text block.
- It is independent of feedback use and thus can be implemented in parallel.

encryption



Decryption



* S-DES (Simplified Data Encryption Standard)

S-DES is a simple version of DES Algo. It is similar to DES algorithm but it is smaller algo and has few parameters than DES

It is a symmetric key cipher i.e they use same key for both encryption & decryption

- Input block:- 8 bits
- Output block (i.e Cipher text):- 8 bit
- key :- 10 bits
- Rounds 2
- Round keys generated using permutation & left shift
- Encryption: Initial permutation, round fun^n Switch halves
- Decryption: Same as encryption except round keys used in opposite order.

✱ Attacks on DES.

1. Differential Cryptanalysis -
2. Related-key Cryptanalysis
3. Linear Cryptanalysis
4. Brute Force Attack

✱ S AES (Simplified Advanced Encryption standard)

AES (Advanced Encryption Standard)

AES is specification for the encryption of electronic data established by US National institute of standard & technology in 2001.

AES is widely used today as it is much ~~Stronger~~ stronger than DES.

- AES is block cipher
- key size can be 128 / 192 / 256 bits
- Encrypted data in blocks of 128 bits each.
  i.e it takes 128 bits as i/p & o/p 128 bits of encrypted ciphertext as o/p.

Public key Cryptography

public key cryptography or asymetric cryptography is an encryption scheme that uses two mathematically related, but non identical key, keys - public key & private key

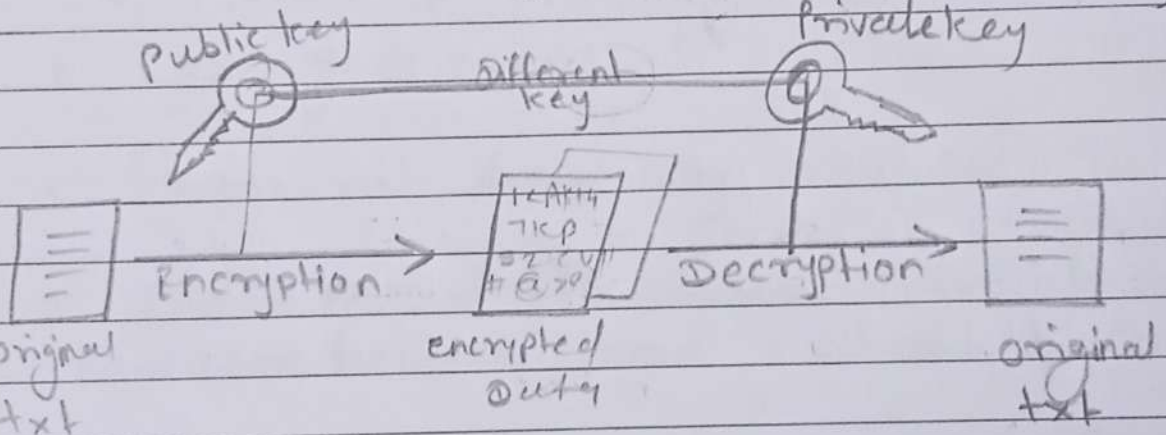
Each key performs a unique fun?. Public key is used to encrypt & private key is used to decrypt.

RSA Algorithm

RSA algorithm can be used for general data encryption & decryption.

(1) Asymmetric Encryption?

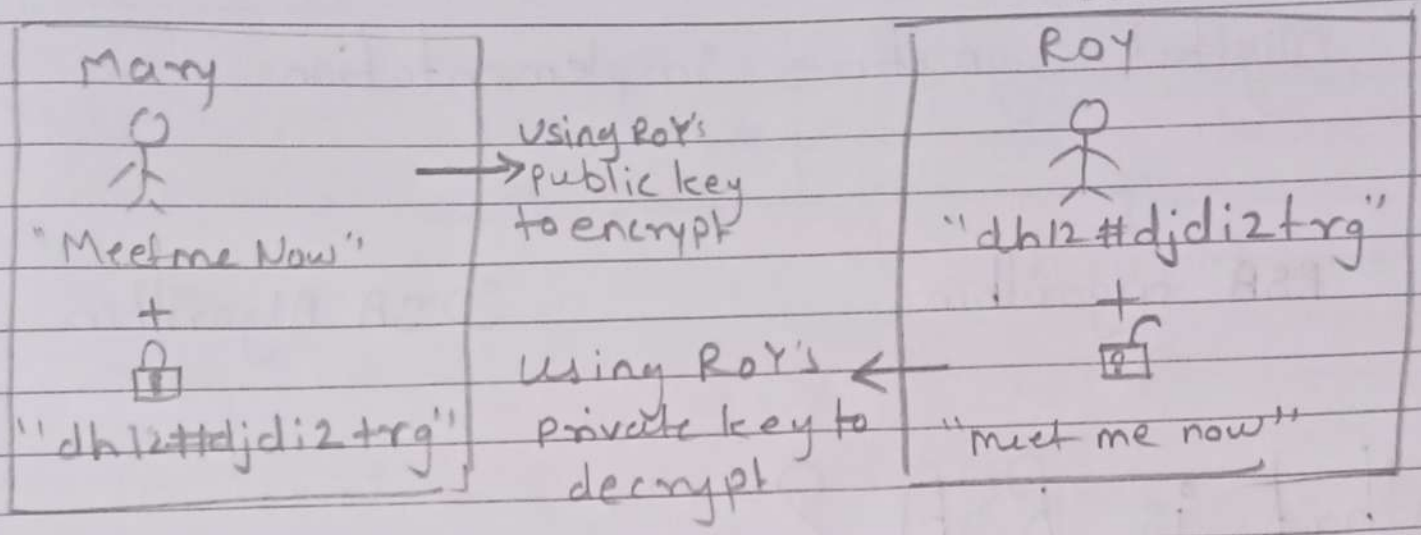
- Asymmetric Encryption uses double layer of protection.
- Two different keys are used in Asymmetric Encryption.
- Private key is used for encrypting data and public key is used for decrypting data.



here sender first encrypt the msg using receiver's private key. After which we receive cipher txt. cipher txt is then transmitted to receiver without any other key. On getting Cipher txt receiver uses his private key to decrypt the cipher text & get plain txt back.

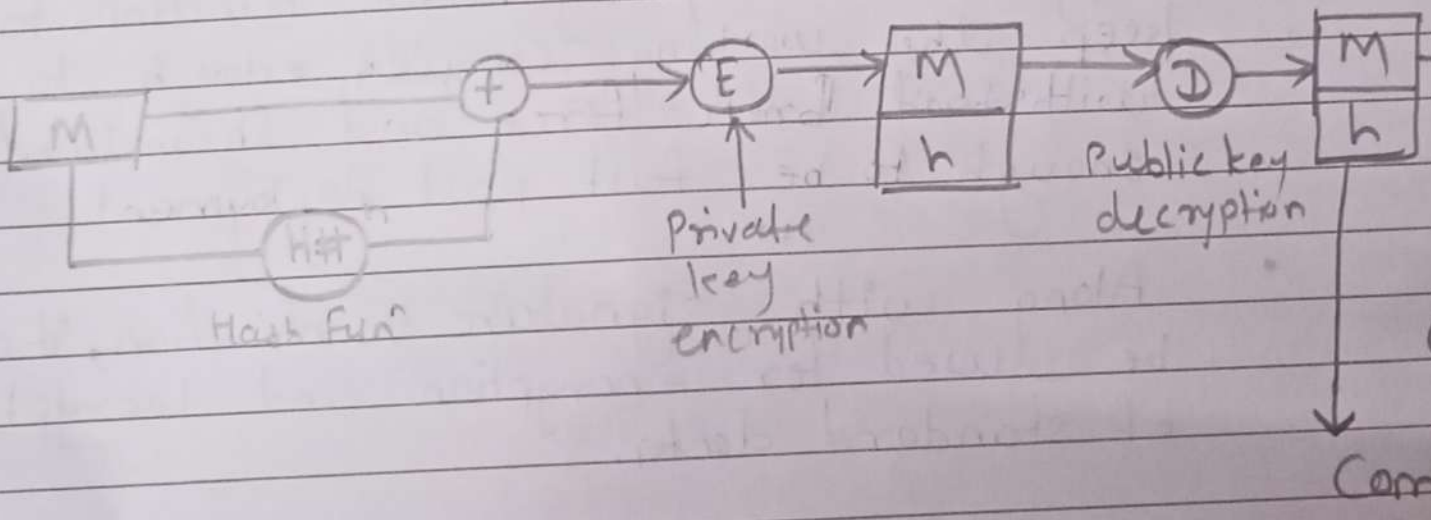
- There is no need of any key exchange throughout this process.

ex. —



What are Digital Signature?

- Mechanism to determine authenticity of a document file.
- Uses public key cryptography mechanism (encrypt using public key & decrypts with private)
- Helpful to authenticate long distance official comm^n channels.



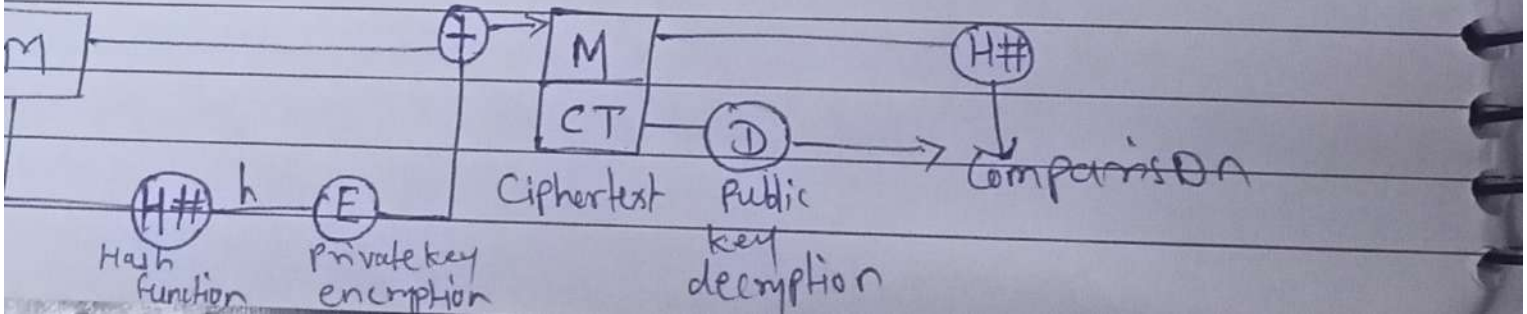
Digital Signature implementation

- RSA algorithm
- DSA Algorithm

What is RSA ?

RSA algorithm is public key signature algorithm, developed by Ron rivest, adi shamir and leonard edelman.

- Rivest - Shamir - Adleman algorithm, named after its 3 founders
- First published in 1997
- Algorithm uses logarithmic functions to keep the working complex enough to withstand brute force and streamlined enough to be fast past deployment
- Along with signature verification, it can be used for encryption and decryption of standard data.
- Below fig is the process of verifying signatures using RSA.



main case of RSA is encryption and decryption of private information before being transmitted accross comm^n channel.

RSA In Data Encryption :—

- Using RSA for encryption and decryption of general data it reverses the key set ussage.
  (key scope is reversed)
- public key of receiver is used to encr data.
- private key of receiver is used to dec the data.
- key exchange not necessary

Two main components :

> key Generation
> Encryption / Decryption Functions

(These steps 4 ciphers need to be run when scrambling data or recovering data f the ciphertxt)

Steps in RSA :-

Key Generation :-

1. Two large prime num are chosen(P & q)
2. Compute $n = p * q$ & $z = (p-1)(q-1)$
3. Choose a number e where $1 < e < (p-q)(q-1)$
4. A number D is selected so that $ed \bmod z = 1$ and calculated as $d = e^{-1} \bmod (p-q)(q-1)$
5. Public key is (n, e) and private key is (n, d)

If the plaintext is m, encrypted ciphertext C is calculated as :

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

Under Similar assumptions, the plaintext can be calculated as :

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

ex. $p = 7$

$q = 13$

① So, that $n = p * q = 91$

② We can select value of e to be 5 since 91- satisfies $1 < e < (p-1)(q-1)$

③ value of $d = e^{-1} \bmod (p-1)(q-1) = 29$

④ Public key $= (91, 5)$, Private key $= (91, 29)$

⑤ Let plaintext m be 10.

Cipher text $(c) = m^e \bmod n = 82$

plain text $= c^d \bmod n = 10$

Advantages of RSA :—

① No need of sharing secret keys.

② proof of owner's authenticity.

③ Faster Encryption than DSA.

④ Data can't be modified in transit.

* Attacks on RSA.

① Plain text Attack :—
classified in three categories

i) Short msg Attack -
Here assumption is that the attacker knows some blocks of the plain text msg. If an attacker knows some block of plain text then he could try to encrypt the blocks of plain text using the into & try to convert it into cipher text.

For prevention from SMA we can use padding bits for encryption

ii) Cycling attack -

iii) Unconcealed msg attack

② Chosen cipher Attack :—

In this type of attack, attacker can find out the plain text from cipher text using extended euclidean algo.

③ Factorization Attack :—
Here, Attacker impersonates the key owners & with the help of stolen cryptographic data, they decrypt sensitive data, bypass the security of the system.

* Elliptic Curve Cryptography (ECC)

ECC is public key encryption technique based on ~~eclip~~ elliptic curve theory that can be used to create faster, smaller & more efficient cryptographic keys.

- ECC is an Alternative to RSA
- It is asymmetric / public key cryptography
- Provides equal security with smaller key size (as compared to RSA) as compared to NonECC algos. i.e Small key size & high security
- It makes use of elliptic curves

elliptic curves are defined by some mathematical fun^n - cubic fun^n/

e.g $y^2 = x^3 + ax + b$

* Elliptic curve over real num.
* Elliptic curve over Zp
* Eliptic curve arithmetic

* Data Integrity :—

- Data Integrity is the assurance that digital information is uncorrupted & can only be accessed or modified by those authorized to do so.

- Ensures that information is not altered or changed.

* Introduction to Hashing :—

Hashing is the process of transforming any given key or string of characters into another value.

This is usually represented by a shorter fixed-length value or key that represents & makes it easier to find or employ the original string

Hash Functions :—

It is a mathematical fun^n that converts a numerical i/p value into another compressed numerical value.

Values returned by hash fun^n are called as hash values.

Page No.
Date:
YOUVA

* Properties of Hash Functions :—

① Pre-Image Resistance :
- means it should be computationally hard to reverse a hash fun^n.

② Second Pre-Image Resistance :
- means given i/p & its hash, should be hard to find a different i/p with same hash.

③ Collision Resistance
- means it should be hard to find two different i/p of any length that result in same hash.
- This property of collision also refferred as collision free hash fun^n.

What is Salt ?

Salting hashes sounds like something that

* What is Salt?

- Salting refers to adding random data to hash func to be obtain a unique o/p which refers to the Hash.

- Salting is used in common passwords to strengthen them.

* HASH + SALT :—

Salted password that are also hashed make it harder for bad ~~attacks~~ actors to crack passwords at scale. Because random characters are added to passwords prior to hashing, the hacker loses the ability to quickly figure out the plaintext password.

M T W T F S S

Page No.: YOUVA

Date:

Hashing Algorithms.

(1) SHA1 (Secure hash algo 1):—

- It is a cryptographic hash fun^n which is designed by United States National Security Agency
- Takes an i/p & produces 160 bits hash value
- Further o/p produced by this fun^n is converted into 40 digits long hexadecimal number.

(2) SHA2 (Secure hash Algo 2):—

- Constructed using the merkle-Damgard structure from a one-way compression fun^n.

SHA1	SHA2
① Published in 1995	① Published in 2001
② produces 160 bits hash value	② produces 224, 256, 384 or 512 bits hash value
③ It is successor to SH0 & predecessor to SH2	③ It is successor to SH1 & Predecessor to SH3
④ less secure	④ More secure
⑤ generate smaller hash	⑤ generates larger hash
⑥ generated hash is weak	⑥ generated hash is strong
⑦ Not widely used nowdays	⑦ widely used.