Rangitha U·N

MODULE 1

Network security consists of the policies and practices adopted to prevent and monitor unauthorized access misuse, modification, denial of computer network and network accessible resource.

Computer security : The protection afforded to an automated info system inorder to attain the applicable objectives of preserving the integrity, availability and confidentiality of info system.

The three concepts is often referred to as the CIA triad

The security requirement triad.

Confidentiality : Preserving authorized restrictions on info access and disclosure.

→ Data confidentiality

→ Privacy

Integrity : Guarding against improper information modification or destruction.

→ Data integrity

→ System integrity

Availability : Ensuring timely and reliable access to and use information, where service is not denied to authorized users

The OSI Security Architecture

The need of some systematic way of defining the requirements for security and characterizing the approach to satisfy those requirements lead to a security architecture.

ITU-T recommendation is the security architecture for OSI defines such a systematic approach The OSI security architecture focuses on security attacks, mechanisms and services.

Security attack: Any action that compromises the security of information owned by † an organization.

Security mechanism: A process that is designed to detect, prevent or recover from a security-attack.

Security service: A processing or comm" service that enhances the security of the data processing system And the info" transfers of an organization.

The service is intended to counter security attacks and make use of one or more security mechanism to provide the service.

Request for Comments IETF

Definitions of Threat & Attack as proposed by RFC 2828

Threat: A potential for violation of security, which exists when there is a circumstance, capability, action or event that could breach security and cause

harm. Threat is a possible danger that might exploit a vuln vulnerability.

Attack: An assault on system security that derives from an intelligent threat. An intelligent act that is a deliberate attempt to evade security services and violate the security policy of a system.

Security Attacks:

- Passive attack: Makes use of info from the system but does not affect system resources.
- Active: Attempts to alter system resources or affect their operation.

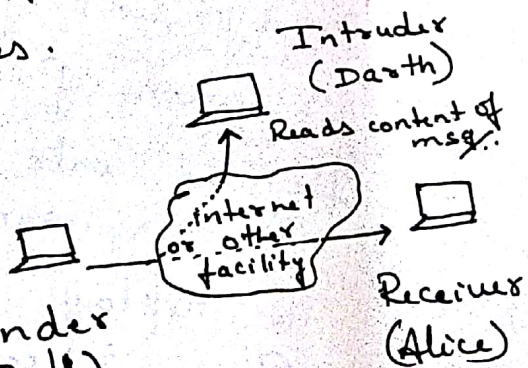
Passive attack:

1. Generally in the nature of eavesdropping or monitoring of transmissions.
2. The goal of the intruder is to obtain info that is being transmitted
3. Two types of passive attack
   - → release of message content
   - → traffic analysis.

Release of message content:-[snooping]

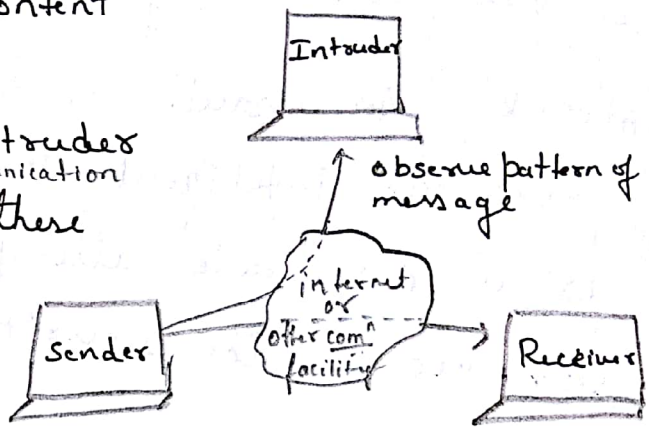
The confidential and sensitive info in the form of email, telephonic conversation, a file has to be prevented from is prone to intruder learning it.

And has to be prevented.



traffic analysis: With encryption of data that is being transmitted, security for the content is provided.

But ~~by analysing~~ the intruder can observe the patterns of these messages & can determine the location and identity of communicating hosts and can note the frequency & length of messages being exchanged.



of communication

military context → frequent comm — denote planning
→ Rapid short comm — denote negotiation
→ who talks to whom - (IP involved)

World War I → British were late to the war Radio waves of Japan field.

Note: Passive attacks are very difficult to detect as there is no alteration of data & even the message traffic is sent & received in an apparently normal fashion.

Emphasis w.r.t passive attacks is on prevention rather than detection.

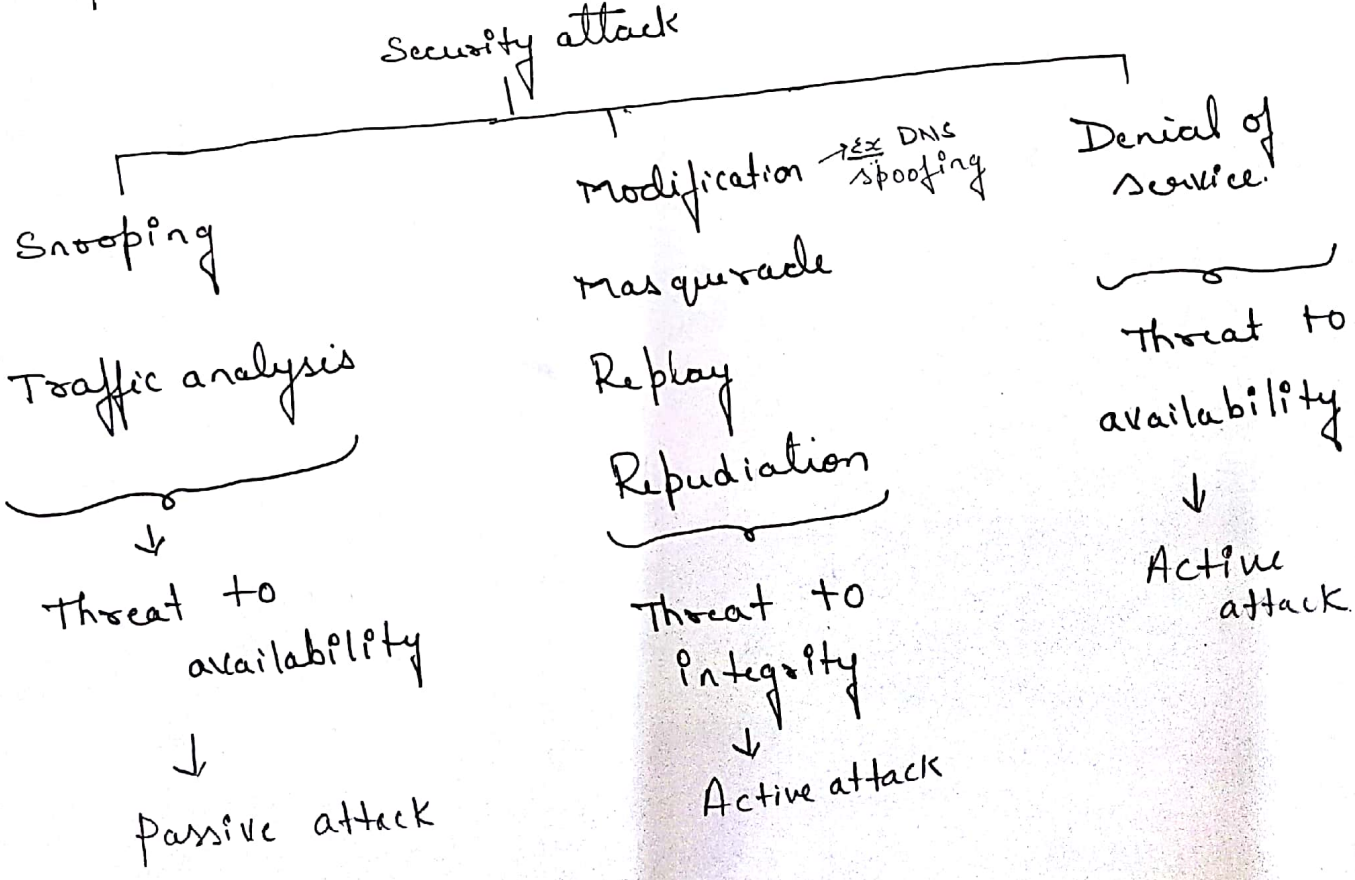
Active attacks

→ modification of data stream
→ Creation of a false stream
→ Devided into four categories viz
  (a) masquerade
  (b) replay
  (c) modification of messages
  (d) denial of service

Attacks

E

* The three goals of security are,
  — Confidentiality, integrity and availability
* These can be threatened by security attacks
* Different literature uses different approaches to categorize the attacks. For example attacks based on infrastructure of the n/w, attacks based on goals of the security etc.
* Attacks with relation to security goals is as below.

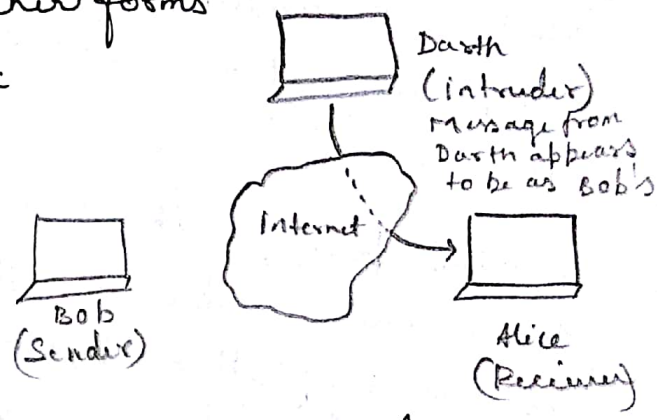


Masquerade attack:- 1. It is an attack in disguise

2. One entity pretends to be different entity.

weak authentication provides chance for masquerade

3. This attack has or includes other forms of attacks Ex: when an authentic user is keying in authentication sequence, it is captured & is replayed after succesfull authentication. This is used by the masqueraded Intruder to get more privileges.



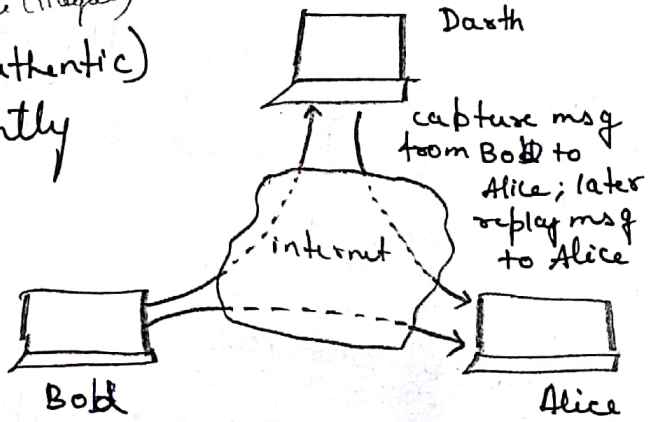
Ex: attacker disguises to be the actual IP

Ex: phising, vishing & send fake page (illegal)

masquerade by spoofing & plans for attack

Replay:- Here passively data(authentic) is is captured & is subsequently retransmitted to produce an unauthorized effect

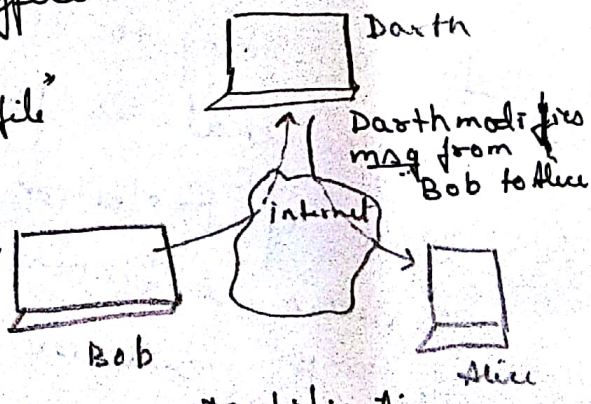
Ex: Key sharing b/w A & B



Replay

modification of messages: Some part of the message is altered or the messages are delayed or reordered to produce an unauthorized effect.

Ex: message "Allow John to read confidential file"
& modified to
message "Allow Fred to read confidential file"

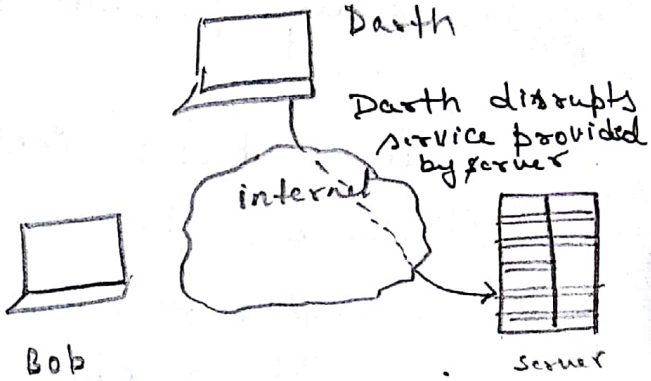


Modification of messages

Denial of service

1. Prevents or stops the normal use or management of communication facilities

Ex :- A destination may be suppressed from receiving messages



Denial of service

2. Other form is the disruption of an entire network. This is done by either disabling the network or by overloading it with messages (junk) so as to degrade performance.

Note: W.r.t active attacks, the goal is to detect [unlike passive], as preventing is difficult because of the potential n/w vulnerabilities, software etc.

Security services

Defn [according to X.800] : Is a service provided by a protocol layer of communicating system that ensures security of the systems or data transfers.

Defn [according to RFC2828] : A processing or communication service that is provided by a system to give a specific kind of protection to system resources. Security services implement security policies and are implemented by security mechanisms.

Security services

Data confidentiality | Data integrity | Authentication | Non repudiation | Access control

X.800 devides the security services into five categories viz:- Authentication, Access control, Data confidentiality Data integrity, Nonrepudiation.

I Authentication :- i. Concerned with assuring an authentic Comm".

ii) In case of a single message tx^n (ex warning message), the authentication service is about assuring the receiver, that the message is from the xt sender.

iii) In case of an interactive to^n blw a source & sender, authentication is viewed at 2 levels.

(a) During the connection initiation that the two communicating entities are authentic (right ones)

(b) Once the connection is established, assurance w.r.t protection the attacks like masquerade has to be provided.

Two specific authentication service defined by X.800

i) Peer entity authentication
Used in association with a logical connection to provide confidence in the identity of the entities connected.

ii) Data origin authentication: Provides assurance that to check whether the source of received data is as claimed [i.e the data is sent from the xt user.]

II Access control : Is the ability to limit and control the access to host systems and applications. DO achieve this, each entity [trying to get the access] is identified or authenticated.

III Data Confidentiality :-

The protection of data from unauthorized disclosure.

The protection of data can be w.r.t to its content (protection), where protocols like TCP can provide confidentiality over a period of time for the complete data or for specific fields of a message.

The protection of data can be w.r.t its traffic (pattern) flow protection.

1) connection confidentiality : Protection of all user data on a connection

2) connectionless confidentiality : Protection of all user data in a single data block!

Data Integrity :-

3) selective-field confidentiality : confidentiality of selected fields of user data.

4) Traffic-flow confidentiality : Protection of "info", that might be derived from the observation of traffic flows.

IV Data integrity:- The assurance that the data received are exactly as sent by an authorized entity (ie, contain no modification, insertion, deletion or replay).

i) Connection Integrity with Recovery [all user data]
ii) connection " without Recovery ["]
iii) Selective-field connection integrity [all user data]
iv) selective field connectionless integrity [for data block]
v) Connection less integrity [for data block]

V Non repudiation: Prevents either sender or receiver from denying a transmitted message.

* Non repudiation, origin: proof that the message was sent by the specified party.
* Non repudiation, destination: Proof that the message was received by the specified party.

Security Mechanisms: these are broadly denided into
1. specific to some protocols (Ex:. TCP)
2. Non specific to " "

I specify security mechanisms
1. Encipherment: mathematical algorithms are used to tranform the data
2. Digital signature: It is a proof for source and the integrity of data as a protection against forgery. Electronically signed by sender and electronically verified by reciver.
3. Access control: Involves mechanisms that enforce access rights.

4. Data integrity:- Mechanisms to assure integrity of data.

5. Authentication Exchange: A mechanism intended to ensure the identity of an entity by means of info" exchange.

6. Traffic padding: Insertion of bits into gaps in a data stream to misguide traffic analysis attempt.

7. Routing control: Allows route selection and route changing mechanisms (Composed of H/w & s/w, helps in selecting the best path for efficient delivery of data configured according to constraints [e.g., cost, performance])

8. Notarization: Use of a trusted third party to assure certain properties of a data exchange.

II Non-specific security mechanisms

1. Trusted functionality: Perceived to be correct (ex. as established by security policy)

2. Security Label: Marking bound to a resource that designates security attributes of that resource.
[ex. 2.4G Motosicc (nodes & routers)]

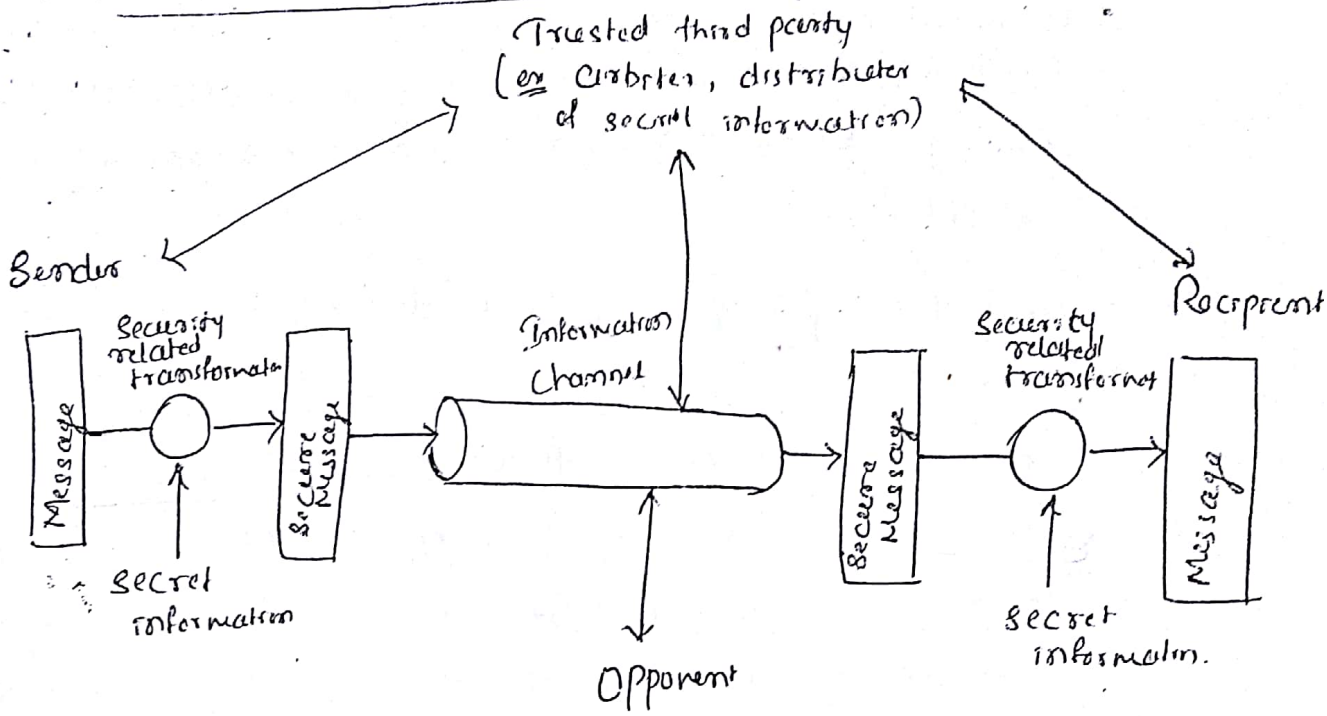
3. Security audit trail: Data collected & used to facilitate a security audit

4. Security Recovery: Takes care of recovery actions using some event handling & management functions.
(& Event detection)

Relation blw security services & security mechanisms

Security service	Security mechanism
Data confidentiality	Encipherment & routing control
Data integrity	Encipherment, digital sig", data integrity
Authentication	Encipherment, " , Auth Exchange
Non repudiation	Dig signature, data integrity & notarization
Access control	Access control mechanism.

* A model for Network security



In the above figure a message is to be transferred from one party to another across some sort of Internet services

→ A logical information channel is established by defining a route through the internet from source to destination and by the cooperative use of communication protocols

→ Security aspects come into play when it is necessary or desirable to protect the information transmission from an opponent who may present a threat to confidentiality, authenticity and so on.

→ All of the techniques for providing security have two components

1) A security related transformation on the information to be sent. eg include the encryption of the message which scrambles the message so that it is unreadable by the opponent and the addition of a code based on the contents of the message, which can be used to verify the identity of the sender.

2) Some secret information shared by the two principals and it is hoped unknown to the opponent. eg an encryption key used in conjunction with the transformation to scramble the message before transmission and unscramble it on reception

→ A trusted third party may be needed to achieve secure transmission.

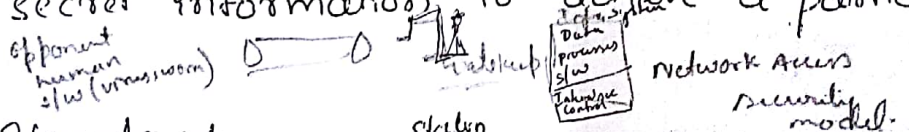
→ The general model shows that there are 4 basic tasks in designing a particular security service

1) Design an algorithm for performing the security related transformation. The algorithm should be such that an opponent cannot defeat its purpose

2) Generate the secret information to be used with algorithm

3) Develop methods for the distribution and sharing of the secret information

4) Specify a protocol to be used by the two entities that makes use of the security algorithm and the secret information to achieve a particular security service.



* Standards

→ The security techniques and applications are specified as standards.

→ The standards have been developed to cover management practices and the overall architecture of security mechanisms and services

→ Various organization have been involved in the development and promotion of these standards namely

1) National Institute of Standards and Technology:

NIST is a US federal agency that deals with measurement

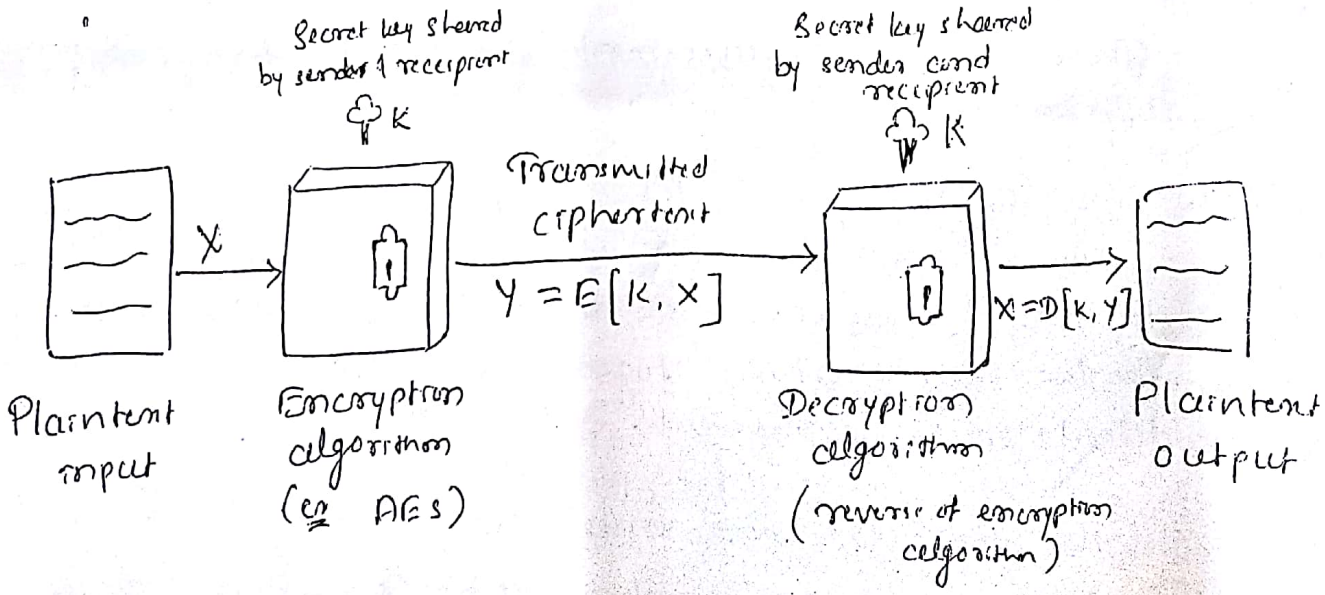
science, standards and technology related to U.S. government use and to the promotion of U.S. private sector innovation
FIPSPubs & Special Publication (SP)

2) Internet Society : ISOC is a professional membership society with worldwide organizational & individual membership. It includes Internet Engineering Task Force (IETF) and the Internet Architecture Board (IAB). These organizations develop Internet standards and related specifications.

* Symmetric Encryption Principles

stallings 4th ed.

Simplified model of symmetric encryption



Symmetric encryption scheme has 5 ingredients

1. *Plaintext : This is the original message or data that is fed into the algorithm as input.
2. * Encryption algorithm : The encryption algorithm performs various substitutions and transformations on the plaintext.

(3) * Secret key : The secret key is used input to the encryption algorithm. The key is a value independent of the plaintext and of the algorithm. The algorithm will produce a different output depending on the specific key being used at the time. The exact substitutions and transformations performed by the algorithm depend on the key

(4) * Ciphertext : This is the scrambled message produced as output. It depends on the plaintext and the secret key. For a given message two different keys will produce two different ciphertexts.

(5) * Decryption algorithm: This is reverse of encryption algorithm. It takes ciphertext and secret key and produces the original plaintext.

There are 2 requirements for secure use of symmetric encryption

1) We need a strong encryption algorithm.

The opponent should be unable to decrypt ciphertext or discover the key even if he or she is in possession of a number of ciphertexts together with the plaintext that produced each ciphertext.

2) Sender and receiver must have obtained copies of the secret key in a secure fashion and must keep the key secure. If someone can discover the key and knows the algorithm all communication using the key is readable.

Cryptographic systems are ~~characterized~~ classified along three independent dimensions

1) The type of operations used for transforming plaintext to ciphertext : All encryption algorithms are based on two

General principles:

Substitution, in which each element in the plaintext is mapped into another element and.

transposition; in which elements in the plaintext are rearranged. The fundamental requirement is that no info be lost.

Product system ⇒ multiple stage of substitution & transposition.

2) The number of keys used: If both the sender and receiver use the same key, the system is reffered to as symmetric, single key, secret key or conventional encryption. If the sender & receiver use different keys, the system is reffered to as asymmetric, two-key or public key encryption.

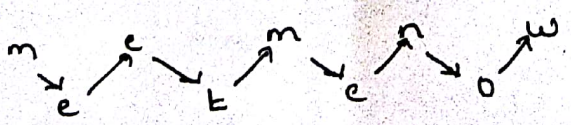
3) The way in which the plaintext is processed: A block cipher processes the i/p one block of element (usually in bits) at a time, produces an o/p block for each i/p block. A stream cipher processes the i/p elements [usually in bytes] continuously, producing o/p, one element at a time as it goes along.

Note:- Ex Plaintext to ciphertext conversion using

Substitution Hello → ABOOR → monoalphabetic

Hello → ABOZR → Non-monoalphabetic

Transposition Ex: rail fence cipher [plaintext is written in zig-zag pattern]



⇒ memnwetEO

memnw etc O
1 3 5 7 9 2 4 6 8

Can be written in matrix also agreeing upon no of colm

m e e
t n e ⇒ mtnemoeeow
n o w

Note:-

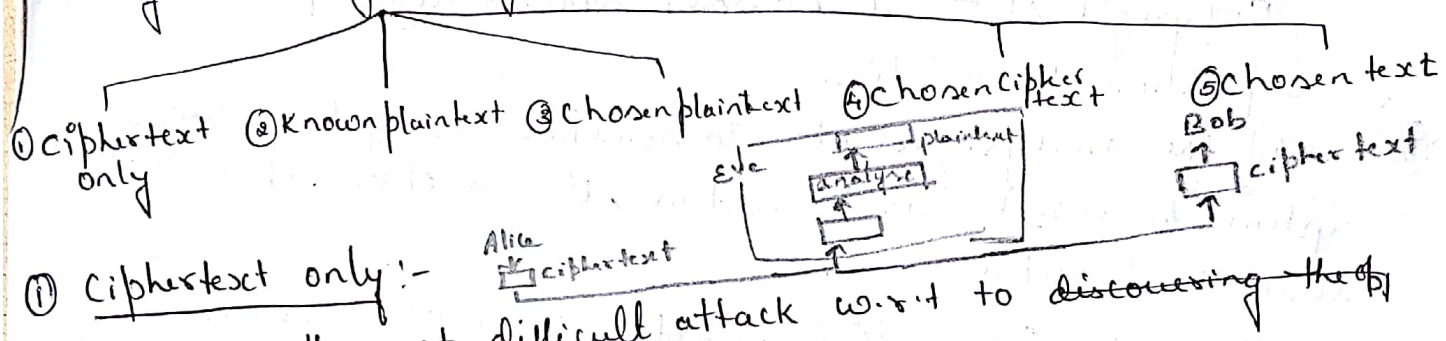
Cryptography is the science and art of creating secret codes.

Cryptanalysis is the science and art of breaking those codes. It is a step towards knowing the vulnerability of the cryptosystem.

The study of cryptanalysis helps us create better secret codes.

Cryptanalysis : The process of attempting to discover the plaintext or the key is known as cryptanalysis. The process of finding these depends on the nature of the encryption scheme and the information available to the cryptanalyst.

Based on the information known, the classification of the cryptanalysis is as shown.



① Ciphertext only :-

* It is the most difficult attack w.r.t to ~~discovering the~~ meeting the objective of cryptanalysis.
* Brute-force approach can be used for trying all possible keys. If the key space is very large, this becomes impractical.
* Here the opponent has only the ciphertext for analysis on which various statistical tests are applied. To use this approach, the opponent must have some general idea of the type of plaintext that is concealed such as English or French text, an exe file, a java src listing, an accounting file etc. To prevent the attack through statistical approach, the cipher should hide the characteristics of the languages.

② Known plaintext :

* The analyst may be able to capture plaintext as well as their encryptions [ie plaintext / ciphertext pairs]
* In some cases analyst may know that certain plaintext patterns will appear in a message.

Ex Postscript format (page description language used in publishing), standardized header or banner to an electronic fund transfer message & so on.

* With the knowledge of the plaint text and its transformation, Key may be deduced.

③ Chosen ~~ciphertext~~ plaintext (~~ciphertext-only~~ probable word attack).

* Here if the opponent is working on some specific info^n, then parts of the message may be known.

Ex In case of accounting file, the opponent may know the placement of certain keywords in the header of the file.

Copyright statement in some standardized position of a corporation transaction.

④ * If the analyst is able to somehow to get the source system to insert into the system, then a chosen-plaintext attack is possible.

④ Chosen ciphertext and ⑤ chosen text attacks are less commonly ~~attacked~~ employed as cryptanalytic techniques.

An encryption scheme is computationally secure if the ciphertext generated by the scheme meets one or both the following criteria.

→ the cost of breaking the cipher exceeds the value of the encrypted info^n..

→ the time required to break the cipher exceeds the ~~less~~ useful lifetime of the info^n.

Table 2.2 [Average time required for exhaustive key search [Brute force].

Feistel cipher structure

The literature devides the symmetric ciphers into two broad categories stream ciphers and block ciphers.

Stream cipher:- Here encryption and decryption are done one symbol (such as a character or a bit) at a time

ex: If we have a plaintext stream P, a ciphertext stream C and the key stream K

$P = P_1 P_2 P_3 \cdots$ $\quad C = C_1 C_2 C_3 \cdots$ $\quad K = K_1, K_2, K_3 \cdots$

$C_1 = E(P_1, K_1)$ $\quad C_2 = E(P_2, K_2)$ $\quad C_3 = E(P_3, K_3)$

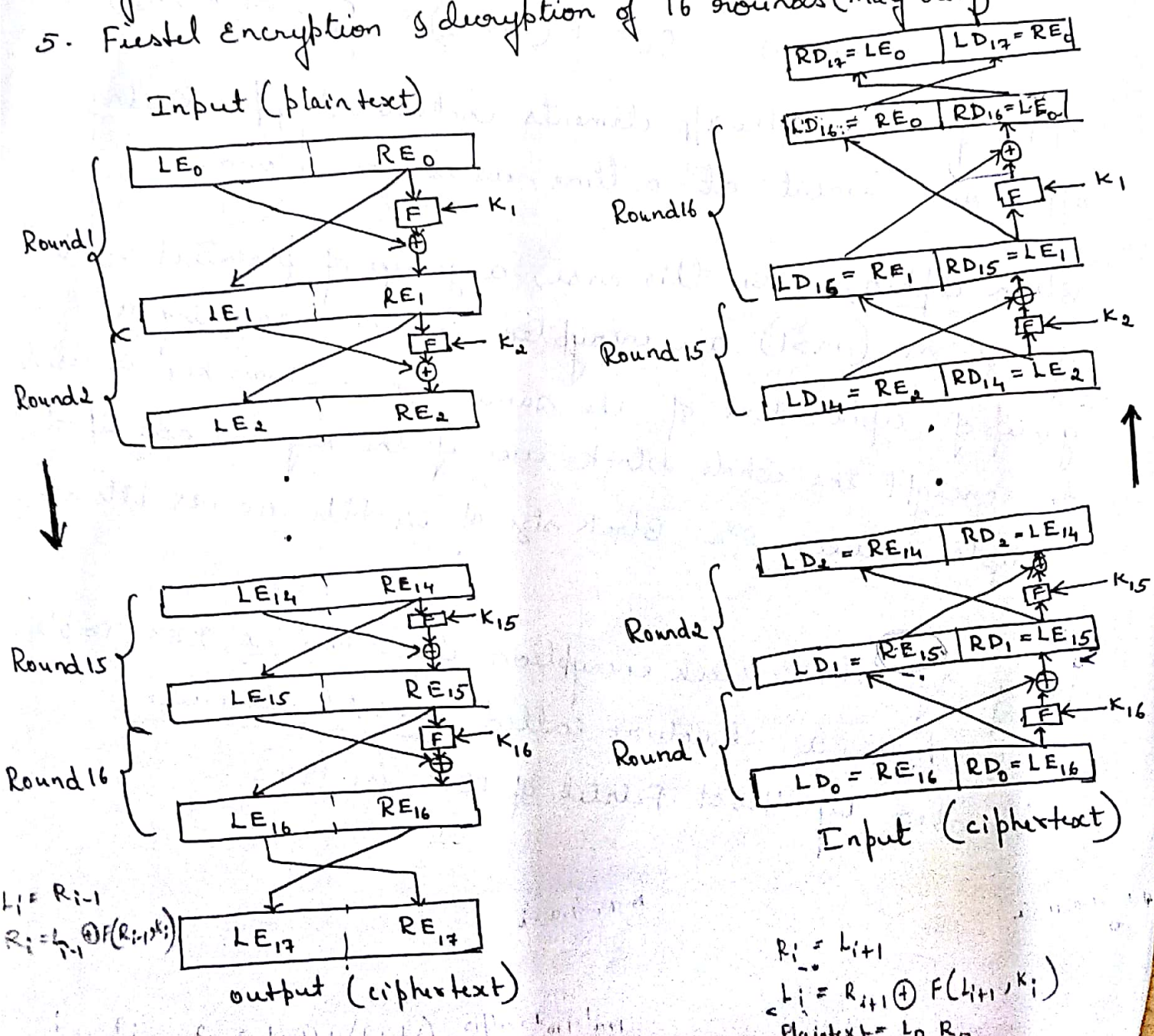
It processes the i/p elements continuously, producing o/p one element at a time, as it goes along.

Block cipher:- In this case, a group of plaintext symbol of size m ($m > 1$) are encrypted together creating a group of cipher text of the same size. Single key is used to encrypt the whole block even if the key is made up of multiple values. ex: Block size of 64 bits or 128 bits etc.

Many symmetric Block encryption algorithms ex: DES, Triple DES have a structure called **Feistel structure** described by Horst Feistel of IBM in 1973.

Description of Feistel Cipher Structure

1. The inputs to the encryption algorithm are a plaintext block of length 2w bits and a key K.
2. The plaintext block is divided into two halves, LE_0 & RE_0.
3. The two halves of data pass through n rounds of processing & then combine to produce the ciphertext block.
4. Each round i has inputs LE_{i-1} & RE_{i-1} derived from the previous round, as well as a subkey K_i derived from the overall key K. K_i's are generated by a subkey generation algorithm. All K_is are different from K and from eachother.
5. Feistel Encryption & decryption of 16 rounds (may vary) is shown below.



$K_1 \rightarrow$ 1

2

3

⋮

14

15

16 $\rightarrow K_{16}$

Encryption

16 — K_1

15

14

⋮

3

2

1 — K_{16}

Decryption

encryption

$$\begin{cases} L_i = R_{i-1} \\ R_i = L_{i-1} \oplus F(R_{i-1}, K_i) \end{cases}$$

or

$$\begin{cases} L_{i+1} = R_i \\ R_{i+1} = L_i \oplus F(R_i, K_{i+1}) \end{cases}$$

Ex ..

$i = 16$

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

$$LE_{16} = RE_{15}$$

$$RE_{16} = LE_{15} \oplus F(RE_{15}, K_{16})$$

Decryption

$$LD_0 = RE_{16} \qquad RD_0 = LE_{16}$$

$$LD_1 = RE_{15} \qquad RD_1 = LE_{15}$$

$$\begin{cases} RE_i = LE_{i+1} \\ LE_i = RE_{i+1} \oplus F(LE_{i+1}, K_{i+1}) \end{cases}$$

or

$$\begin{cases} RE_{i-1} = LE_i \\ LE_{i-1} = RE_i \oplus F(LE_i, K_i) \end{cases}$$

Ex ..

$i = 15$

$$RE_{15} = LE_{16}$$

$$LE_{15} = RE_{16} \oplus F(LE_{16}, K_{16})$$

6. A substitution is performed on the left half of the data. Substitution is done by applying a round function F to the right half of the data & then taking EX-OR of the o/p of that function and the left half of the data.

7. Following substitution is the permutation, where the interchange of two halves of the data takes place.

Parameters & design features in realization of symmetric block cipher

1. Block size:- Larger block size yields greater security but with the reduced encryption/decryption speed. 128 bits block size is universal among recent block cipher designs.

2. Key size:- Larger key size greater security with reduced speed. Generally used length is 128 bits.

3. Number of rounds:- Increased security with increased no. of rounds. Typically used is 16 rounds.

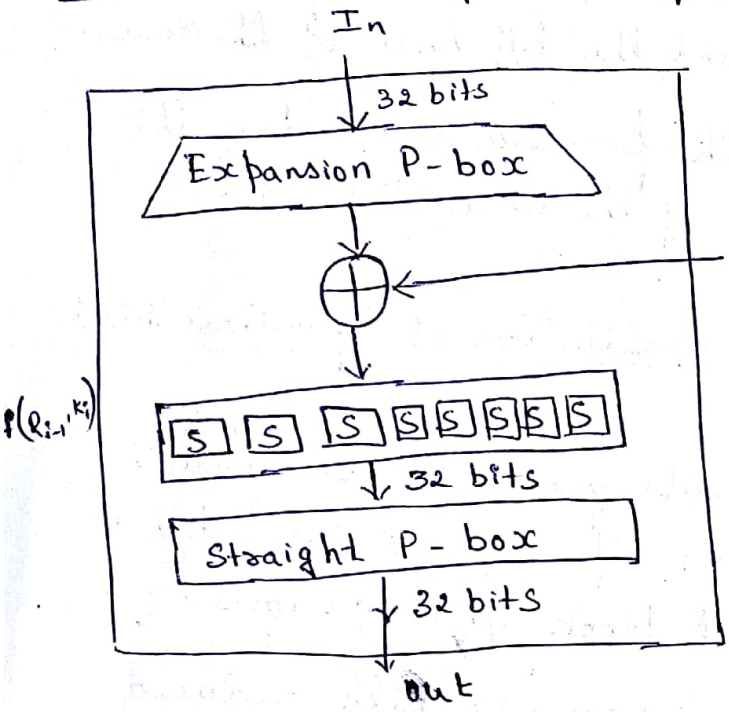
4. Subkey generation algorithm:- Greater complexity should lead to greater difficulty of cryptanalysis.

5. Round function:- Greater complexity leads to greater complexity.

6. Fast software encryption/decryption: In many cases encryption is embedded in applications or utility functions in such a way that it prevents a H/w implementation. Hence speed of algorithm becomes a concern.

7. Ease of analysis: With ease of analysis, cryptanalytic vulnerabilities can be identified & therfore develop higher level of assurance to its strength.

Note: DES algorithms function Description (DES topic next)



① DES function applies a 48-bit key to the rightmost 32 bits (R_{i-1}) to produce 32-bit o/p

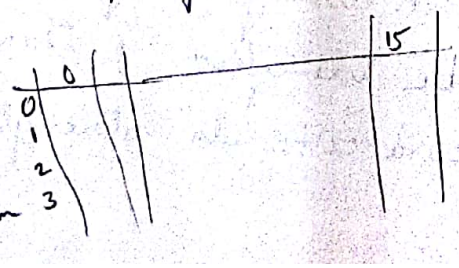
② This function is made up of four sections
- → expansion P-box
- → whitener (adds key)
- → group of S-boxes
- → straight P-box

① Expansion P-box:- 32 bit R_{i-1} is expanded to 48 bits. 32 bits R_{i-1} is devided into 8 chunks of 4 bit each. Expanded to 6 bit chunk as shown

② whitener (XOR) : XOR performed on expanded right section and the round key.

③ S-boxes: Does the real mixing (confusion). DES uses 8 s-boxes, each with 6 bit input & 4 bit o/p. Substitution in each box follows a predetermined rule based on a 4-row by 16 column table.

④ straight permutation:- 32 bit i/p with 32 bit o/p. I/P - O/P relationship for this op^n is according to a fixed table.



1000 !
11 - 3 row
01 - 1 column

general principles : substitution, in which each element in the plaintext is mapped into another element and transposition in which elements in the plaintext are rearranged. The fundamental requirement is that no information be los

2) The number of keys used: If both the sender and receiver use the same key, the system is referred to as symmetric, single-key, secret key or conventional encryptio If the sender and receiver use different keys, the system i referred to as asymmetric, two-key or public key encryption

3) The way in which the plaintext is processed : A block ciphe processes the input one block of elements at a time, produci an output block for each input block. A stream cipher processes the input elements continuously, producing output one element at a time, as it goes along.

* Symmetric block encryption algorithms

The most commonly used symmetric encryption algorithms are block ciphers.

A block cipher is one in which a block of plainte is treated as a whole and used to produce a ciphertext block of equal length. Typically a block size of 64 or 128 bits is used.

Stream cipher

* Data Encryption Standards.

DES ① - William Stallings

→ The most widely used encryption scheme is based on the Data Encryption standard (DES) in 1977 as Federal Information Processing standard 46 (FIPS 46) by the National Bureau of standards now known as National Institute of Standards and technology (NIST).

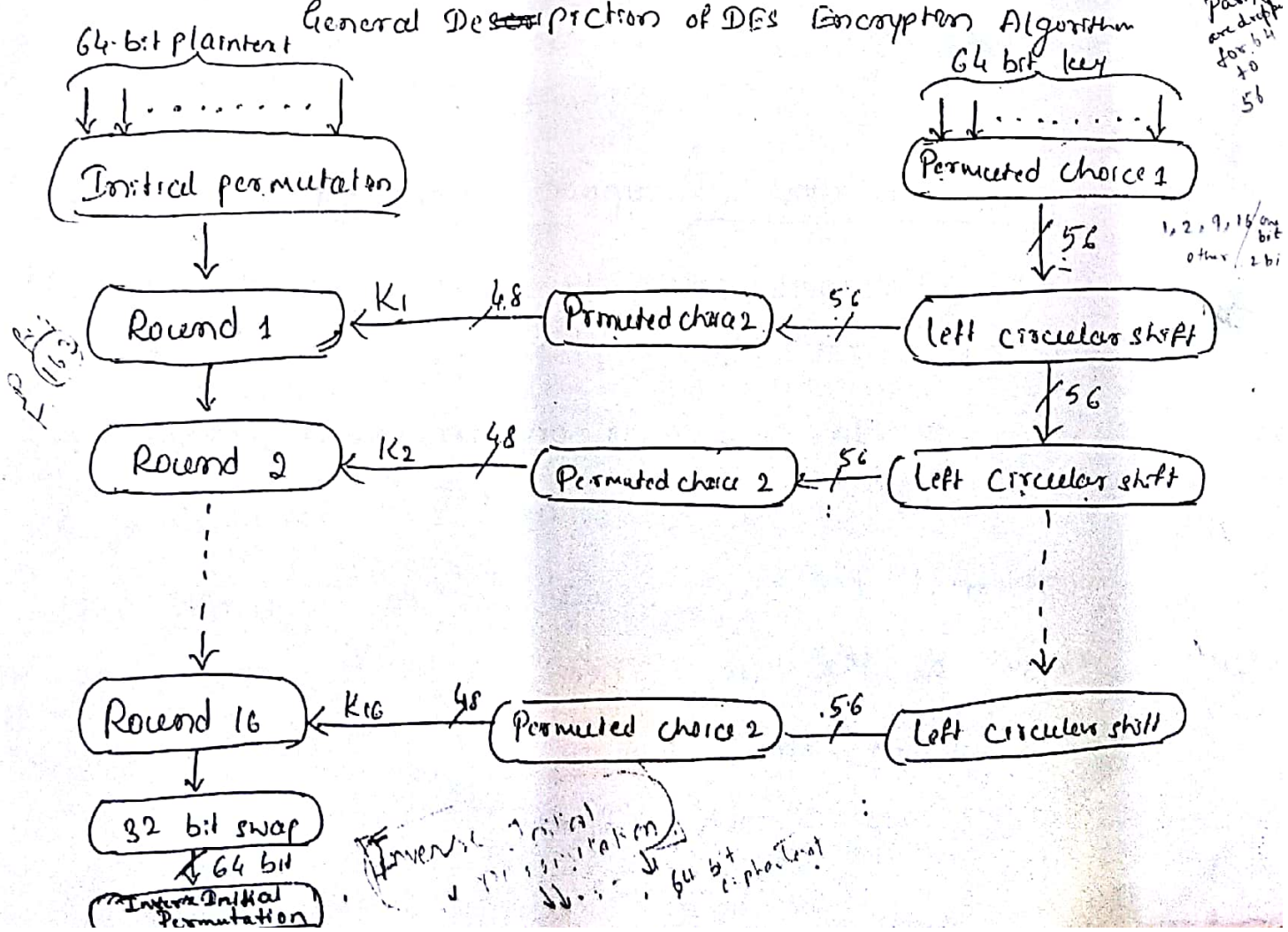
→ The algorithm itself is referred to as the Data Encryption Algorithm (DEA)

IBM (LUCIFER).

Discription of the algorithm: The plaintext is 64 bits in length and the key is 56 bits in length. Longer plaintext amounts are processed in 64 bit blocks.

There are 16 rounds of processing. From the original 56 bit key, 16 subkeys are generated, one of which is used for each round.

General Description of DES Encryption Algorithm



DES (2) With respect to figure on the left hand side the processing of the plaintext proceeds in 3 phases.

→ First the 64 bit plaintext passes through an initial permutation (IP) that rearranges the bits to produce the permuted input.

→ This is followed by a phase consisting of sixteen rounds the same function, which involves both permutation and substitution functions.

→ The o/p of the last (16th) round consists of 64 bits that are a function of the input plaintext and the key

→ The left and right halves of the output are swapped to produce the preoutput.

→ Finally the preoutput is passed through a permutation [IP⁻¹] that is the inverse of the initial permutation function to produce 64 bit ciphertext.

→ The right hand portion of the figure shows the way in which 56 bit key is used.

→ Initially the key is passed through a permutation function. Then for each of the 16 rounds a subkey is produced by the combination of a left circular shift and a permutation.

→ The permutation function is same for each round but a different ~~key~~ subkey is produced because of repeated shifts of the key bits

DES (5) encryption process.

→ Use the ciphertext as input to the DES algorithm, but use the subkeys K_i in reverse order. i.e. Use K_{16} on the first iteration, K_{15} on second iteration and so on until K_1 is used on 16th and last iteration.

* Avalanche effect -

* Strength of DES

Stallings

The strength of DES depends upon 2 points

→ Nature of the DES algorithm

→ Use of 56 bit keys.

Nature of DES algorithm :

→ This point explains the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm.

→ Over the years, there have been numerous attempts to find and exploit weaknesses in the algorithm, making DES the most studied encryption algorithm in existence.

Use of 56 bit keys :

→ With a key length of 56 bits there are 2^{56} possible keys., which is approximately 7.2×10^{16} keys.

→ On the face of it, a brute force attack appears impractical.

→ Assuming that on average half the key space h
to be searched, a single machine performing on
DES encryption per microsecond would take more
than a 1000 years to break the cipher.

→ However the assumption of one encryption per mic
is overly conservative.

→ DES finally proved insecure in July 1988 coz o
less price in hardware as ~~speed~~ increase
speed.

EFF

→ It is important to note that there is more to
key search attack than simply running through a
possible keys.

→ The only form of attack that could be made on
encryption algorithm is brute force.

→ The way to counter such attacks is use longer
keys.

* Triple DES

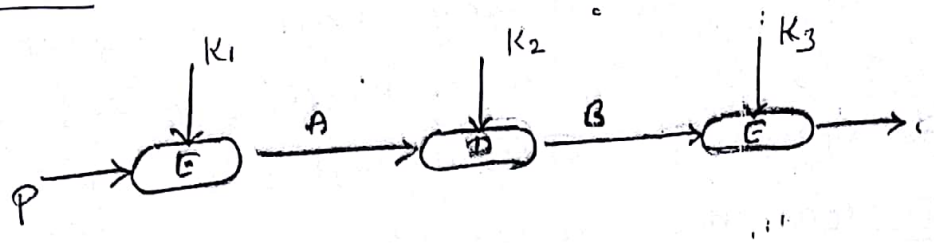
→ Triple DES (3DES) was first standardized for use in
financial applications in ANSI standard X9.17 in 198

→ 3DES uses three keys and three executions of the DES
algorithm.

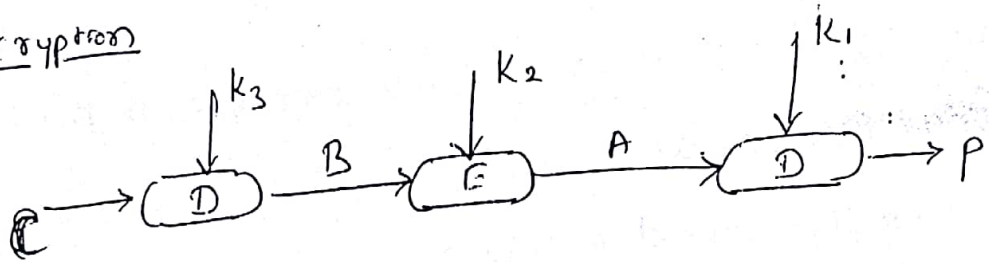
$K = K_1, K_2, K_3$

$3 \times 56 = 168$ bits

Encryption



Decryption



→ The function follows an encrypt-decrypt-encr (EDE) sequence.

$$C = E(K_3, D(K_2, E(K_1, P)))$$

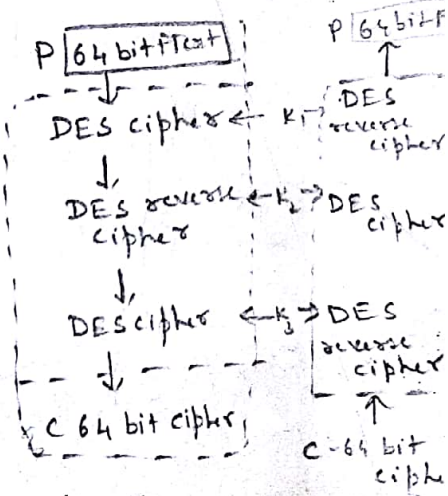
Where

C = Ciphertext

P = plaintext

E [K, X] = encryption of X using key K

D [K, Y] = decryption of Y using key K



Decryption is simply the same operation with the keys reversed

$$P = D(K_1, E(K_2, D(K_3, C)))$$

There is no cryptographic significance to the use of decryption for the second stage of 3 DES encryption.

Its only advantage is that it allows users of 3DES to decrypt data encrypted by users of the older single DES.

$$C = E(K_1, D(K_1, E(K_1, P))) = E[K, P]$$

With 3 distinct keys, 3 DES has an effective key length of 168 bits. FIPS 46-3 also allows for the use of two keys with $K_1 = K_3$ this provides for a key length of 112 bits.

64×2 = 128, 64×3 = 192

FIPS (Federal Information Procedures System) 46-3 includes the following guidelines for 3DES

→ 3DES is the FIPS approved symmetric encryption algorithm of choice

→ The original DES, which uses a single 56-bit key is permitted under the standard for legacy systems only. New procurements should support 3DES

→ Government organizations with legacy DES systems are encouraged to transition to 3DES

→ It is anticipated that 3DES and AES will coexist as FIPS-approved algorithms, allowing for a graduated transition to AES.

0 1 2 3
4x8 4x8 4x8 4x8
32 32 32 32 = 128

* Advanced Encryption Standards

32x6 = 192

Drawbacks of 3DES

→ the algorithm is relatively sluggish (later or lazy) in software.

→ the original DEA was designed for mid-1970s hardware implementation and does not produce efficient sw c

→ 3DES has 3 times of rounds than DEA hence it is correspondingly slower.

→ Another drawback is that both DEA and 3DES uses a 64 bit block size. For reasons of both efficiency and security a larger block size is desirable

B.C → Every to all
Dr → one to all

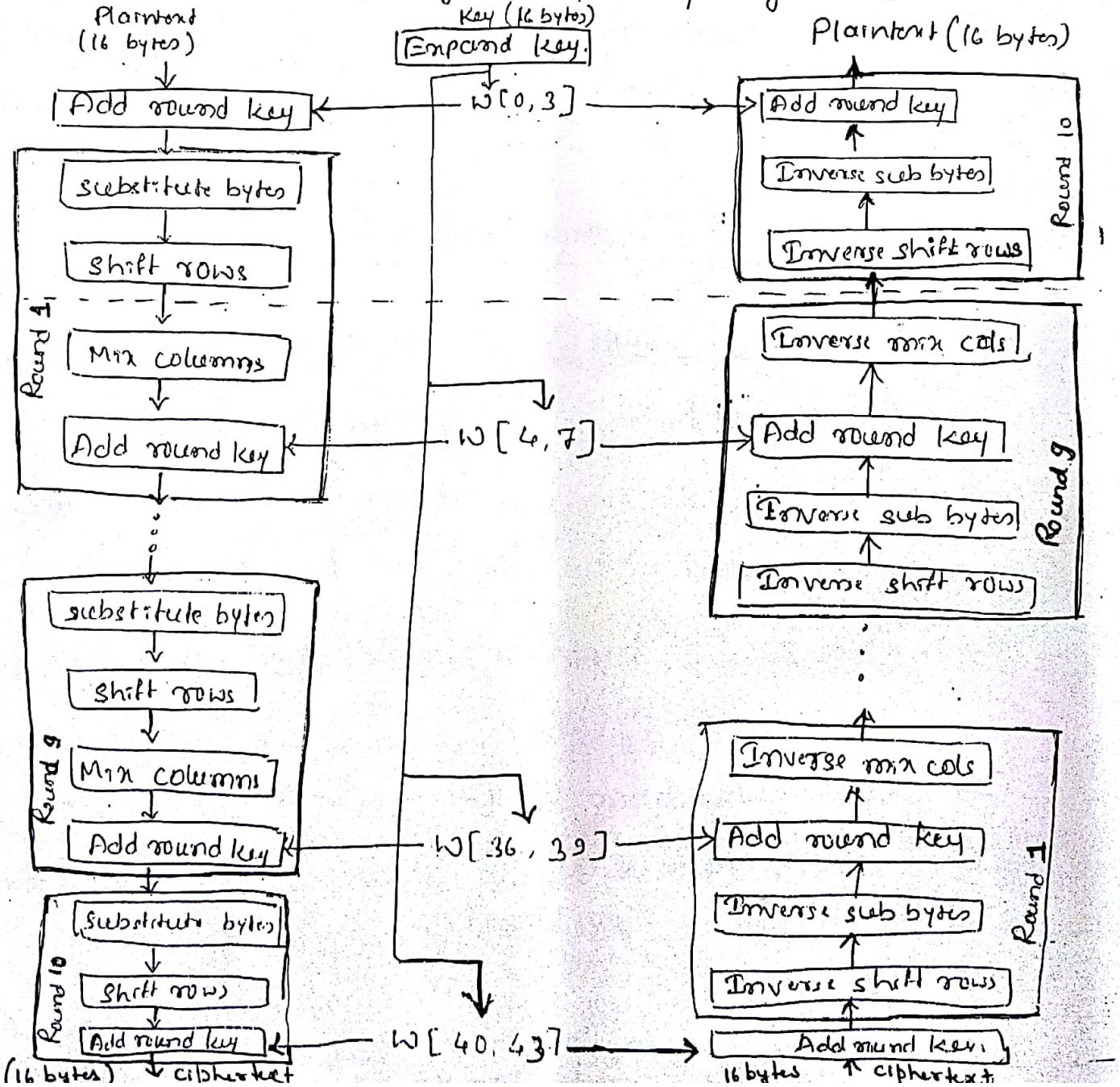
Because of the above drawbacks 3DES is not a reasonable candidate for long term use. As a replacement NIST in 1997 issued a call for proposals for a new Advanced Encryption Standard (AES) which should have security strength equal to or better than 3DES and significantly improved efficiency.

Rijndael (Dr John Daeman & Dr. Vincent Rijmen)

Overview of the Algorithm

→ AES uses a block length of 128 bits and a key length that can be 128, 192 or 256 bits (10 rounds, 12 rounds, 14 rounds)

→ Here we are considering 128 bit key length.



→ The input to the encryption and decryption algorithms is a single 128 bit blocks.

The following ~~observations has been made~~ is the structure for AES

1) AES does not use a Feistel structure but processes the entire data block in parallel during each round using substitutions and permutations

2) The key that is provided as input is expanded into an array of forty-four 32 bit words w[i]. Four distinct words (128 bits) serve as a round key for each round.

3) 4 different stages are used, one of permutation and 3 of substitution.

- Substitute bytes :- Uses a table [S-box] to perform a byte-by-byte substitution of the block.
- Shift rows :- A simple permutation that is performed row by row
- Mix columns :- A substitution that alters each byte in a columns as a function of all of the bytes in the column.
- Add round key :- A simple bitwise XOR of the current block with a portion of the expanded key.

4) For both encryption and decryption the cipher begins with an Add Round Key stage, followed by nine rounds that each includes all four stages, followed by a tenth round of 3 stages.

5) Using the Add round key stage makes use of the key. The cipher begins and ends with an Add Round Key stage. Any other stage, applied at the beginning or end, is reversible without knowledge of the key and so would add no security [other stages provide confusion, diffusion and nonlinearity]

6) The Add Round Key stage by itself would not be formidable.

7) Each stage is easily reversible. For the substitute byte, shift row, and Mix column stages, an inverse function is used in the decryption algorithm. For the Add Round key stage, the inverse is achieved by XORing the same round key to the block, using the result that $A \oplus B \oplus B = A$

8) As with most block ciphers the decryption algorithm makes use of the expanded key in reverse order.

However the decryption algorithm is not identical to the encryption algorithm.

9) Once it is established that all 4 stages are reversible, it is easy to verify that decryption does recover the plaintext.

10) The final round of both encryption and decryption consists of only 3 stages.

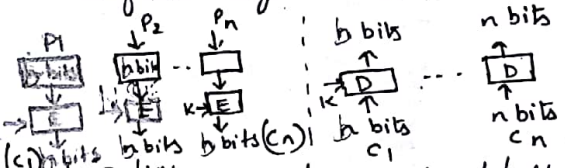
E C B
C B C
C F B
O F B
C T R

CIPHER BLOCK MODES OF OPERATION.

To apply a block cipher in a variety of applications, 5 modes of operation have been defined by NIST.

ECB, CBC, CFB, OFB

1. Electronic Codebook Mode:



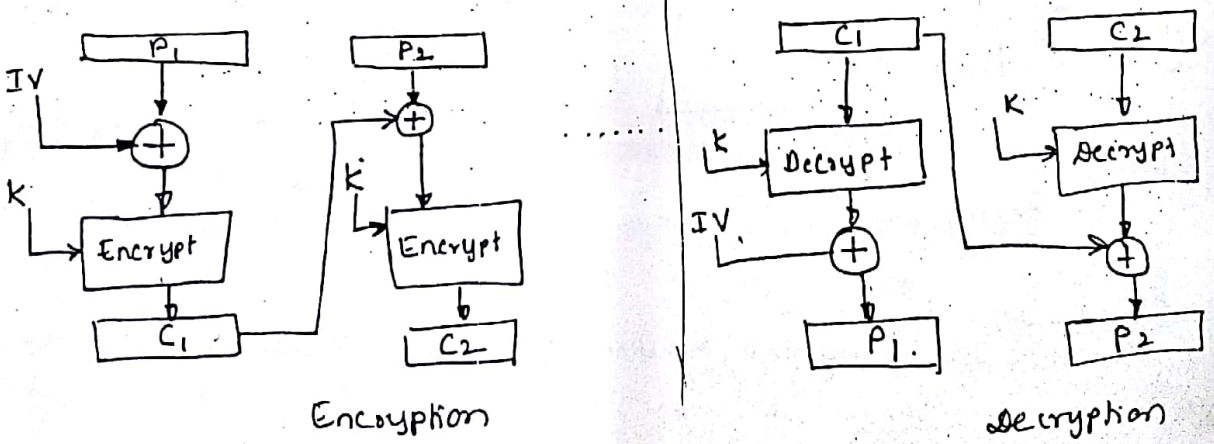
encryption for detailed

The plaintext is handled b bits at a time and each block of plaintext is encrypted using the same key. The term Codebook is used because, for a given key, there is a unique ciphertext for every b-bit block of plaintext.

Disadv: ① ECB mode may not be secure for lengthy messages because appln → short data → Storage in DB the same b-bit block of plaintext appears more than once produces the same ciphertext.

② Block independency creates opportunities to exchange ciphertext blocks. knowing that some block conveys some specific info, interpretation can be made

2. Cipher Block Chaining Mode:



Encryption Decryption

The input to the encryption algorithm is the XOR of current plain block & preceding cipher text block; the same key is used for each

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

For the initial block, Initialization vector is (IV) used which is predetermined by sender & receiver

$$D(K, C_j) = D(K, E(K, [C_{j-1} \oplus P_j]))$$

$$= C_{j-1} \oplus P_j$$

$$C_{j-1} \oplus D(K, C_j) = C_{j-1} \oplus C_{j-1} \oplus P_j$$

$$= P_j$$

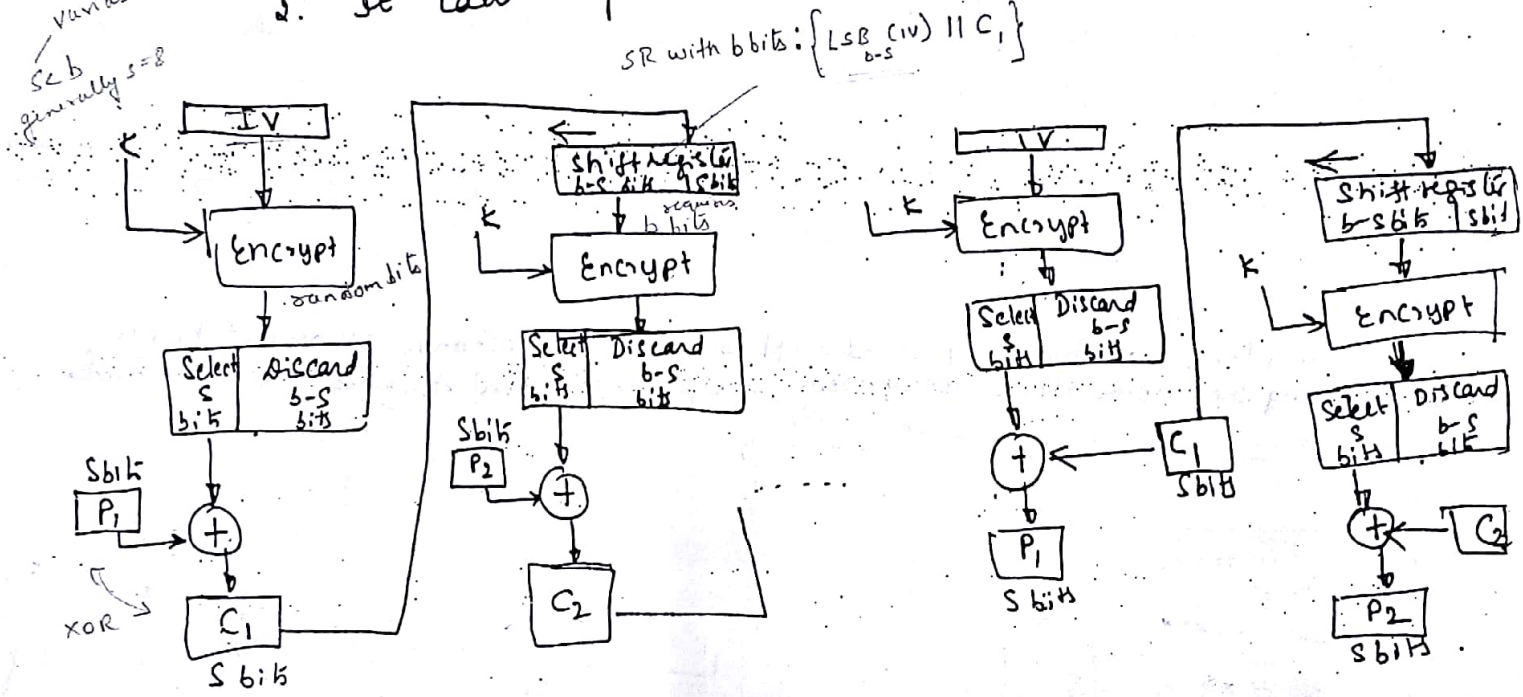
To produce the first block of ciphertext an (IV) initialization vector is XORed with the first block of plaintext.

The IV must be known to both sender & receiver. On decryption, the IV is xored with the output of the encryp algorithm to recover the first block of plaintext.

3. Cipher Feedback Mode:

Using this mode any block cipher is possibly converted into a stream cipher.

Adv: 1. It eliminates the need of padding a message
2. It can operate in real time.



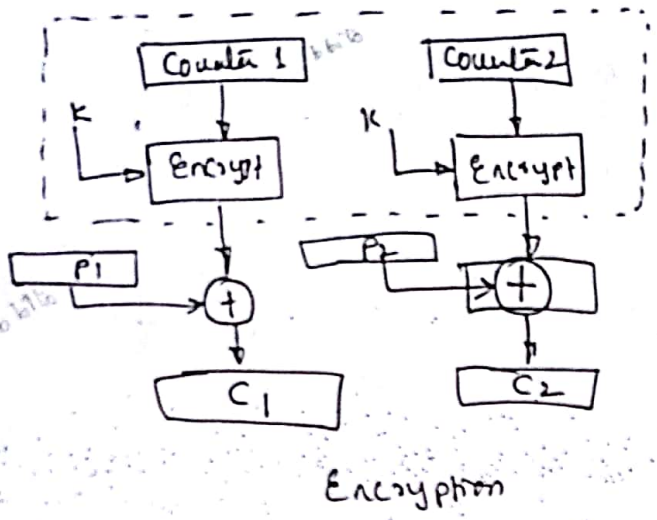
Common value of $s=8$.
The input to the encryption function is a b-bit shift register that is initially set to some (IV) Initialisation vector. The left most (most significant) S bits of the output of encryption function are X-ORed with the first unit of plaintext P_1 to produce the first unit of ciphertext C_1. The contents of shift register are shifted left by S bits & C_1 is placed in right most (Least significant) S bits of S

For decryption, the received ciphertext unit is X-ORed with the output of the encryption function to produce the plaintext unit.

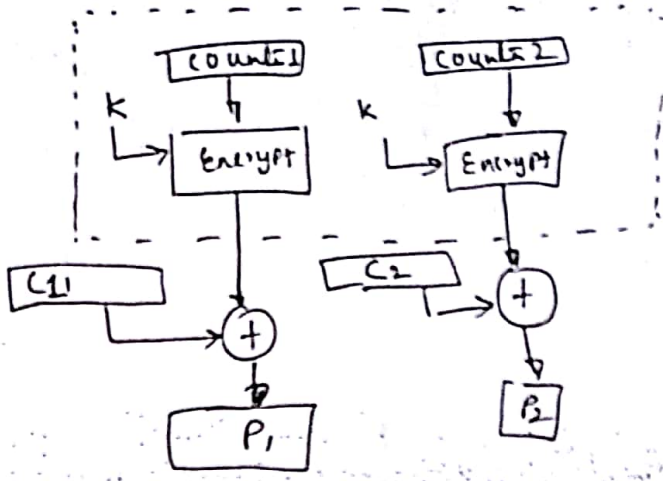
$$C_1 = P_1 \oplus S_s[E(k, IV)]$$
$$P_1 = C_1 \oplus S_s[E(k, IV)]$$

4. Counter Mode:

It was proposed early on ([DIFF79]). but interest is increased wi applications of ATM (asynchronous transfer mode) n/w security & IP



Encryption



Decryption.

A counter equal to the plaintext block size is used. Its value must be different for each plaintext block that is encry For encryption, the counter is encrypted and then XORed wi the plaintext block to produce the cipher text block. There is no chaining.

For decryption, the same sequence of counter values is used, with each encrypted counter XORed with a cipher text block recover the corresponding plaintext block

Adv: H/w & s/w Efficiency, Preprocessing, Random Access, Provable Security & Simplicity

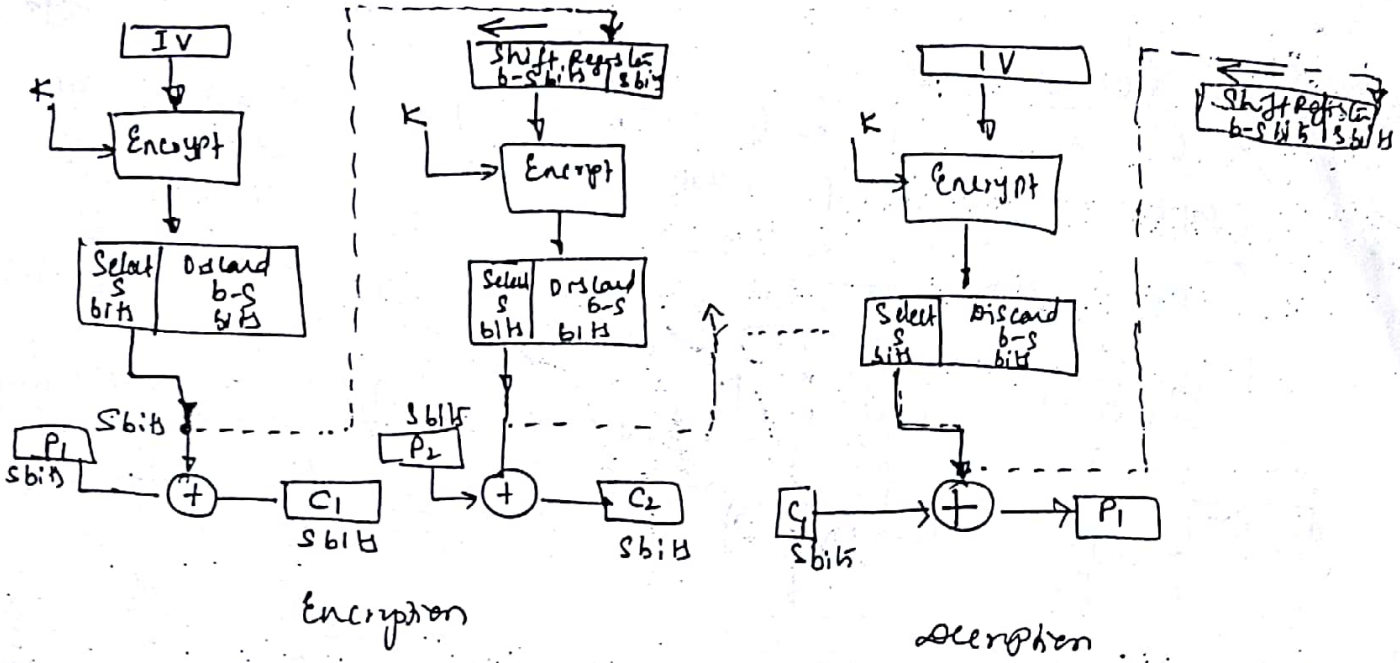
- → no feedback
- → dependency is from built in counter
- → suffers ill propagation
- → counter values must be secure initialized & incremented

used in ATM n/w and IPSec

5. Output Feedback (OFB) Mode

It is similar to CFB mode but each bit in the ciphertext independent of the previous bit or bit. This avoids error propagation.

$$C_i = P_i \oplus \text{shiftleft}_s\left(E_K(\text{shiftleft}_s(S_{i-1}) \,|\, s)\right)$$



Modern block ciphers → DES employs 64 bits, AES employs 128 bits.

Modes of op^n have been devised to encipher text of any size employing either DES or AES.

Block cipher to Stream cipher

needed ∵ blocks required padding (integral no of block

can process in real time as the data enter text (bit oriented stream cipher)

Avalanche effect : The desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext.

In particular a change in one bit of plaintext or one bit of the key should produce a change in (atleast half of) many bits of cipher text. This effect is known as avalanche effect.

OFB