# CNS..

## Important Questions.

UNIT-1 :-

1) Types of security Attacks.
2) Security Mechanisms
3) caesar cipher, Monoalphabetic cipher, Playfair cipher, hill cipher, polyalphabetic Substitution.
4) Steganography.

UNIT-II :-

1) DES (Data Encryption Standard) ⊗
2) AES ( Advanced Encryption standard) ⊗
3) Block cipher role of operation.

UNIT-III :-

1) Fermat & Euler's theorem
2) chinese Remainder Theorem ⊗
3) Diffie Hellman key Exchange.
4) RSA algorithm ⊗

## UNIT-IV:-

1) SHA (Secure Hash Algorithm) ⊗

2) Digital Signature Standard.

3) Kerberos.

4) MAC

## UNIT-5:-

1) PGP operations ⊗

2) S/M/ME

3) IP security Architecture ⊗

4) Intrusion Detection techniques.

UNIT-I :-

## Caesar Cipher Problem :-

Def :-

* It is a type of substitution cipher in which each letter in the plain-text is replaced by a letter some fixed number of positions down the alphabets.

Formula,

Encryption → $c = (p + sk) \bmod 26$

Decryption → $p = (c - sk) \bmod 26$.

where,

P → plain text , Sk → Shift key.
C → cipher text

Eg:

P = ATTACK , Sk = 3.

To know,

| A | B | C | D | E | F | G | H |
|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 |

| I | J | K | L | M | N | O | P |
|---|---|---|---|---|---|---|---|
| 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

| Q | R | S | T | U | V | W | X | Y | Z |
|---|---|---|---|---|---|---|---|---|---|
| 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

Encryption, $c = (p + sk) \bmod 26$

| | | | | | | |
|---|---|---|---|---|---|---|
| | A | T | T | A | C | K. |
| p → | 0 | 19 | 19 | 0 | 2 | 10 |
| sk → | 3 | 3 | 3 | 3 | 3 | 3 |
| c → | 3 | 22 | 22 | 3 | 5 | 13 |
| ⇒ | D | W | W | D | F | N |

Decryption, $p = (c - sk) \bmod 26$.

| | | | | | | |
|---|---|---|---|---|---|---|
| | D | W | W | D | F | N |
| c → | 3 | 22 | 22 | 3 | 5 | 13 |
| sk → | 3 | 3 | 3 | 3 | 3 | 3 |
| p → | 0 | 19 | 19 | 0 | 2 | 10 |
| | A | T | T | A | C | K |

Cryptanalysis of caesar cipher :-

* Only have 26 possible ciphers
* A maps to A, B, C, ..., Z
* Brute force Search
* Could simply try each in turn
* given ciphertext, just try all shifts of letters.

# MONOALPHABETIC CIPHER :-

* Monoalphabetic cipher substitutes a letter of the alphabets with another letter of the alphabets. However, rather than substituting according regular pattern, any letter for any other letters, as each letter has a unique substitute left and vice-versa.

To know,

| plaintext → | A | B | C | D | E | F | G | H | I | J | K |
|---|---|---|---|---|---|---|---|---|---|---|---|
| Ciphertext → | t | u | v | w | x | y | z | a | b | c | d |

| | L | M | N | O | P | Q | R | S | T | U | V |
|---|---|---|---|---|---|---|---|---|---|---|---|
| | e | f | g | h | i | j | k | L | m | n | o |

| | W | X | Y | Z |
|---|---|---|---|---|
| | p | q | r | s |

3

Eg:

Encryption,

plaintext message → Hi, I am fine.

ciphertext message → ab, b tf ybgx

Decryption,

Ciphertext → ab, b tf ybgx

Plaintext → Hi, I Am Fine.

Eg 2:

Plaintext → We Bare Bears.

Ciphertext → px utkx Uxtkl

↓

Ciphertext → px utkx Uxtkl

Plaintext → We Bare Bears.

# PLAYFAIR - CIPHER.

Def :-

Playfair cipher is a diagraph substitution cipher. It employs a table where one letter is omitted and the letter are arranged in a 5x5 grid.

5

KEYWORD → Monarchy.

If two letter are in same row, then it moves forward.

| | | | | |
|---|---|---|---|---|
| M | O | N | A | R |
| C | H | Y | B | D |
| E | F | G | I/J | K |
| L | P | Q | S | T |
| U | V | W | X | Z |

If two letter are in same column, then it moves downward.

Balloon → BA LX LO ON

IB SU MP NA

(or)

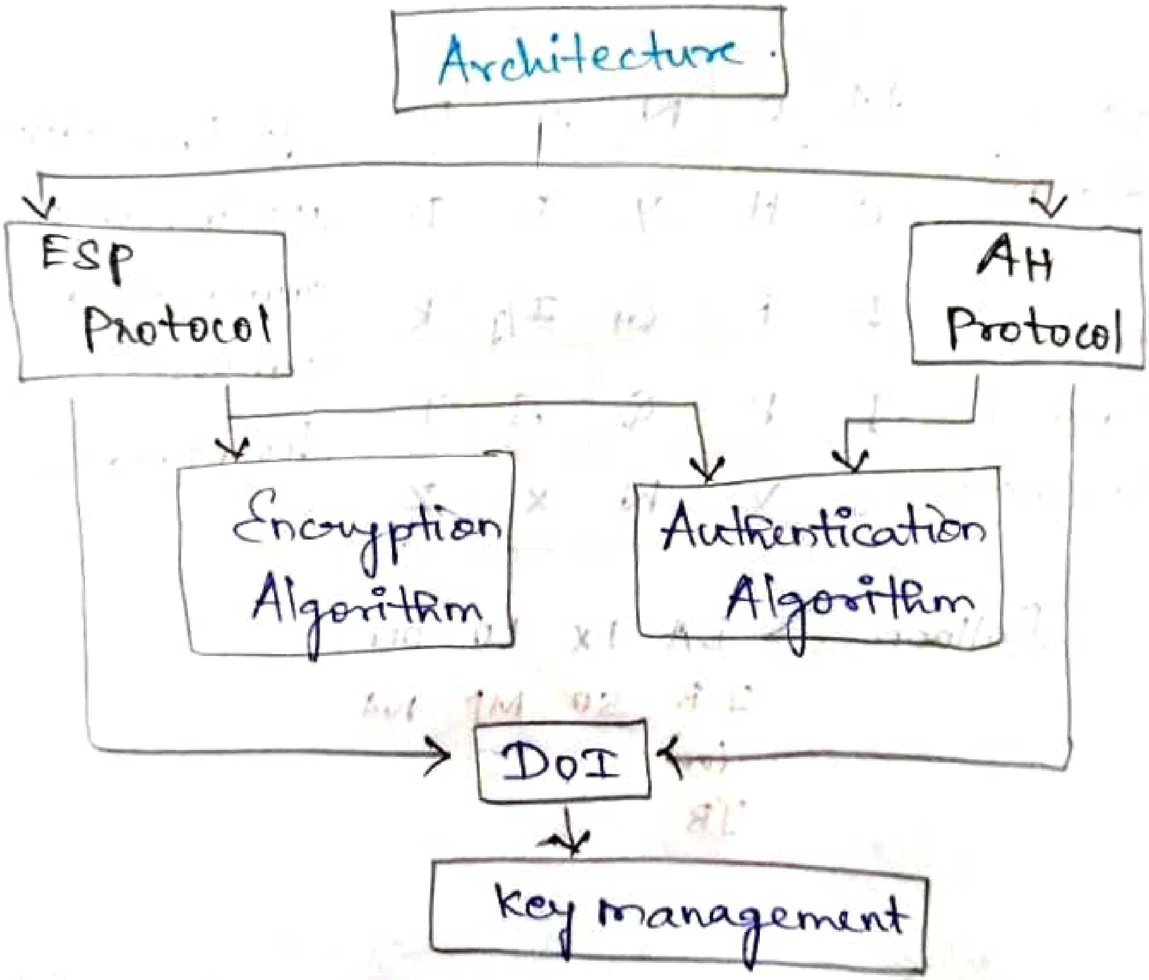
JB

## Unit-V :-

## IP security :-

### Architecture :-

* Covers the general concepts, security requirement, definitions and mechanisms defining IPsec technology.



### Encapsulation Security Payload (ESP) :

* It covers the packet format and general issues related to ESP for packet encryption and Authentication.

Authentication Header (AH) :-

* covers the packet format and general issues related to the use of AH for packet authentication.

Encryption Algorithm :-

* A set of algorithm documents that describe how various encryption algorithms are used to ESP.

Authentication Algorithm :-

* A set of documents that describe how various authentication algorithms are used for AH and for ESP.

Key Managements :-

* Documents that describes key management schemes.

Domain of Interpretations (DOI) :-

* contains values needed for other documents relate to each other, includes identifiers for approved encryption & authentication algorithms, as well as

operational parameters such as key life-time.

Ip-Sec Services :-

* Ipsec provides security services at the Ip layer by enabling a system to select required security protocols, determine the algorithms to use for the services and cryptographic keys required to provide the requested services.

* Two protocols are used to provide security,

⇒ Authentication protocol : Designated by the header of protocol and AH.

⇒ Encryption/Authentication protocol : Designated by the format of packet of protocol, Encapsulating security protocol (ESP).

Services :-

- * Access control
- * Connectionless Integrity.
- * Data Origin Authentications
- * Rejection of replayed packets
- * Confidentiality.
- * Limited traffic flow.

Modes of Transfer :-

* Both AH and ESP support two modes of use,

⇒ Transport Mode [protects upper-layer protocol]

⇒ Tunnel Mode [protects Entire IP].

Authentication Header :-

| | | |
|---|---|---|
| Next header | Payload Length | RESERVED |
| Security Parameter Index (SPI) | | |
| Sequence number | | |
| Authentication data | | |

* Authentication Header provides support for data Integrity & Authentication of IP packets.

Applications :-

* Ipsec provides the capability to Secure communications across a LAN, across private and public WAN and across the Internet.

*Ipsec can play a vital role in routing architecture required for Internet working.

Benefits :-

* It can be transparent to end users.

* There is no need to train users on Security mechanisms..

* Ipsec can provide Security for individual users if needed.

Key Management :-

*Manual

* Automated

* Oakley key Determination protocol

* ISAKMP.

5

UNIT-V :-

## S/MIME :-

S/MIME → Secure/Multipurpose Internet Mail Extension.

* S/MIME is a security enhancement to the MIME internet e-mail format standard, based on RSA Data Security.

## MIME :-

* MIME is an extension to RFC 822-framework that is intended to address some of the problems and limitations of the use of SMTP and some other mail transfer protocol and RFC 822 for electronic mail.

## Limitations of MIME :-

* SMTP can't transmit executable files or other binary objects.

* SMTP can't transmit text data that includes national language characters.

* SMTP Servers may rejects mail message over a certain size.

* SMTP gateway that translate between ASCII and the character code.

* SMTP gateway to X400 electronic mail networks can't handle not textual data included in X400 messages.

* Some SMTP gateway implements do not adhere completely to the SMTP Standard defined in RFC - 821.

## Structure of S/MIME :-

* A MIME email message comprises

  * Text message
  * Specific headers
  * formatted text parts.

* Each segment may includes an ASCII. Encoded portion of data and the techniques for decoding at data at

the receiver's end.

* MIME headers provides the following informations are,

⇒ MIME version

⇒ Content ID

⇒ Content type.

⇒ content transfer encoding.

⇒ content Description.

Functions :-

* Enveloped data

* Signed data

* clear-signed data

* Signed and enveloped data.

Cryptographic Algorithm :-

* MUST

* SHOULD.

Enchanced security services :-

* signed receipts

* Security labels

* Secure mailing list

Advantages :-

* It is available in various modern mail agents like netscape, ms outtook, etc.

* It is utilized to commercial or industrial settings.

* The digital signature protects the email by using email spoofing.

Disadvantages :-

* All users are unable to benefit from S/MIME due to the enforced certificate need because some users simply desire encryption.

All email clients do not support S/MIME signatures.

4

UNIT - III :-

## Chinese Remainder Theorem :-

* the chinese Remainder Theorem (CRT) is used to solve a set of different congruent equations with one variable but different moduli which are relatively prime as shown below,

$$x \equiv a_1 (\mod m_1)$$
$$x \equiv a_2 (\mod m_2)$$
$$x \equiv a_3 (\mod m_3)$$
$$\cdots$$
$$\cdots$$
$$x = a_n (\mod m_n)$$

* CRT states that the above equation have a unique solution of the moduli are relatively prime.

FORMULA :-

$$x = a_1 y_1 m_1 + a_2 y_2 m_2 + a_3 y_3 m_3 (\mod M)$$

Example :-

$x \equiv 1 \pmod 5$

$x \equiv 2 \pmod 7$

$x \equiv 3 \pmod 9$

$x \equiv 4 \pmod{11}$

Soln:

$$x \equiv \overset{\to a}{1} \pmod{\overset{\to m}{5}}$$

$x \equiv 2 \pmod 7$

$x \equiv 3 \pmod 9$

$x \equiv 4 \pmod{11}$

~~$M = m_1 \times m_2 \times m_3 \times m_4$~~

$M = 5 \times 7 \times 9 \times 11$

$\boxed{M = 3465}$

$m_1 = 693 \pmod 5$

$\boxed{y_1 = 3}$

$$\begin{array}{r} 138 \\ 5\overline{)693} \\ \underline{5\phantom{93}} \\ 19\phantom{3} \\ \underline{15\phantom{3}} \\ 43 \\ \underline{40} \\ 3 \end{array}$$

$m_2 = 495 \pmod 7$

$\boxed{y_2 = 5}$

$m_3 = 385 \pmod 9$

$\boxed{y_3 = 7}$

$$\begin{array}{r} 28 \\ 11\overline{)315} \\ \underline{22\phantom{5}} \\ 95 \\ \underline{88} \\ 7 \end{array}$$

$m_4 = 315 \pmod{11}$

$\boxed{y_3 = 7}$

$$X = a_1 m_1 y_1 + a_2 y_2 m_2 + a_3 y_3 m_3 +$$

$$a_4 y_4 m_4 \ (\text{mod } M)$$

$$= 1 \cdot 3 \cdot 693 + 2 \cdot 5 \cdot 495 + 3 \cdot 7 \cdot 385 +$$

$$4 \cdot 7 \cdot 315$$

$$= 2079 + 4950 + 8085 + 8820.$$

$$= 23934 \text{ mod } 3465.$$

$$\boxed{X = 3144}$$

3

## UNIT - III :-

### RSA Algorithm :-

* RSA Algorithm is a public key, encryption technique and is considered as the most secure way of encryption

* RSA Algorithm is an asymmetric cryptography algorithms this means that it uses a public key & a private key.

### Generating the keys :-

1) Select two large prime numbers p and q.

2) Calculate $n = p \times q$

3) Calculate the totient function :

$$\phi(n) = (p-1)(q-1)$$

4) select an integer e,

where e is co-prime to $\phi(n)$ and $1 < e < \phi(n)$.

the pair of numbers $(n, e)$ makes up the public key.

5) Calculate d such that $e.d = 1 \bmod \phi(n)$

d can be Euclican algoritham.

The pair (n, d) makes up the private key.

2) Encryption:-

$$C = M^e \bmod n.$$

3) Decryption:-

$$M = C^d \bmod n.$$

Example :-

$p = 3,\ q = 5$

step 1: $n = p \times q$

$= 3 \times 5$

$= 15$

step 2: $\phi(n) = (p-1)\ (q-1)$

$= 2 \times 4 \Rightarrow 8.$

step 3: $e,$

$\gcd(e, \phi(n)) = 1$

$\therefore e = 3$ [Let us consider)

Step 4:

d,

$d \times e \bmod \phi(n) = 1$

$d \times 3 \bmod 8 = 1$

if, $d = 3$, (considu)

$9 \bmod 8 = 1$

$\therefore d = 3.$

Public key $= \{e, n\} = \{3, 15\}$

Private key $= \{d, n\} = \{3, 15\}.$

Encryption :-

$m = 4 < n$ ($m = 4$ is assumption)

$c = m^e \bmod n$

$c = 4^3 \bmod 15$

$c = 64 \bmod 15 \Rightarrow c = 4.$

Decryption :-

$m = c^d \bmod n$

$= 4^3 \bmod 15$

$= 64 \bmod 15$

$m = 4.$

## Unit-II :-

## Data Encryption Standard :- (DES) :-

* The most widely used encryption Scheme is used based on Data Encryption Standard (DES) adopted in 1977.

Encryption :-

* Takes an 8-bit block of plaintext and a 10-bit key as input and produces an 8-bit of cipher.

Decryption :-

* Takes an 8-bit blocks of cipher and the same 10-bit Key as Input and produces an 8-bit of original plaintext.

⇒ Both subtitution and transposition operations are used.

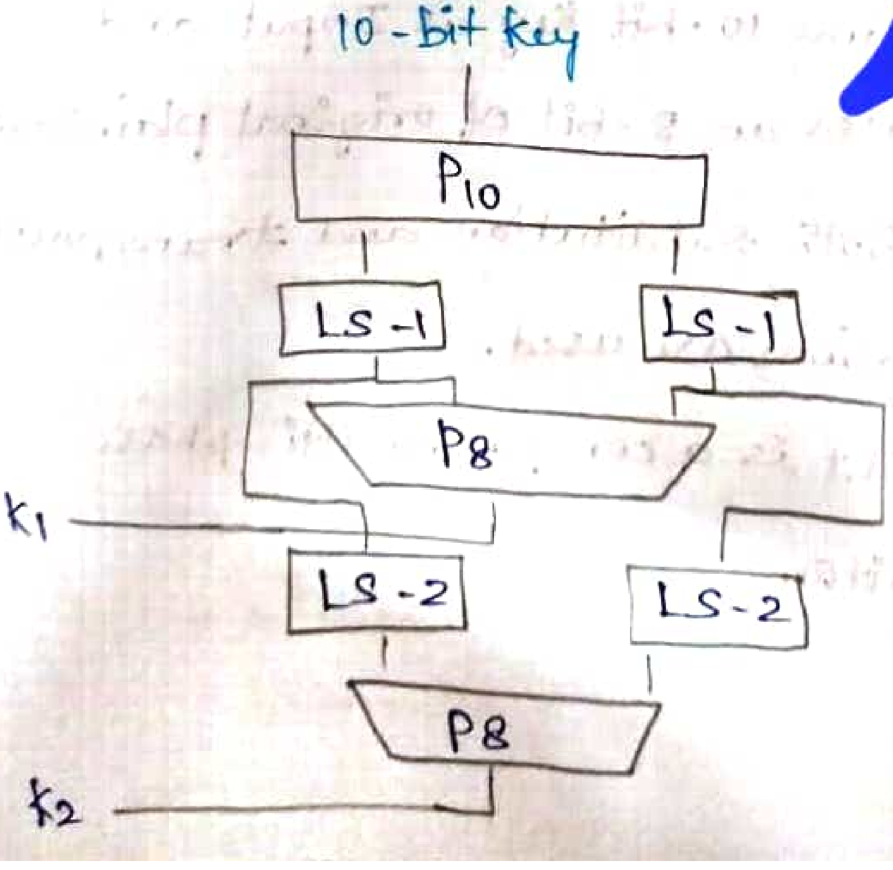
⇒ It is a complex, multi-phase algoritham.

## Five functions to Encrypt :-

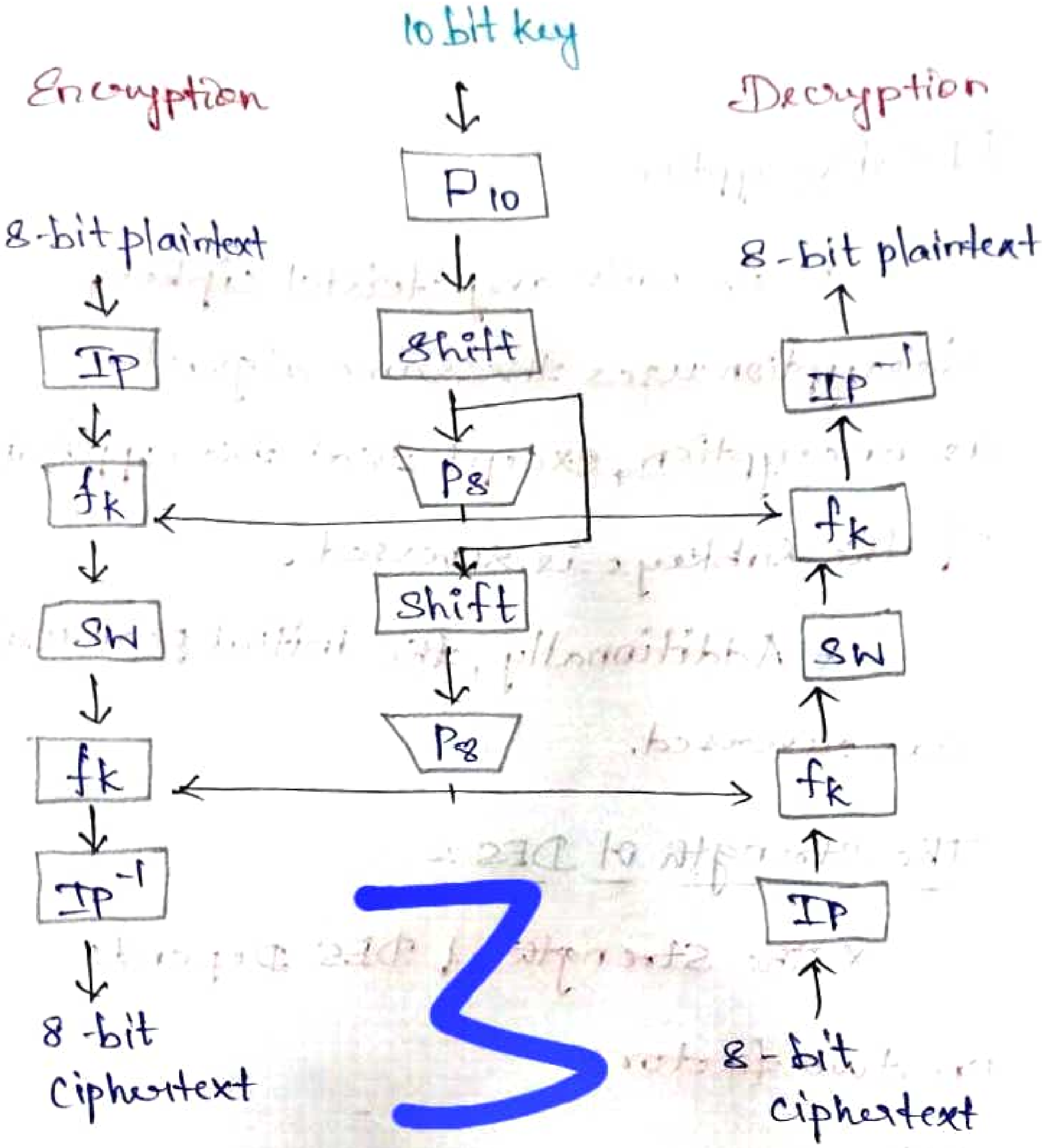
- * Ip → Initial permutation
- * $f_K$ → key dependent scrambler
  - ↳ It is use a 8-bit key
  - ↳ performs both permutation and substitution.
- * SW → Simple permutation functions
  - ↳ Swap the two halves of data.
- * $f_K$ again (different key)
- * $Ip^{-1}$ : Inverse permutation.

## Key functions :-

2



## Architecture :-



## Encryption :-

8-Bit plaintext : Makeup by Sender.

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 1 | 1 | 1 | 1 | 0 | 0 | 1 | 1 |

$P_4$ : permutation 4 (constant)

| | | | |
|---|---|---|---|
| 2 | 4 | 3 | 1 |

## DES Decryption :-

* As with any feistel cipher, decryption uses the same algorithm as encryption, except that the application of the subkeys is reversed.

* Additionally, the initial permutation are reversed.

## The strength of DES :-

* The strength of DES Depends on two factors.

They are,

⇒ Key Size.

⇒ Nature of Algorithm

* The use of possible keys are listed below,

i) The use of 56-Bit keys

ii) Nature of the DES Algorithm

iii) Timing Attacks.

## Attacks On DES :-

* There are two approaches are,

⇒ Differential crypt analysis

⇒ Linear crypt analysis.

5

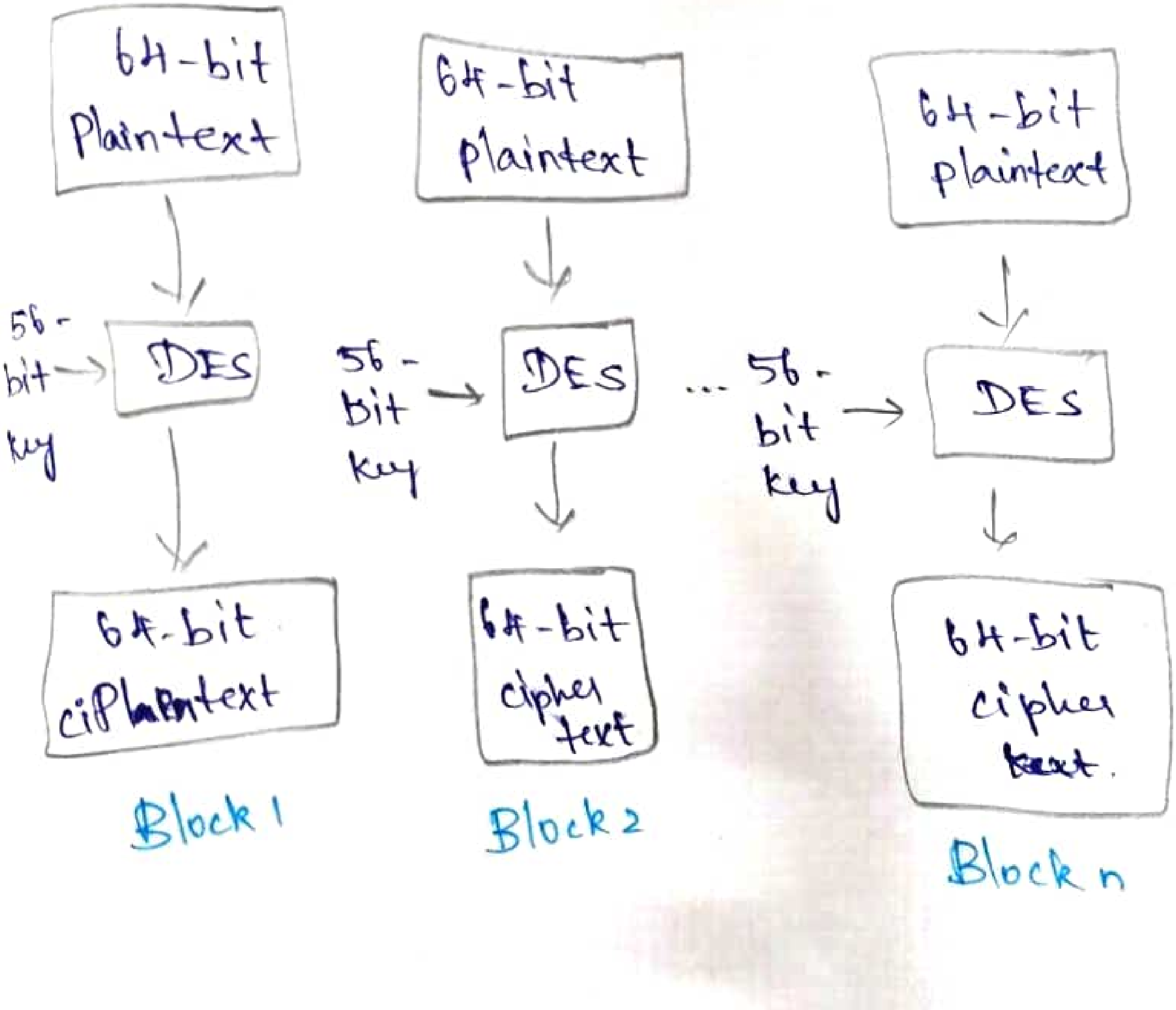
DES :-

* There are two approaches are,

⇒ Differential cypt analysis

⇒ Linear crypt analysis.

Key Length :-



## UNIT-I :-

[redacted]

### OSI Security Architecture :-

* ITU-T Recommendation X-800, Security, Architecture for OSI, defines such a systematic approach.

* The OSI security architecture focuses on security attacks, mechanisms and services.

### Security Attack :-

* Any actions that compromises the security of information owned by an organization.

* It means of classifying security attacks, used both in X.800 and RFC-2828.

* The security attacks are classified into two types. they are,

→ Active Attacks

⇒ Passive Attacks.

* A passive attack attempts to learn or make use of information but does not affect system resources

* An active attack attempts to alter system resources or affect their operations.

Security services :-

* A processing or communication services that enhances the security of the data processing system that the information transfer of an organization.

* The services are intended to counter security attacks and they make use of one or more security mechanisms to provide the services.

Security Mechanisms :-

A process that is designed to detect, prevent or recover from a

Security attacks.

Passive Attacks :-

* It is the nature of eavesdropping on , or monitoring of, transmission.

* The goal is to obtain information that is being transmitted.

* It is very difficult to detect, because they do not involve any alteration of the data.

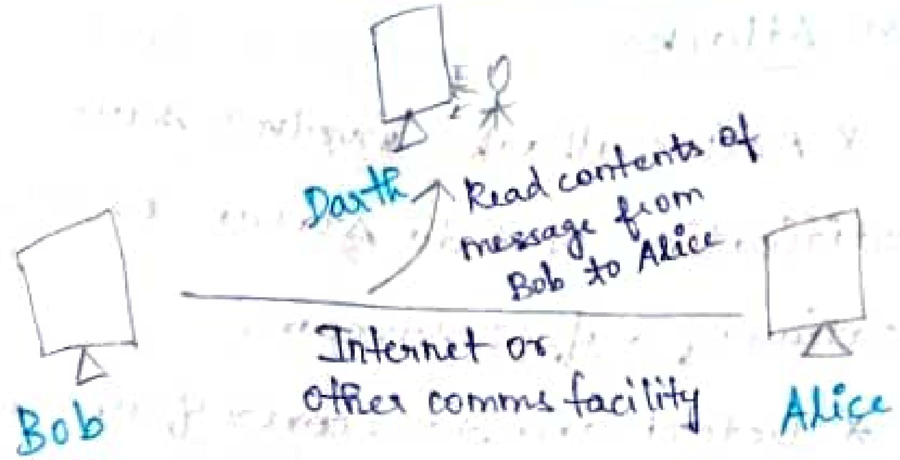
* feasible to prevent the success of these attacks, usually by means of encryptions.

* It emphasis in dealing with passive attacks is on prevention rather than detection.

Types of passive Attacks :-

* Release of message contents

* Traffic Analysis.


Darth
Read contents of message from Bob to Alice
Internet or other comms facility
Bob
Alice

Release of Message Contents :-

* A telephone conversation, an electronic mail message and a transferred file may contain sensitive or confidential information.

Traffic Analysis :-

* It observe the pattern of these message.

* The opponent could determine the location and identity of communication hosts and observe the frequency and length of the message being exchanged.

* the information may be useful in guessing nature of communication.

## Active Attacks :-

* Active attacks involves some modification of data stream or the creation of a false stream.

* Detect and to recover from any disruption. or delay caused.

* It is categorized into,

- => masquerade
- => Replay
- => modification of message
- => denial of service.

## Masquerade :-

* one entity pretends the different entity.

* It includes one of the other forms of active attacks.

## Replay :-

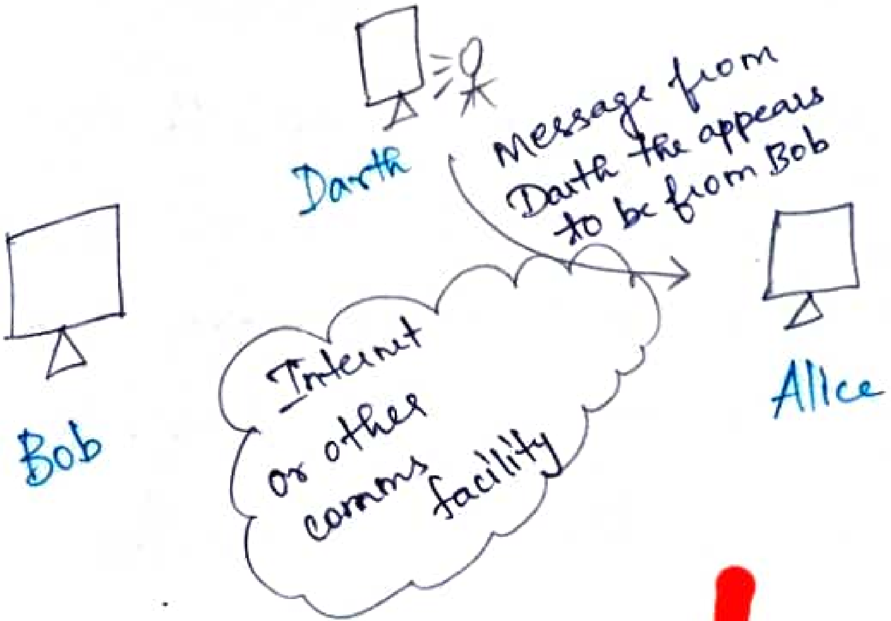
* passive capture of a data unit and its subsequent retransmission to produces an unauthorized effects.

## modification of message :-

* Some portion of message is altered or delayed or reordered to produced unauthorized effect.

## Denial of Service :-

* Disruption of an entire network either by disrupting the network or by over-loading it with network message so as to degrade performance.


Darth
Message from Darth the appears to be from Bob
Bob
Internet or other comms facility
Alice

## UNIT-IV :-

## Kerberos :-

* Kerberos provides a centralized authentication server whose function is to authenticate users to servers and servers to users.

* In kerberos Authentication Server and database is used for client authentication.

* Kerberos runs an third-party trusted server known as the key - Distributed center (KDC)

* Each user and Service on the network is principal.

* The main components of kerberos are,

⇒ Authentication Server (AS)

⇒ Database

⇒ Ticket Granting Server (TGS)

Authentication Server (AS):-

* The Authentication Server performs the iridial authentication and ticket for Ticket Granting Services.

Database:-

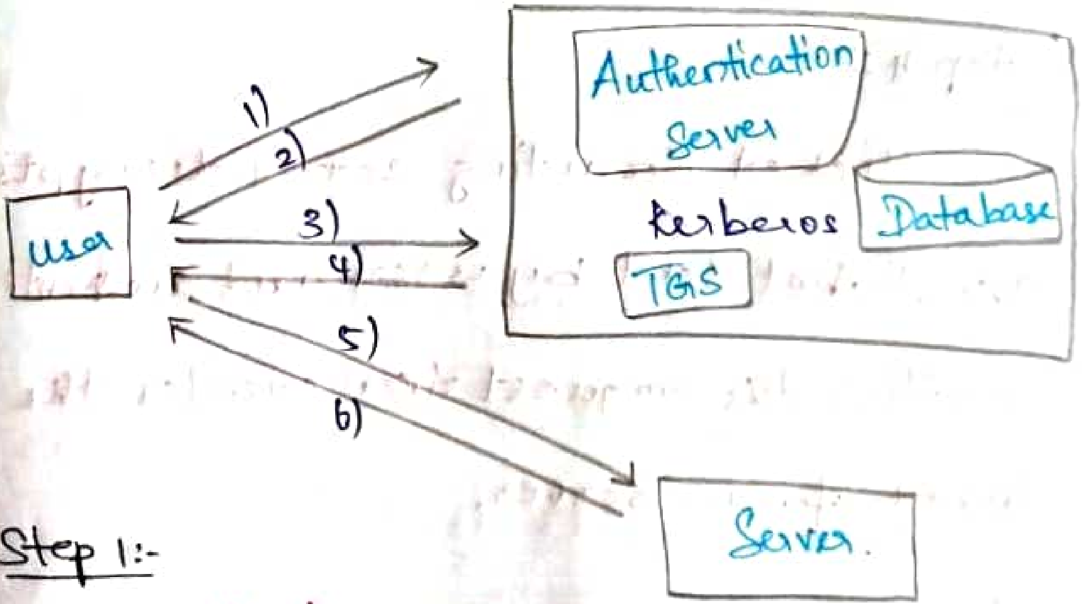
* The Authentication Server verifies the access rights of users in the Database

Ticket Granting service:-

* The TGS issues ticket for the Server.

2

Kerberos overview:-



Step 1:-

User login and request service on the host. thus user requests for ticket - Granting Service.

Step 2 :-

Authentication server verifies user's access right using database and then gives ticket - granting ticket and session key. Results are encrypted using the password of the user.

Step 3 :-

the decryption of the message is done using the password then send the ticket to TGS. the ticket contains authenticators like user-name.

3

Step 4 :-

Ticket Granting server decrypts the ticket sent by user and authenticator verifies the request then creates the ticket from server.

Step 5 :-

the user sends the ticket and Authenticator to the server.

Step 6 :-

The server verifies the ticket & authenticators generate access to the service. After this user can access the service

Limitations :-

* Each network service must be modified individually for use with kerberos.

* It doesn't Work Well in a timeshare environment

* Secured Kerberos Server.

* Requires an always on Kerberos server.

* Stores all password with the encrypted key.

* Scalability.

* workstations are Secured.

* cascading loss of trust.

Kerberos Version 4 :-

* It is an update of the kerberos Software that is a computer authentication system.

* It is a web-based authentication software.

* It was launched in late 1980's.

5

Kerberos version - 5 :-

* It is a later version of the Kerberos Software came after the Kerberos version 4 developed for enchanking security in the authentication.

* It provides the single authentication Service.

* It was launched in 1993.

Uses of Kerberos :-

* Kerberos is used for,

=) Posix

=) NFS

=) Active Directory.

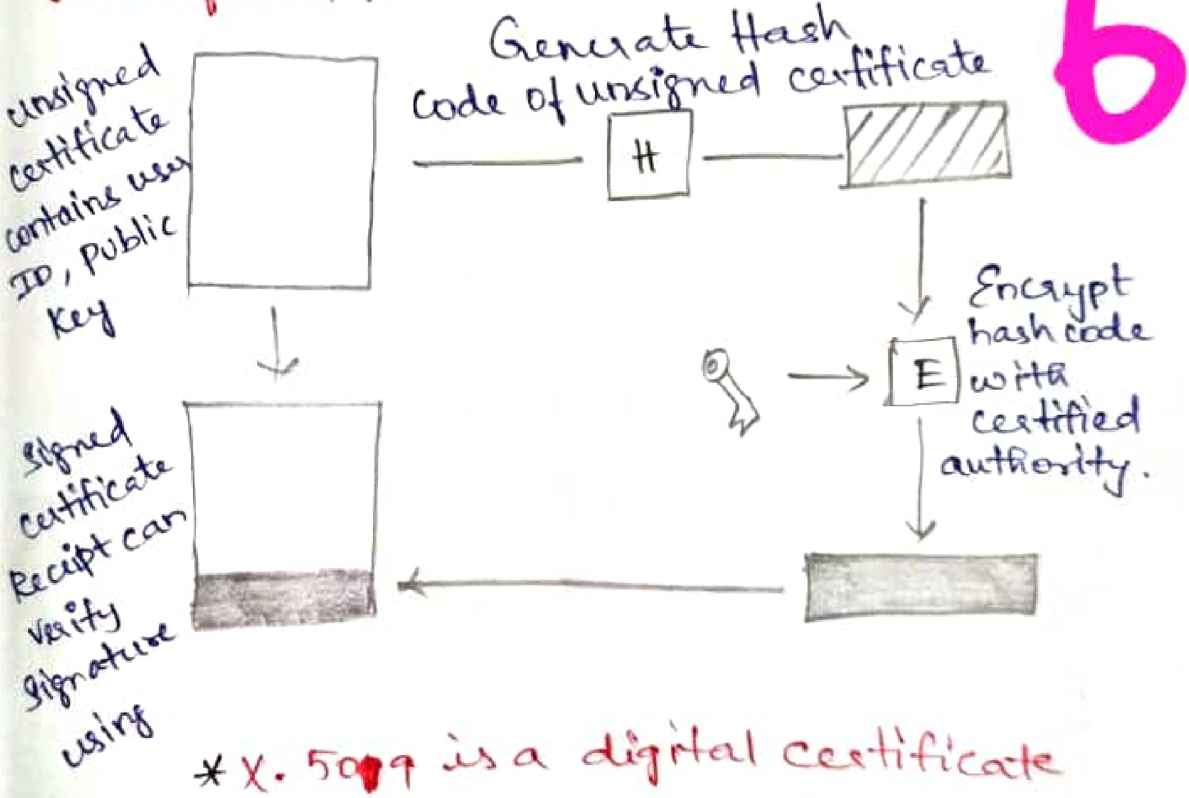
=) samba authentication.

UNIT-IV :-

## X.509 Authentication Service :-

X.509 is a digital certificate that is built on top a widely trusted Standard known as ITU or International Telecommunication union X.509 standard, in which the format of PKI certificate is defined.

6



unsigned certificate contains user ID, public key
Generate Hash code of unsigned certificate
H
E
Encrypt hash code with certified authority.
signed certificate Recipt can verify signature using

*X.509 is a digital certificate that is certificated based authentication security framework that can be used for providing secure transaction processing & private Information.

* these are primarily used for handling the security and identity in computer networking and internet based communication.

validity the

in computer networking and internet based communication.

Diffie Hellman key Exchange:-

* The purpose of algorithm is not the encryption and securely exchange a key that can subsequent encryption of message.
* limited to exchange of secret value.
* Effectiveness
* Difficult of computing discrete - algorithm.

$$K = (Y_B)^{X_A} \bmod q$$

$$K = (Y_A)^{X_B} \bmod q.$$