Cryptography and Network Security

Unit-1

Introduction.

The OSI Security Architecture.

OSI security architecture is a framework that provides a systematic way of defining the requirements for security and characterizing the approaches to satisfying those requirements.

To assess effectively the security needs of an organization and to evaluate and choose various security products & policies, the manager is responsible for security needs such as systematic way of defining the requirements for security & characterizing the approaches to satisfying those requirements.

OSI security architecture focuses on security attacks, mechanisms & services.

→ Security attacks

Are classified either as passive attacks, which include unauthorized reading of message or file. Active attacks, such as modification of message or files. "Any action that compromises the security of information owned by an organization".

→ Security mechanisms

Is any process that is designed to detect, prevent or recover from a security attack.

Ex: Encryption algorithms, digital signatures & authentication protocols.

→ Security Services

A process that includes authentication, access control, data confidentiality, data integrity, Non-repudiation & availability. "A processing or communication service that enhances the security of the data processing systems."

Threat and Attack.

→ Threat: A potential for violation of security. A potential cause of an unwanted incident, which may result in harm to a system or organization.

Different types of computer security threats are Trojan, Spyware, Viruses, worms etc.

→ Attack: An attempt to destroy, expose, alter, steal or gain unauthorized access to make unauthorized use of an asset.

Ex: password cracks, Brute force, Denial-of-service.

OSI security architecture focused on

* Security attacks: 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 communication service that enhances the security of data processing systems & the information transfers of an organization.

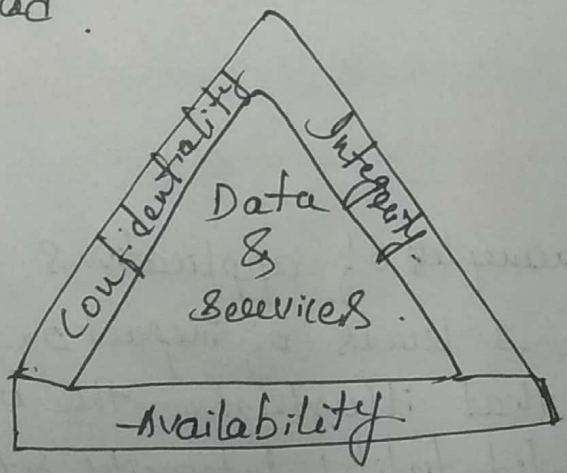
Definition of Computer Security.

Computer Security, also known as cyber Security, is the protection of information systems from theft or damage to the H/W & S/W.

Computer Security also introduces 3 key objectives that are the heart of computer Security.

→ confidentiality.
→ Integrity.
→ Availability.

The above 3 concepts are referred as "CIA triad".



Confidentiality → Data confidentiality
→ privacy.

preserving unauthorized restrictions on information access & disclosure, includes protection of personal privacy & proprietary information.

A loss of confidentiality is the unauthorized disclosure of information.

→ Integrity ← Data integrity
→ System integrity.

Assures information & programs are changed only in a specified & authorized manner.

A loss of integrity is the unauthorized modification of information.

→ Availability.

Ensures timely & reliable access to & use of information. System works promptly & service is not denied authorized user.

A loss of availability is the disruption of access to or use of information.

Additional concepts

→ Authenticity
→ Accountability.

We now discuss some examples of applications. For these examples we use 3 levels of impact on organizations or individuals that ill create the breach of security (i.e. loss of confidentiality, Integrity & Availability).

→ Low : limited adverse effect.
→ Moderate : Serious adverse effect.
→ High : Severe adverse effect.

confidentiality

Student grade information → Moderate confidentiality rating

Directory information → low confidentiality rating.

Integrity

Hospital patient's allergic information → High Integrity rating.

Anonymous online poll → low integrity rating.

Availability.

Systems that provides authentication services for critical systems, applications & devices → High level of availability

public website for a university → Moderate level of availability.

online telephone directory → low availability requirement.

Security attacks

classification of security attacks are

- passive attacks.
- Active attacks.

Passive attacks.

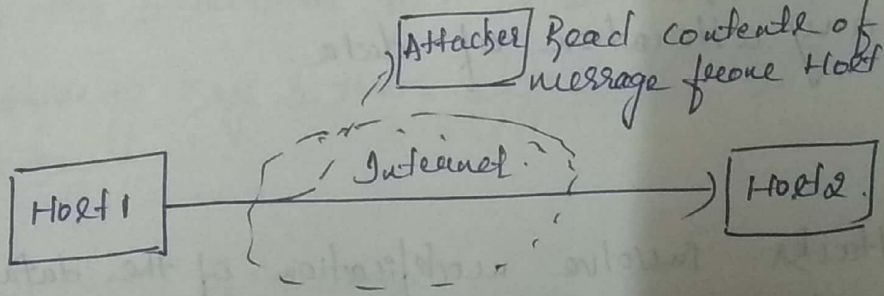
Passive attacks are in the nature of eavesdropping on or monitoring of transmissions.

The goal of the opponent is to obtain information that is being transmitted.

2 types of passive attacks are.

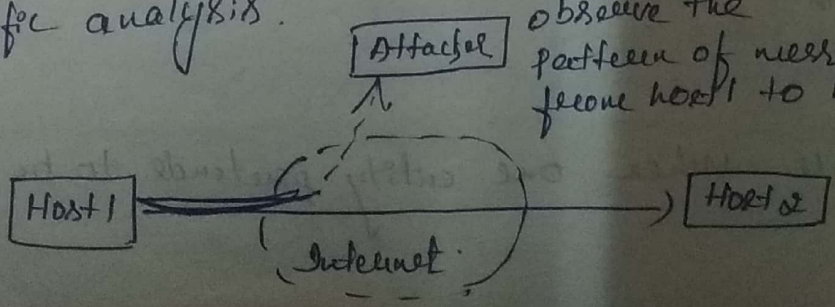
* Release of message content (snooping)
* Traffic Analysis.

* Release of message content.



A telephone conversation, an electronic mail message & a transferred file may contain sensitive information. we would like to prevent an opponent from learning the content of these transmission. Snooping can be prevented using encipherment techniques.

* Traffic analysis.



Traffic analysis is subtler. Suppose that we had a way of masking the contents of messages or other information traffic so that opponents, even if they captured the message, could not extract the information from the message. The opponent could determine the location & identity of communication hosts & could observe the frequency & length of the message being exchanged. This is useful in identifying the nature of communication that was taking place.

The common technique for masking contents is encryption. Though we had this protection in place, an opponent might still be able to observe the pattern of these messages.

Passive attacks are difficult to detect, because they do not involve any alteration of data.

Active attacks.

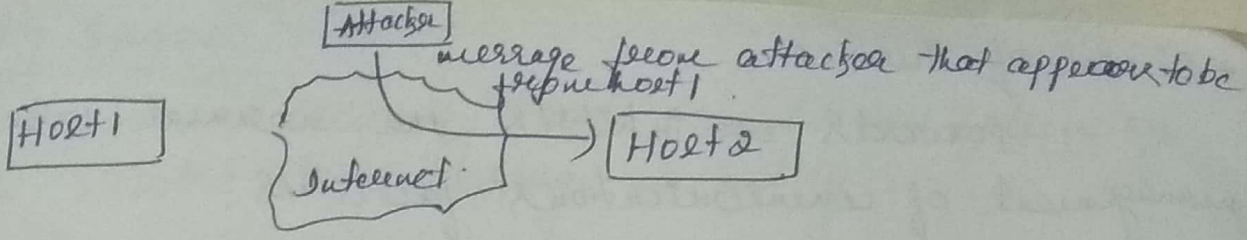
Active attacks involve modification of the data or creation of fake stream.

It divided into 4 categories

* Masquerade.
* Replay.
* Modification of message
* Denial of service.

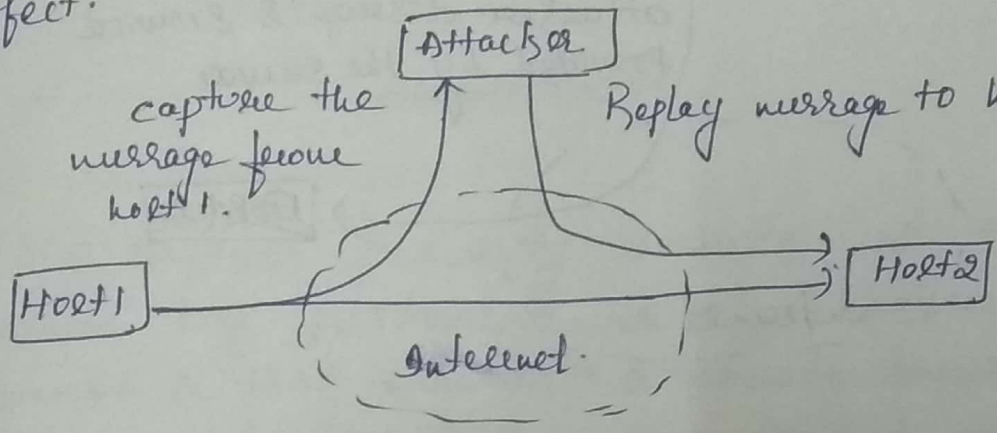
* Masquerade.

Takes place when one entity pretends to be a different entity.



* Replay

Involves the passive capture of a data unit & its subsequent retransmission to produce an unauthorized effect.

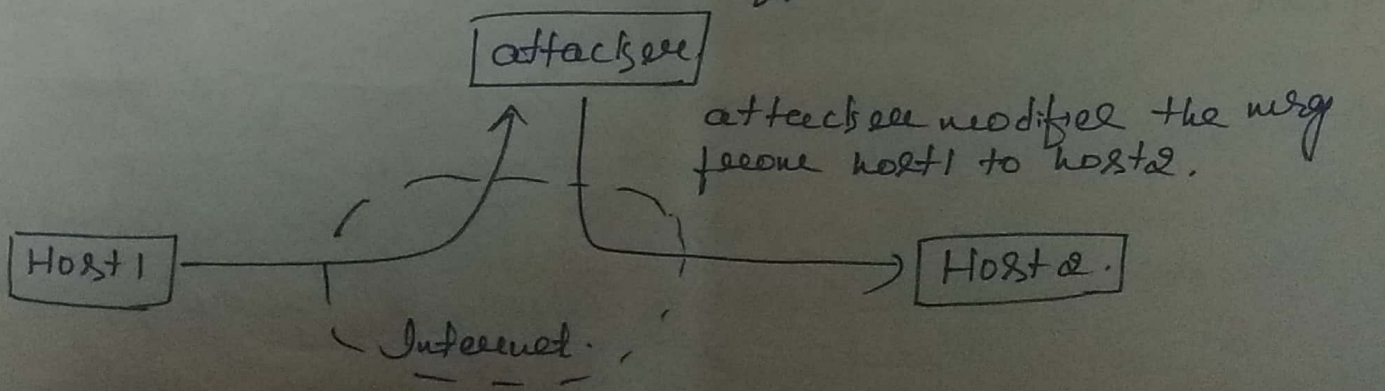


In this case, attacker spies the conversation blw the sender & receiver and takes authenticated information.

Ex:- sharing key & then contact to the receiver with that key.

* Modification of messages.

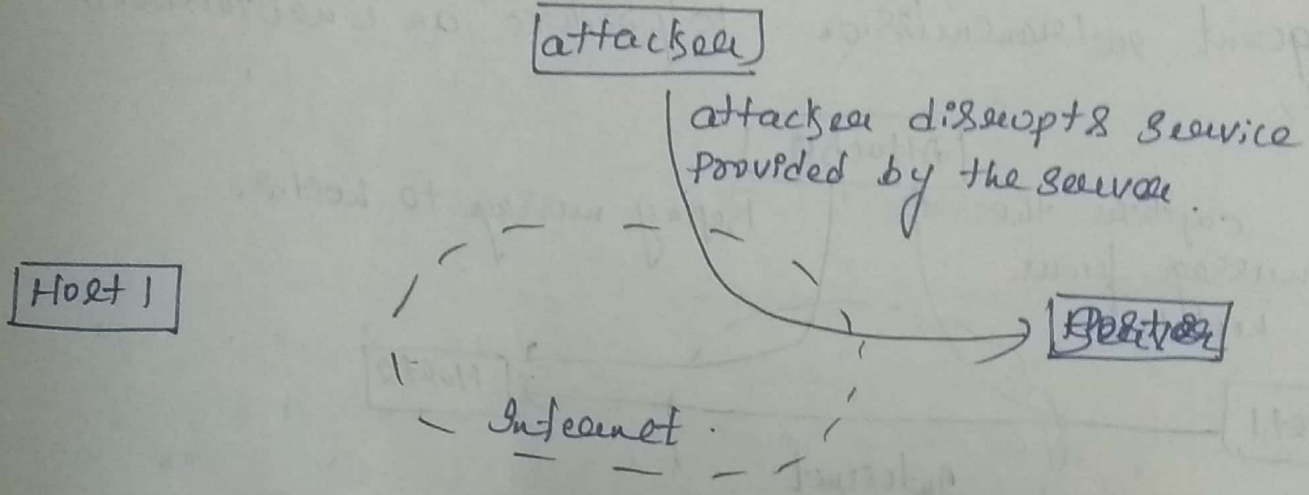
Some portion of a legitimate message is altered, or that messages are delayed or reordered to produce an unauthorized effect.



* Denial of Service.

prevents or inhibits the normal use or management of communications facilities.

Disruption of an entire network, either by disabling the network or by overloading it with messages so as to degrade performance.

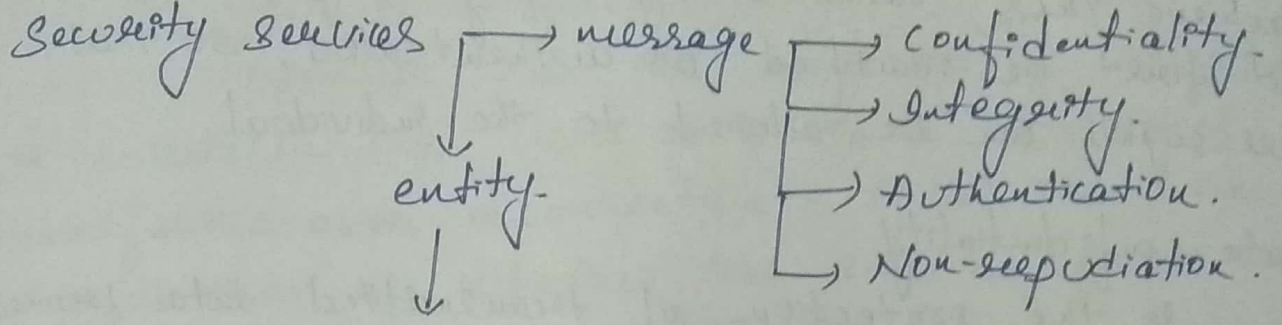


Distinguish b/w active & passive attacks.

Active attacks	Passive attacks
→ Is an attempt to change data or alter the functioning of system.	→ Is an attempt to obtain or make use of information.
→ Results in damage of systems, data, infrastructure or facilities → They may also result in loss of data.	→ Do not alter a system but are intended to gather data or execute transactions.

Security Services.

Network security can provide the following services related to a message or entity.



X.800 defines Security service as service that is provided by protocol layer of communicating open systems & that ensures adequate security of the systems or data transfer.

It divide these services into 5 categories.

(i) Authentication.

This service is concerned with assuring that a communication is authentic.

& Specific authentication services

* peer entity authentication

used in association with logical connection to provide confidence in the identity of the entities connected.

* Data origin authentication.

In a connectionless transfer, it provides the protection against source of data unit. It doesn't provide protection against duplicaton or modification of data units.

(ii) Access control.

It the ability to limit & control the access to host systems & applications via communications links. To achieve this, each entity trying to gain access must first be identified or authenticated, so that access rights can be tailored to the individual.

(iii) Data confidentiality

It the protection of transmitted data from passive attacks.

* connection confidentiality.
The protection of all user data on a connection.

* connectionless confidentiality.
The protection of all user data in a single data block.

* Selective field confidentiality
The confidentiality of selected fields within the user data on a connection or in a single data block.

* Traffic flow confidentiality
The protection of the information that might be derived from observation of traffic flows.

(iv) Data integrity.

The assurance that data received are exactly as sent by an authorized entity. i.e. Data contains no modification, insertion, deletion or replay.

* connection integrity with recovery [Addresses both modification & denial of service]
provided for the integrity of all user data on a connection & detects any modification, insertion, deletion or replay of any data within an entire

data sequence, with recovery attempted.

* connection integrity without recovery
provides only detection without recovery.

* Selective-field connection integrity.
provides for the integrity of selected fields within the user data of a data block transferred over a connection & takes the forme of determination of whether the selected fields have been modified, inserted, deleted or replayed.

* connectionless integrity
provides for the integrity of a single connecti-onless data block & may take the forme of detection of data modification. Additionally, limited forms of replay detection may be provided.

* Selective-field connectionless integrity
Provides for the integrity of selected fields within a single connectionless data block. Takes the forme of determination of whether the selected fields have been modified.

(v) Non-repudiation.
Prevents either Sender or receiver from denying a transmitted message.

Non-repudiation, Origin.
proof that message was sent by the specified party.

Non-repudiation, destination.
proof that message was received by the specified party.

Security mechanisms.

List of security mechanisms defined in X.800
There mechanisms are divided into those that are implemented in specific protocal layers. (Application layer)
Those that are not specific to any particular protocol layer or security service.

→ Specific Security mechanism.

Incorporated into the appropriate protocol layer in order to provide some of the OSI Security Services.

* Encipherment → hiding or covering data, can provide a confidentiality.

The use of mathematical algorithms to transform data into a form that is not readily intelligible.

The transformation & subsequent recovery of the data depend on an algorithm & also depend on some or more keys.

* Digital Signature.

Is a type of electronic signature that encrypts documents with digital codes that are difficult to duplicate.

Used to authenticate the identity of the Sender of message or the signer of document.

Possibly to ensure that the original content of message or document that has been sent is unchanged.

*Access control.

It an approach to securing data by encryp-ting it with a key, so that only users which have correct key are able to decrypt the data.

A variety of mechanisms that enforce access rights to resources. such as → Role based. → Role based. → Lattice-based.

Mandatory Access control

* Data Integrity.

A variety of mechanisms are used to assure the integrity of data. Some of the mechanisms are Mirroring, checkscanning.

In all the above mentioned techniques, maintain some redundant information about the data & ensure integrity by recomputing the redundant data from the actual data & comparing it with the stored redundant information.

*Authentication exchange

A mechanism intended to ensure the identity of an entity by means of information exchange.

* Traffic padding

Inserting some junk data into the data traffic to thwart the adversary's attempt to use the traffic analysis.

* Routing control.

Selecting & continuously changing different available routes b/w sender & receiver to prevent the opponent from eavesdropping on a particular route.

* Notarization

Selecting a 3rd trusted party to control the communication b/w 2 entities.

The receiver can involve a trusted 3rd party to store the sender request in order to prevent the sender from later denying that she had made a request.

Pervasive Security mechanism.

These mechanisms are not specific to any particular OSI Security Service.

* Trusted functionality.

Any functionality that directly provides access to security mechanism should be trustworthy.

* Security labels.

Systems resources may have security labels associated with them.

Security label is one-to-eight byte, installation-defined character string.

It comes in all shapes & sizes.

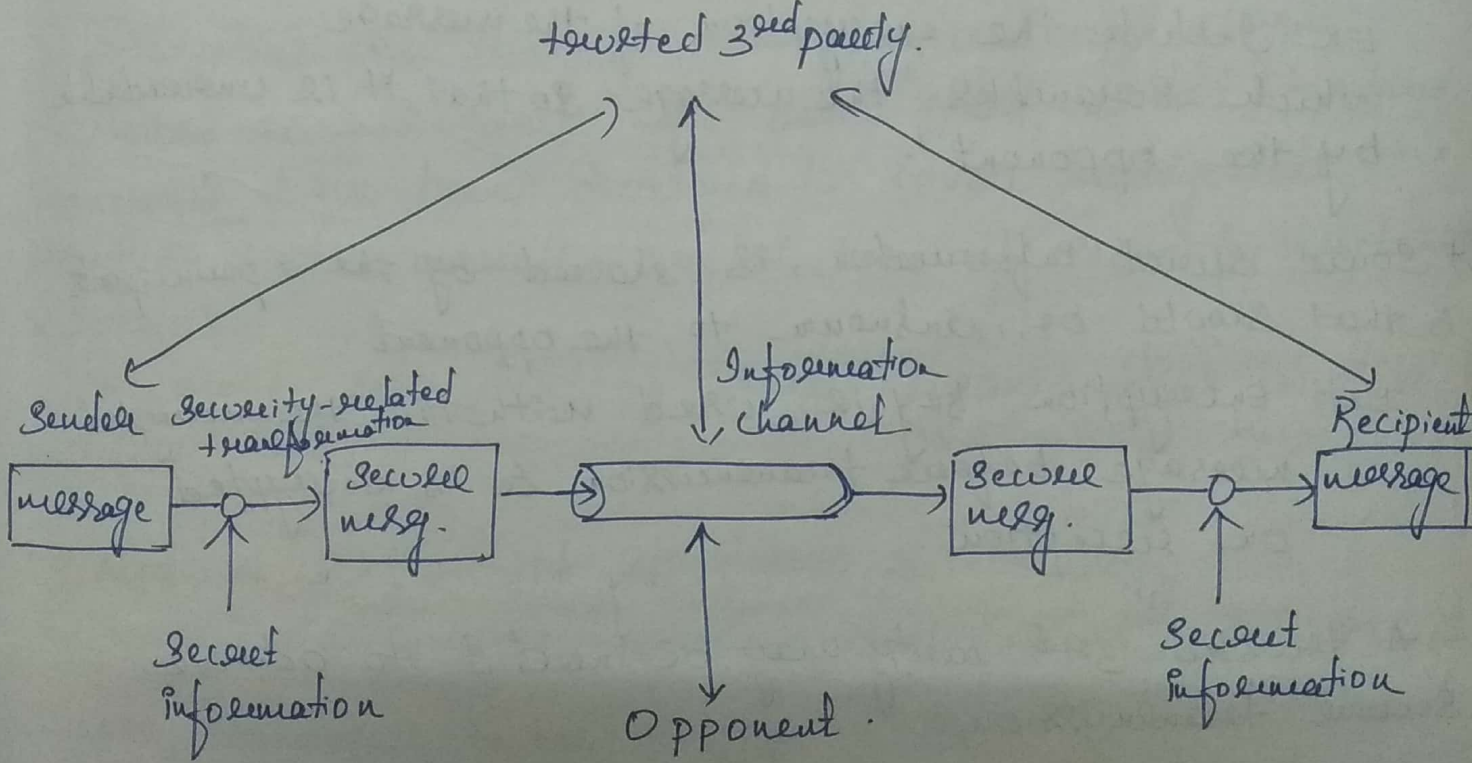
* Event detection
Detection of security related events.

* Security audit trail
Data collected & potentially used to facilitate the security audit.

* Security Recovery
Deals with requests from mechanisms such as event handling & management functions & takes recovery actions as the result of applying set of rules.

A model for networks security

The below diagram illustrates the model for networks security.



→ A message is to be transferred from one party to another across some sort of internet service.
→ The 2 parties who are principals in this transaction must cooperate for the exchange to take place.
→ A logical information channel is established by defining a route through the internet from source to destination.
→ Security aspects come into play when it is necessary to protect the information transmission from an opponent who may present a threat to authenticity, confidentiality & so on.
→ Techniques for providing security have 2 components

* A security related transformation on the information to be sent.

Ex: Include the encryption of the message which scrambles the message so that it is unreadable by the opponent.

* Some secret information is shared by the 2 principals & that should be unknown to the opponent.

Ex: Encryption key is used with the the encrypted message before transmission & is decrypted on reception.

→ A trusted 3rd party may be needed to achieve secure transmission.

Ex: 3rd party is responsible for distributing the secret information among 2 principals while keeping that information away from an opponent.

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

(i) Design an algorithm for performing security-related transformation. The algorithm should be in such way that an opponent should not defeat its purpose.

(ii) Generate a secret information that is to be used with algorithm.

(iii) Develop a methods for distribution & sharing of secret information.

(iv) Specify a protocol to be used by a principals that makes use of security algorithm & secret information to achieve a particular security service.

Standards.

Many of the security techniques and applications described in this course have been specified as standards. Standards have been developed to cover management practices & the overall architecture of security mechanisms & services.

The most important of these organizations are as follows.

→ National Institute of Standards & Technology

U.S. Federal agency deals with measurement science, standards & technology related to U.S.

→ Internet society: ISOC is a professional membership society with worldwide organization & individual membership.

→ ITU-T: International Telecommunication Union is an international organization within the United Nation System in which governments & the private sector coordinate global telecom networks & services.

cryptography.

Is about constructing & analyzing protocols that prevent 3rd parties or public from reading private messages.

Is the practice & study of technique for securing communication & data in the presence of adversaries.

original message is known as plaintext.
coded message is known as ciphertext.
The process of converting from plaintext to ciphertext is known "encryption".
The process of restoring plaintext from ciphertext is known as "decryption".

Symmetric Encryption principles.

Symmetric encryption is also referred as conventional encryption, Secret key or single key encryption.

Symmetric encryption scheme has 5 ingredients.

→ plaintext : This is the original message or data that is fed into the algorithm as i/p.

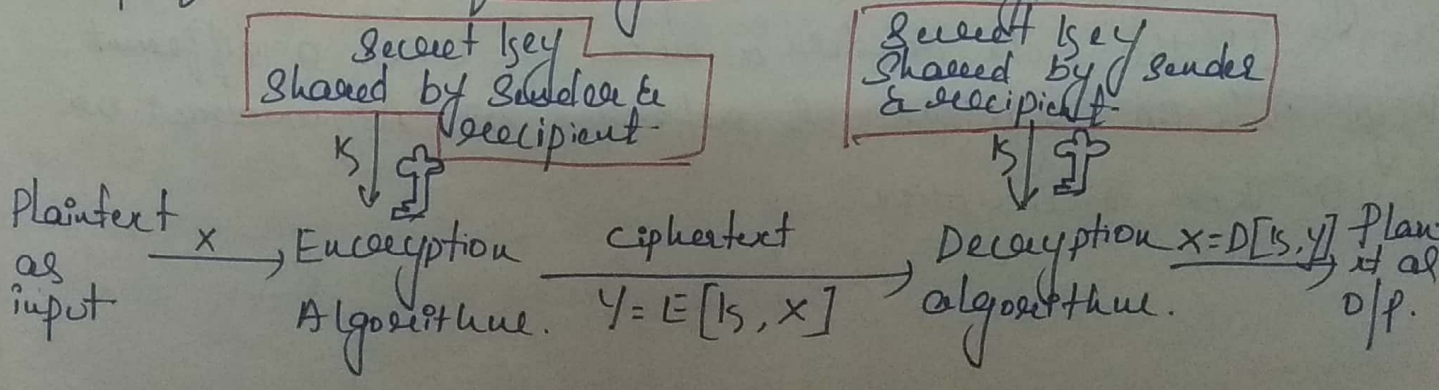
→ Encryption algorithm : performs various substitution & transformations on the plaintext.

→ Secret key : It is also i/p to the algorithm. The exact substitutions & transformations performed by the algorithm depend on the key.

→ Ciphertext : This is the scrambled message produced as o/p. It depends on the plaintext & secret key. For a given message, a different keys will produce a different ciphertexts.

→ Decryption algorithm : This is essentially the encryption algorithm runs in reverse. It takes the ciphertext & the same secret key & produces the original plaintext.

Simplified model for Symmetric Encryption.



There are 2 basic requirements for secure use of symmetric encryption.

→ Need a strong encryption algorithm.

→ Sender & receiver must have obtained copies of secret key in a secure fashion & must keep the key secure.

Cryptographic systems are generally classified along 3 independent dimensions.

(i) The type of operations used for transforming plaintext to ciphertext.

Encryption algorithms are based on 2 general principles (i) Substitution → in which each element in the plaintext is mapped to another element.
(ii) Transposition → in which elements in the plaintext are rearranged.

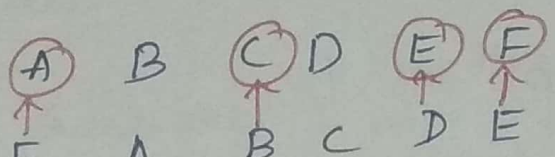
(ii) The no of keys used.

If both sender & receiver uses same key, then that system is referred as "symmetric" or "conventional encryption".

If the both sender & receiver uses a different keys, then the system is referred as "Asymmetric" or "public key encryption".

(iii) The way in which the plaintext is processed.

A Block cipher processes the i/p one blocks of elements at a time, producing an o/p blocks for each i/p blocks.



Decrypt the following message using the above table

EFBD → ciphertext.
FACE → plaintext.

ciphertext = plaintext >> k
E(k, M) = M >> k.

Block cipher is just a function with a key & plaintext outputs plaintext shifted over by the key.

~~A stream cipher~~

Block ciphers are used everywhere in CS to encrypt your phone, computer & to secure your bank information. Algorithms used for this are AES, DES, & RC6.

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

plaintext digits are combined with a keystream. In this case, each digit of plaintext is encrypted with a corresponding digit of the key stream one at a time, in order to give a digit of ciphertext stream.

(Example of substitution) Ex: Additive Cipher.

Encryption in streame cipher

plaintext : R E V A.

Numerical Value for plaintext : 17 4 21 0

key streame : B D L M.
(OTP)

Numerical : 1 3 11 12
OTP → 21+11 = 32 mod 26
= 06

Numerical ciphertext : 18 7 6 12

Ciphertext : S H G M.

Decryption in streame cipher

ciphertext : S H G M

Numerical : 18 7 6 12.

OTP : B D L M.

Numerical : 1 3 11 12. → 6-11 = 21

Numerical plaintext : 17 4 21 0

26-11 = 15+6 = 21

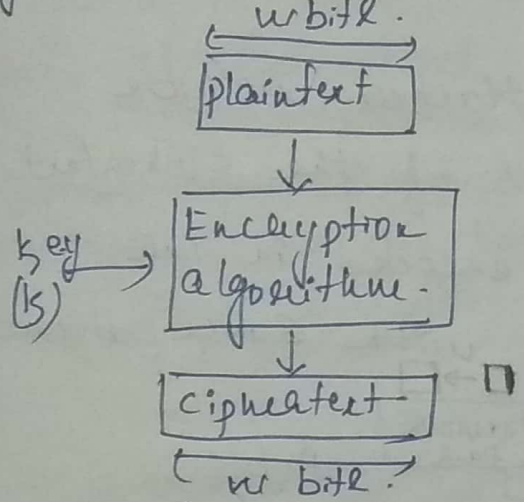
plaintext : R E V A.

Blocks cipher

(i) A blocks of plaintext are encrypted to create a blocks of ciphertext
Ex: Hill cipher.

(ii) Typical blocks sizes are 64 or 128 bits.

(iii) Model of operation used to apply blocks ciphers to larger plaintext



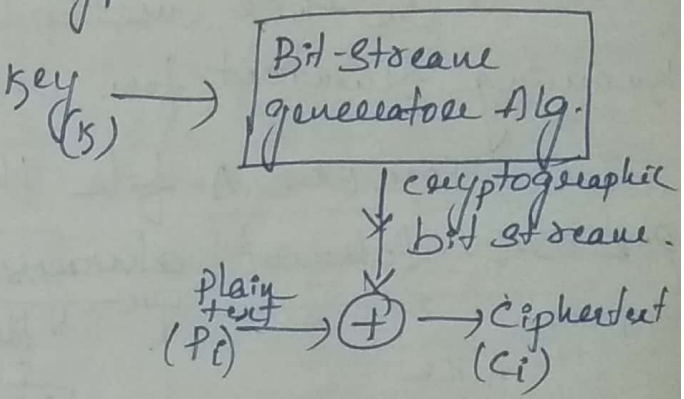
Streame cipher.

(i) One character or one bit of plaintext is encrypted to create a one bit of ciphertext.

(ii) one time pad is an example.

(iii) Typical approaches

* key is used as i/p to bit stream generator algorithm.
* Algorithm generates crypto graphic bit stream used to encrypt plaintext.



Cryptanalysis.

The process of attempting to discover the plaintext or key is known as ~~pto~~ "cryptanalysis".

It is an attacks. It is a process of finding weakness in cryptographic algorithms & using these weaknesses to diciphr the ciphertext without knowing secret key.

Following are the various types of cryptanalytic attacks is based on the amount of information known to cryptanalyst.

→ Ciphertext only attacks:-

In this method, the attacker has access to a set of ciphertext. He doesn't have access to corresponding plaintext.

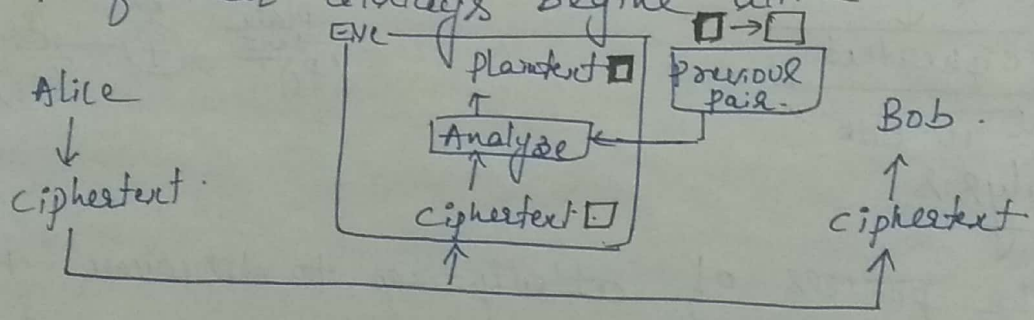
COA is said to be successful when the corresponding plaintext can be determined from a given set of ciphertext.

occasionally, encryption key can also be determined from this attacks.

→ Known plaintext attack.

In this method, the attacker will be knowing plaintext for some parts of the ciphertext.

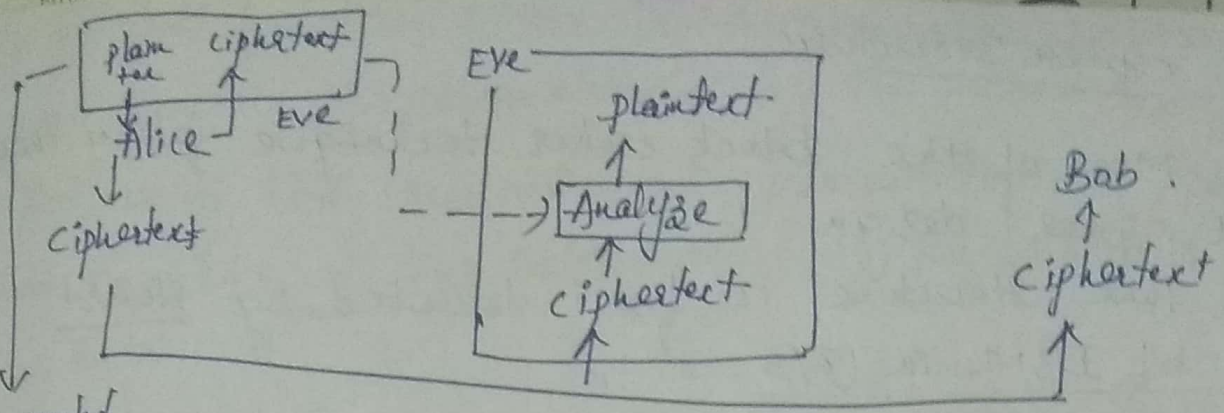
For Ex: A file that is encoded in the Postscript format always begins with same pattern.



Alice has sent a secret message to Bob, but she has later made the contents of the message public. Attacker has kept both ciphertext & plaintext to use them to break the next secret message from alice to Bob, Assuming that alice has'nt changed her key.

→ chosen plaintext attacks.

It is similar to known-plaintext attack, but the plaintext / ciphertext pairs have been chosen by an attacker itself.

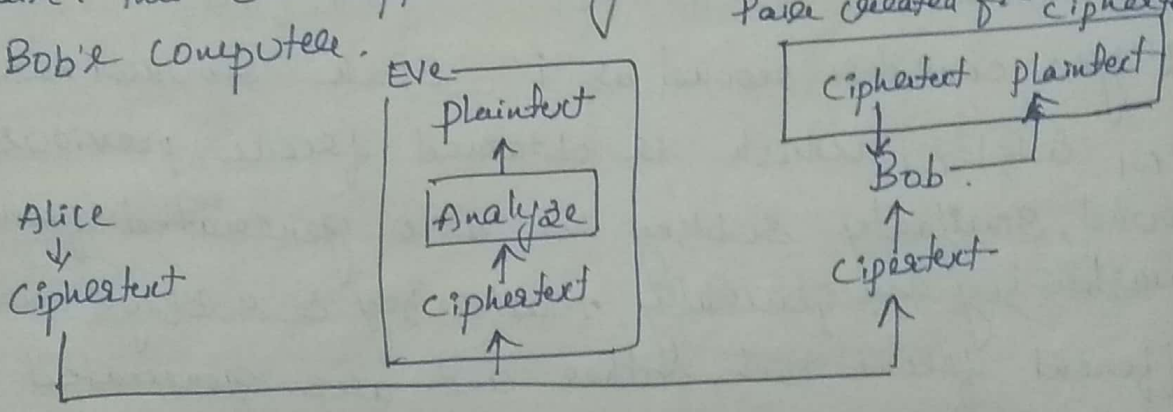


Pair created from chosen plaintext.

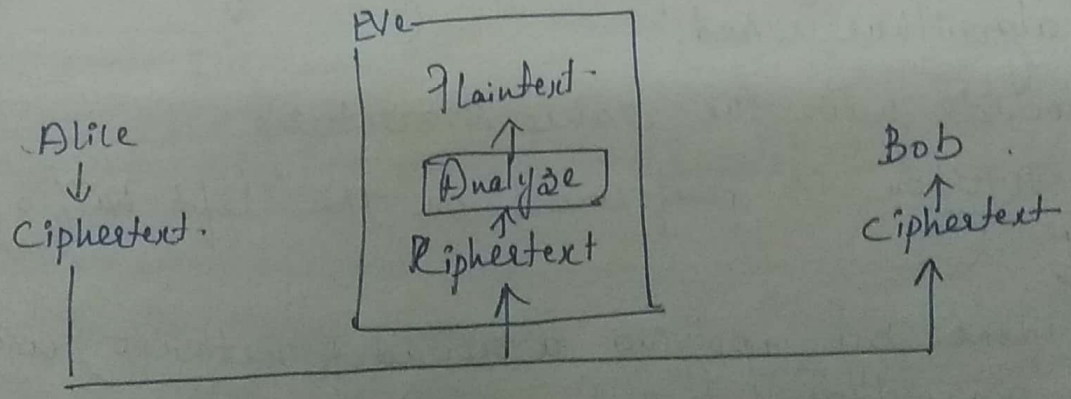
This can happen, only if eve has access to Alice's computer. She can choose some plaintext & intercept the created ciphertext. of course, she doesn't have key because key is embedded in the software used by the sender (here it is Alice). This type of attack is much less likely to happen.

→ chosen ciphertext attacks.

It is similar to chosen plaintext attacks, except that Eve chooses some ciphertext & decrypts it to form a ciphertext/plaintext pair. This can happen only when attacker has access to Bob's computer.



ciphertext only attacks.



Feistel cipher structure

Most of the block cipher technique follow this feistel cipher design.

This structure is first described by Horst Feistel of IBM in 1973.

Design:

→ The i/p to an encryption algorithm are a plaintext block of length n bits & a key K.

→ The plaintext block is divided into 2 halves, say LE_0 & RE_0.

→ The 2 halves of data pass through n rounds of processing and then combine to produce the ciphertext block.

→ If you consider round as 'i', Each round i has i/ps LE_{i-1} & RE_{i-1} which is obtained from previous round, Similarly subkey is also generated from the master key K. Generally, Master key & subkeys are different from each other and are generated by a subkey generation algorithm.

→ Likewise, we can implement any no of rounds based on the algorithm used.

→ All rounds have the same structure.

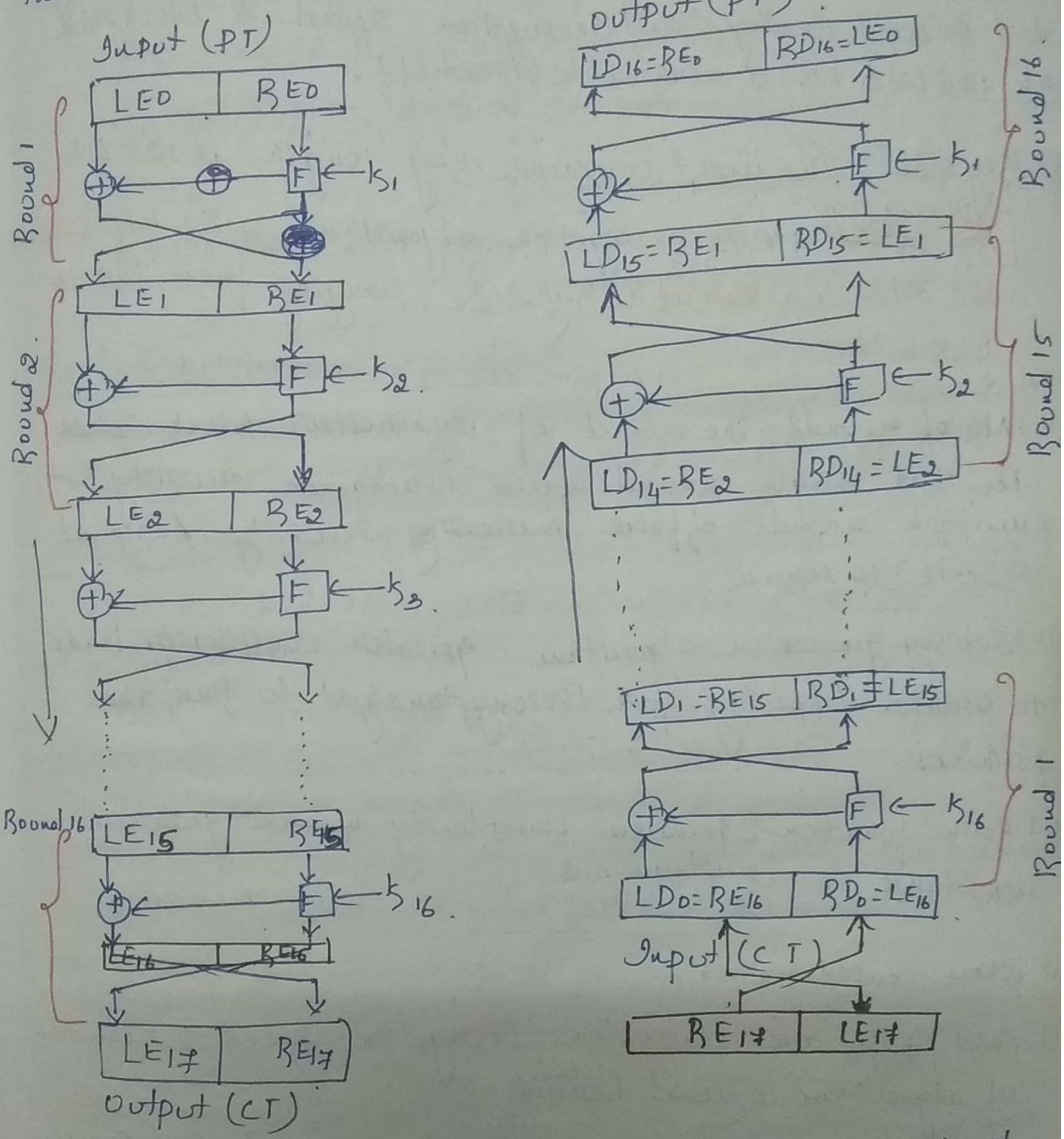
→ A Substitution is performed on the left half of the data.

↓

It is done by applying a round function(F) which may be any logical function depends on the algorithm, to the right half of the data & then taking XOR of the

off of that function & the left of the data. In each round round function is parameterized by the round subkey k_i.

→ Following this substitution, permutation is performed that consists of the interchange of the 2 halves of the data.



The feistel structure is a particular example of the more general structure used by all symmetric block ciphers. In general, symmetric block ciphers consists of a sequence of rounds with each round performing

Substitutions & permutations conditioned by secret key value.

Following are the parameters & design features that are to be considered to design symmetric block cipher

(i) Block size :- Larger block size means greater security but reduced encryption/decryption speed. A block size of 128 bits is a reasonable tradeoff.

(ii) Key size :- The most common key length is 128 bits. [During 1998 ~~The Winner~~ MARS Encryption algorithm, with block size 128 bits & a variable key size, ranging from 128 to 448 bits.]

(iii) No of rounds :- The essence of symmetric block cipher is that single round offers inadequate security but multiple rounds offers increasing security. A typical size is 16 rounds.

(iv) Subkey generation algorithm :- greater complexity leads to greater difficulty for the cryptanalyst to find the plaintext.

(v) Round function :- Greater complexity means greater resistance to cryptanalysis.

& other consideration.

(i) Fast software encryption/Decryption :- Speed of execution of algorithm is main concern.

(ii) Ease of analysis :- Develop an algorithm in such a way that the algorithm shouldn't be vulnerable to any cryptanalysis. Therefore, develop a higher level of assurance as to its strength.

Symmetric Block encryption algorithm.

The most commonly used symmetric encryption algorithms are block ciphers.

Block cipher processes the plaintext i/p in fixed-size blocks & produces a blocks of ciphertext of equal size.

The 3 most important symmetric block ciphers:

(i) The Data Encryption standard.

(ii) Triple DES.

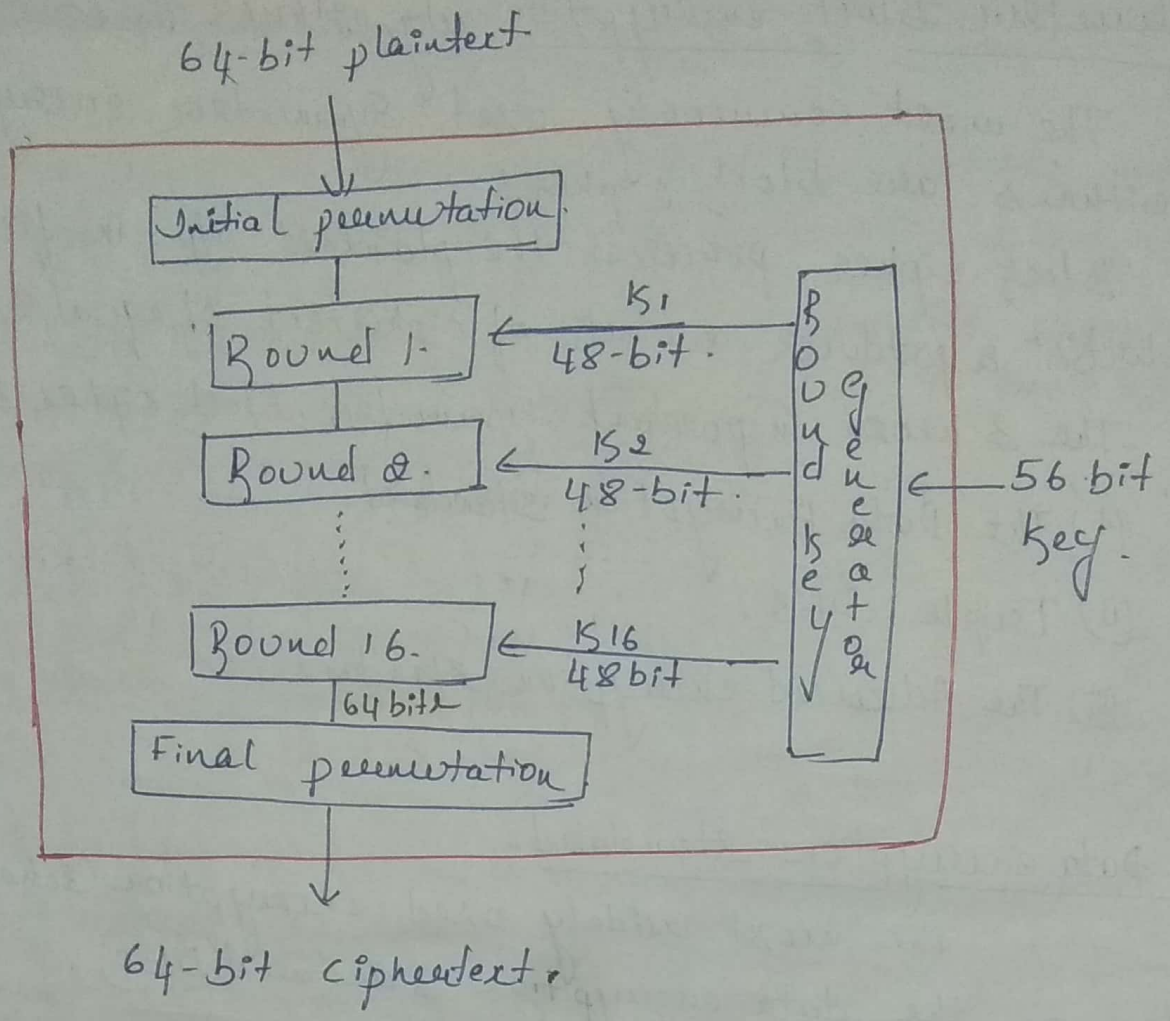
(iii) The Advanced encryption standard.

The Data encryption standard.

The most widely used encryption scheme is based on the data encryption standard (DES).

Description:

* The plaintext is 64 bits in length & the key is 56 bits in length.
* DES structure is a minor variation of Feistel networks.
* 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 structure of DES.



DES encryption.

→ In this case, the plaintext must be 64 bits in length & the key is 56 bits in length.

→ looking at the left-hand side of the figure, we can see that processing of plaintext proceeds in 3 phases.

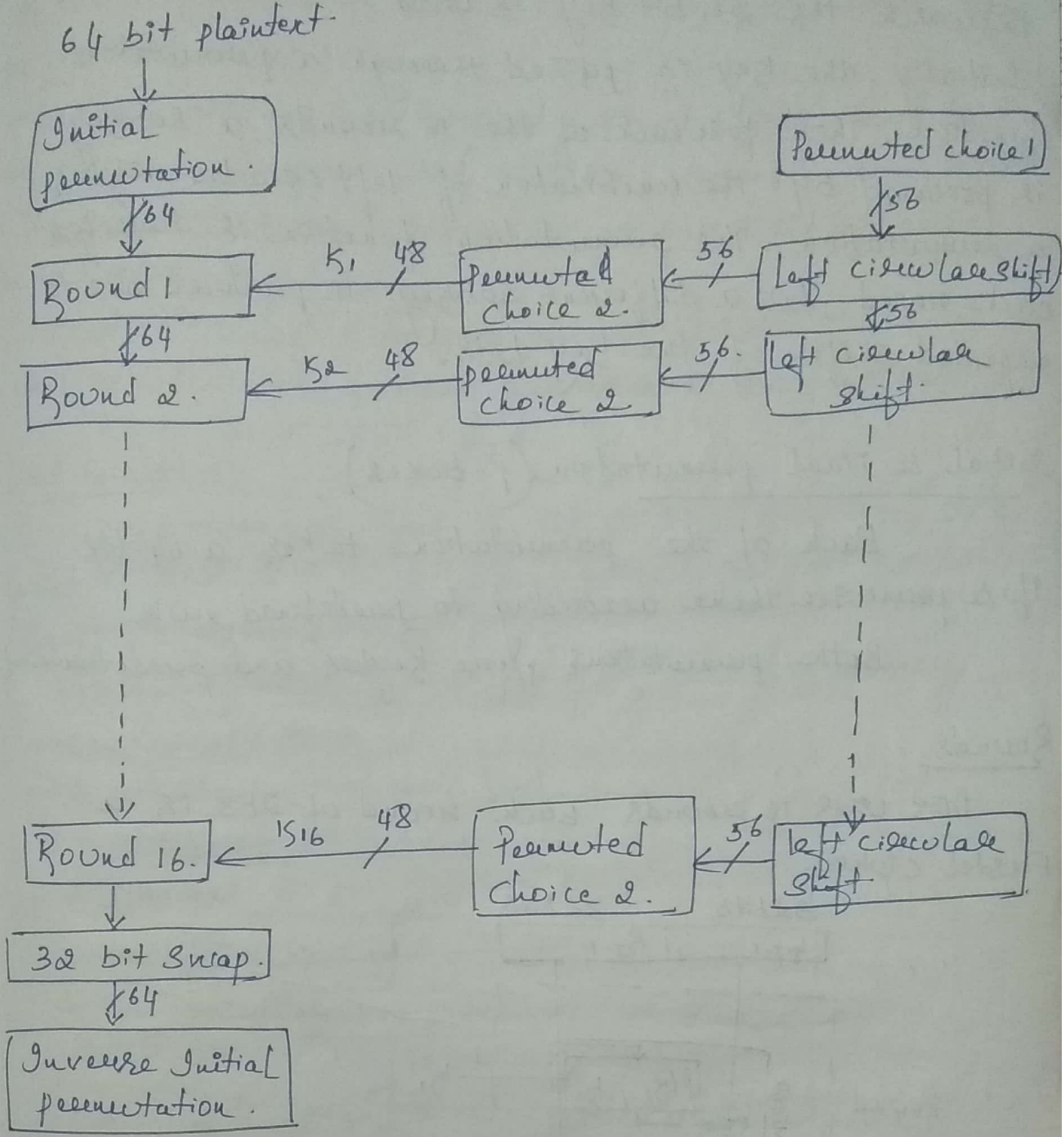
(i) 64 bit plaintext passes, through an Initial permutation, that rearranges the bits to produce the permuted i/p.

(ii) This is followed by a phase consisting of 16 rounds of same function, which involves both permutation & substitution functions.

The o/p of sixteen round consists of 64 bits that are a function of the i/p plaintext & key.

The left & right halves of the o/p are swapped to produce the preoutput.

General Description of DES encryption Algorithm.



(iii) Finally, the preoutput is passed through a permutation (IP^{-1}) i.e. inverse of initial permutation function, to produce the 64-bit ciphertext.

(Final permutation)

→ The right hand portion of the figure shows the way in which the 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 left circular shift & a permutation. The permutation function is same for each round, but a different subkey is produced due to repeated shifts of the key bits.

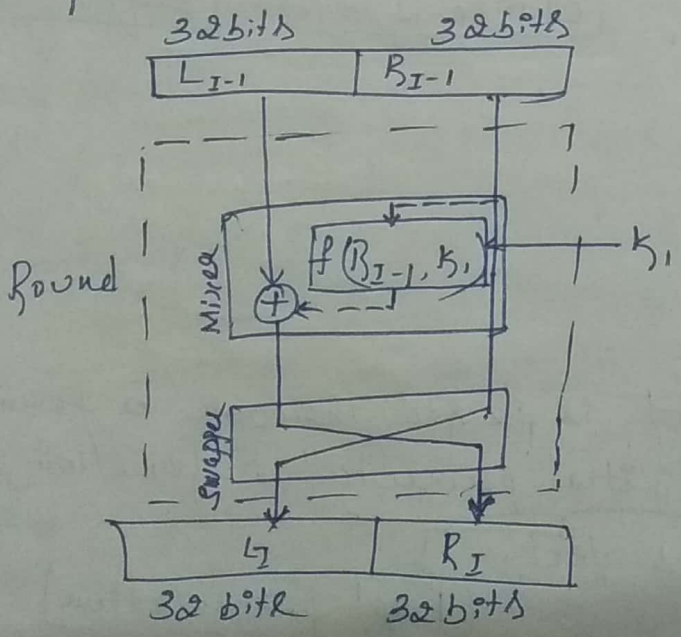
Initial & Final permutation (P-boxes)

Each of the permutation takes a 64-bit i/p & permutes them according to predefined rule.

Both permutations are keyless and predetermined.

Rounds.

DES uses 16 rounds. Each round of DES is a Feistel cipher.



The round takes L_{I-1} & R_{I-1} from the previous round (or Initial permutation box) & creates L_I & R_I which goes to the next round.

We can assume each round has 2 cipher elements say Mixer & Swapper. Each of these elements are invertible. Swapper is obviously invertible, it swaps the left half of the text with right half.

Mixer is invertible because of XOR operation.

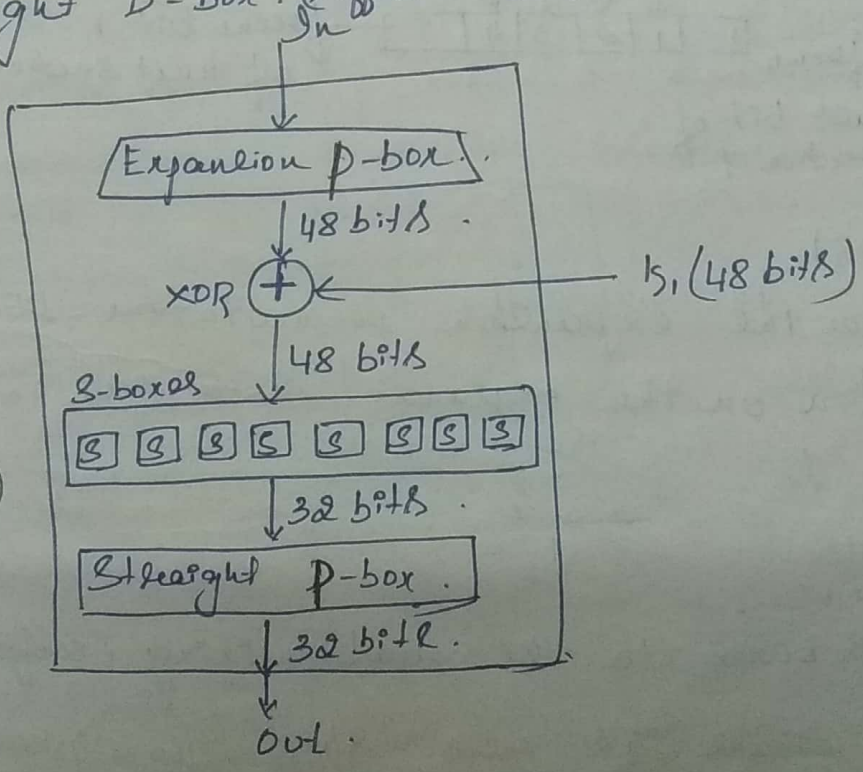
All non-invertible elements are collected in function f.

DES Function

The heart of DES is the DES function. The DES function applies a 48-bit key to the rightmost 32 bits (R_{I-1}) to produce a 32-bit o/p.

This function is made up of 4 sections namely,

→ An expansion P-box.
→ A whitener (that adds key).
→ A group of S-boxes.
→ A straight P-box. (Diffusion Box).



→ Expansion p-box.

Since R_{I-1} is a 32-bit i/p & K_1 is a 48 bit key, we first need to expand R_{I-1} to 48 bits.

R_{I-1} is divided into 8 4-bit sections. Each 4-bit section is then expanded to 6 bits.

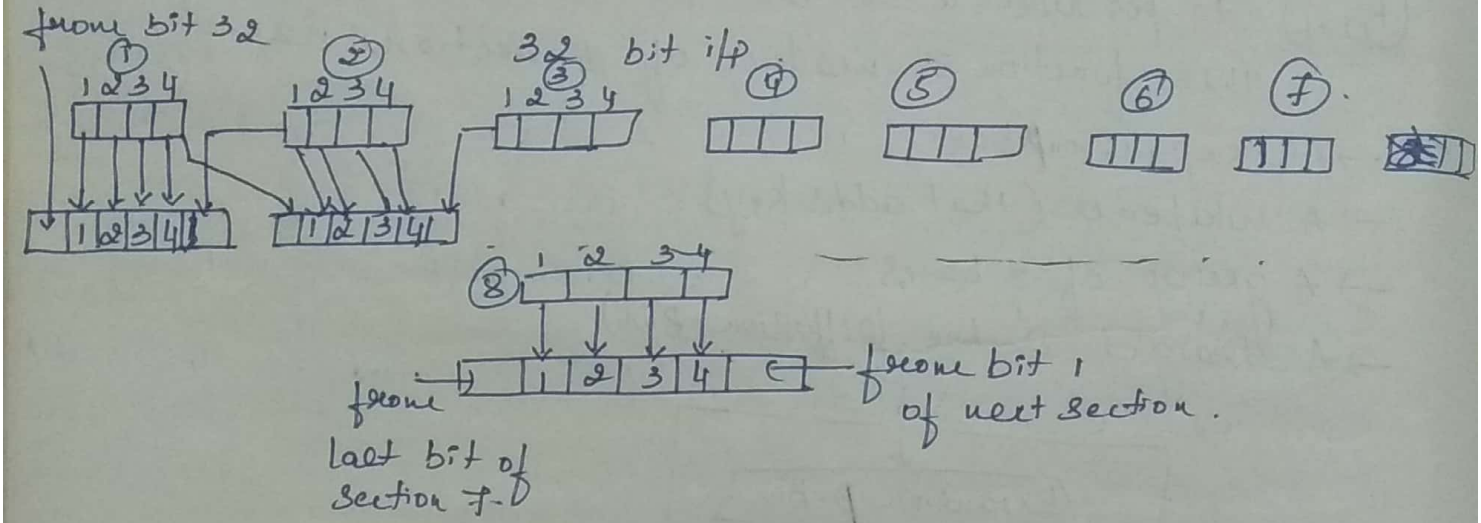
This expansion permutation follows a predetermined rule.

For each section, i/p bits 1, 2, 3 & 4 are copied to o/p bits 2, 3, 4 & 5 respectively.

The o/p bit 1 comes from bit 4 of the previous section.

o/p bit 6 comes from bit 1 of the next section.

If sections 1 & 8 can be considered adjacent sections, the same rule applies to bits 1 & 32.



→ whitening (XOR)

After the expansion permutation. DES uses the XOR operation on the expanded right section & the round key.

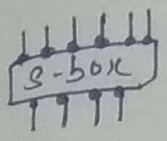
→ S-box.

The S-boxes do the real mixing (confusion).

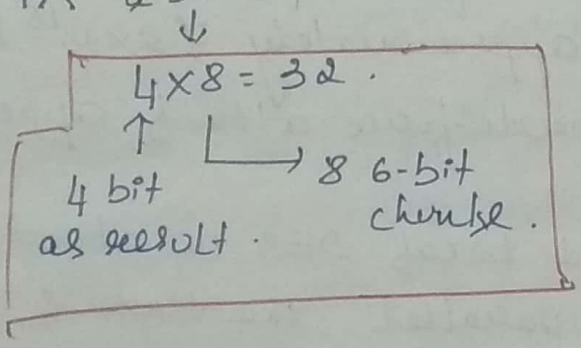
Confusion: Hides the relationship b/w ciphertext & key.

Diffusion: Hides the relationship b/w the ciphertext & plaintext.

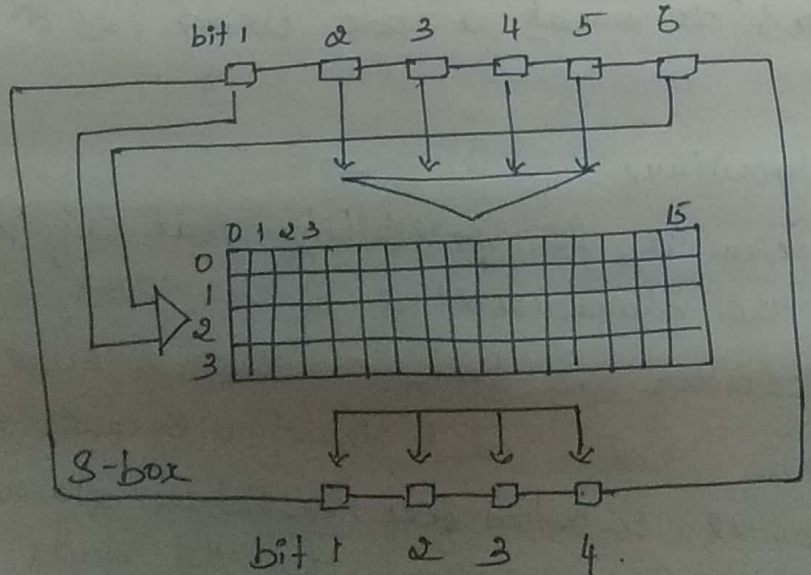
DES uses 8 S-boxes, each with 6 bit i/p & 4 bit o/p.



48 bit data from the 2nd operation is divided into eight 6-bit chunks and each chunk is fed into box. result of each chunk is a 4-bit chunk. when these are combined the result is a 32-bit text.



The substitution in each box follows a pre-determined rule based on a 4-row by 16-column table.
The combination of bits 1 & 6 of the i/p define one of 4 rows.
The combination of bits 2 through 5 defined one of 16 columns



Round Key Generator of DES.

Round key generator creates 16 48-bit keys out of a 56-bit cipher key.

Key is normally given as a 64-bit key in which 8 extra bits are parity bits, which are dropped before the actual key generation process.

* parity drop: The preprocess before key expansion is a compression transposition step that we call parity-bit drop.

It drops the parity bits (bits 8, 16, 24, 32.... 64) from the 64-bit key & permutes the rest of the bits.

The remaining 56-bit value is the actual cipher key which is used to generate round keys.

parity bit drop table is shown in (table 6-12).

* Shift left: After parity bit drop, the key is divided into 2 28-bit parts.

Each part is shifted left (circular shift) one or two bits.

In rounds 1, 2, 9 & 16 shifting is one bit.

In the other rounds it is 2 bits.

The 2 parts are then combined to form a 56-bit part. No. of shifts.

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
1	1	2	2	2	2	2	2	1	2	2	2	2	2	2	1

* compression P-box.

It changes 56-bits to 48 bits, which are used as key for a round.

DES Decryption

DES decryption uses the same algorithm as encryption, except that the application of subkeys are reversed. Additionally, initial & final permutations are reversed.

Strength of DES.

→ The 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. Thus, on the face of it, a brute-force attack appears impractical.

A single pc could break DES in about years, if multiple pcs works in parallel, the time is drastically shortened. And today's supercomputers should be able to find a key in about an hour. keysizes of 128 bits or greater are effectively unbreakable using simple a brute force approach. Even if we managed to speedup the attacking system by a factor of 1 trillion (10^{12}), it would still take 1,00,000 years to break a code using 128 bit key.

→ The nature of DES algorithm.

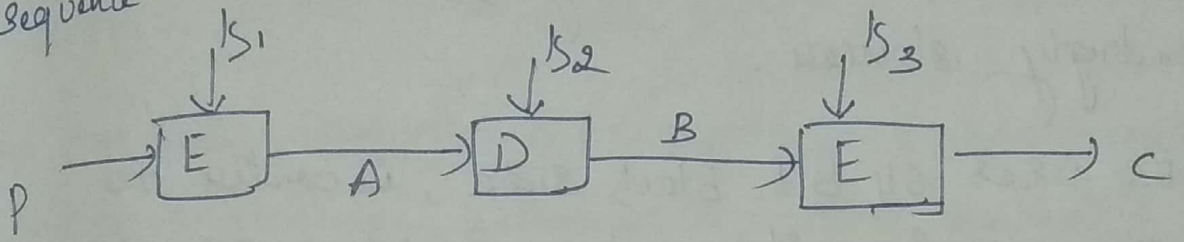
Another concern is the possibility that cryptanalysis is possible by exploiting the characteristics of the DES algorithm. The focus of concern has been on the S-Substitution tables or s-boxes, that are used in each iteration. Because the design criteria for these boxes, & indeed for the entire algorithm were not made public, there is a suspicion that the boxes were constructed in such a way that cryptanalysis is possible for an opponent who knows the weakness in the s-boxes.

~~Advanced Encryption Standard~~

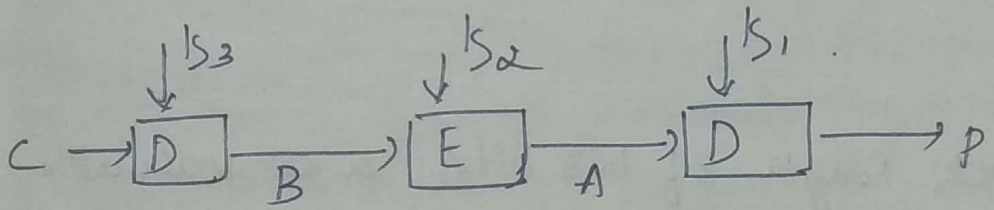
Triple DES.

This was first standardized for use in financial applications in ANSI standard.

Triple DES uses 3 keys & 3 executions of the DES algorithm. The function follows an encrypt-Decrypt-Encrypt sequence.



(i) Encryption.



(ii) Decryption.

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

C → ciphertext, P → plaintext.

E [K, X] → encryption of X using key K.

D [K, y] → Decryption of y using key K.

$$P = D\left(K_3, E\left(K_2, D\left(K_1, P\right)\right)\right)$$

Advanced Encryption standard.

Principal Drawbacks of 3DES is that.

→ Algorithm is relatively sluggish in software. Original DEA was designed for mid 1970s hardware implementation & doesn't produce efficient s/w code.
3 DES which has 3 times as many rounds as DEA. is correspondingly slower.

→ DEA & 3DES uses 64-bit block size, in order to achieve efficiency & security, a larger block size is desirable.

AES algorithm.

* AES uses a block length of 128 bits & a variable key length of 128, 192 or 256 bits.
* The diagram illustrates the overall structure of AES.
→ I/p to the encryption & Decryption algorithm is a single 128-bit block.
→ AES processes the entire data block as a single matrix during each round using substitution & permutation.
→ The key which is provided as I/p is expanded into an array of 44 32-bit words.
4 distinct words (128 bits) serve as a round key for each round.
→ Four different stages are used, one of permutation & Three of substitution.

(i) Substitute bytes: Uses an S-box to perform a byte-by-byte substitution of the block.

(ii) Shift Rows: A simple permutation.

(iii) Mix columns: A substitution that makes use of arithmetic over $GF(2^8)$. GF → Galois Field.

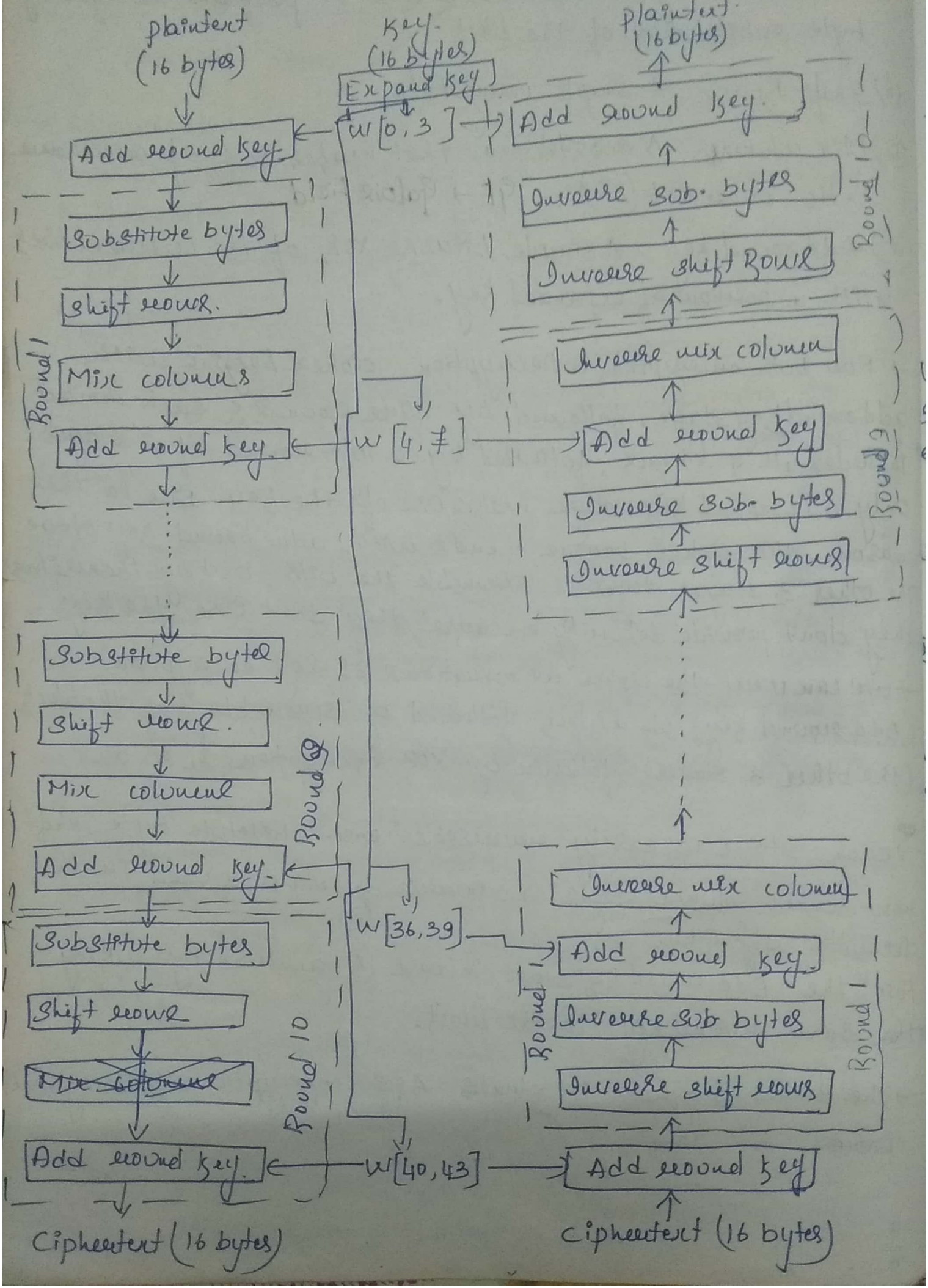
(iv) Add round key: A simple bitwise XOR of the current block with a portion of expanded key.

→ For both encryption & Decryption, cipher begins with addroundkey stage, followed by Nine rounds & each round includes all 4 stages, followed by a 10th round of 3 stages. Only add round key stage makes use of the key. Due to this reason, the cipher begins & ends with add round key stage. The other 3 stages together scramble the bits, but by themselves they don't provide security because they don't use the key.

→ We can view the cipher as operations of XOR encryption (Add round key) of a block, followed by scrambling of the block (the other 3 stages), followed by XOR encryption & so on.

→ Each stage is easily reversible. For Substitute byte, shift row & mix column stages, an inverse function is used in the decryption algorithm.
For the Add round key stage, inverse is achieved by XORing the same round key to the block.

→ The Below diagram illustrates AES encryption & Decryption process.



Advanced encryption Standard.

why AES doesn't follow feistal cipher structure.

→ AES is a Substitution - permutation n/w

→ In feistal cipher, the round function is not necessarily invertible, but in AES, Substitution - permutation rounds are invertible: this is a property of the construction itself.

→ By definition, Feistal cipher uses a series of rounds that split the i/p block into 2 halves, uses one side to permute the other side, then swaps the sides.

→ AES doesn't do this, Each round consists of Subbytes, shiftrows, Mix columns & Add round key steps.

AES Encryption process

→ The i/p to the encryption & decryption algorithm is a single 128-bit block. this block is depicted as 4×4 square matrix of bytes.

→ This block is copied into state array, which is modified at each stage of encryption or decryption.

[state: Refer slide no-12 of AES].

Data units

Bits : 0 or 1, represented as b_0, b_1, b_2.

Byte : Eight bits. $[b_0, b_1, b_2, b_3, b_4, b_5, b_6, b_7]$.

word : 32 bits. $[B_0\ B_1\ B_2\ B_3]$ → 1 byte; $B_0 B_1 B_2 B_3$ → 4 bytes

represented as "w"

Block : can be represented as a row matrix of 16 bytes. (128 bits)

State : can be represented as (4×4) matrices are made of 16 bytes. "s".

plaintext to state.

"AES uses a matrix."

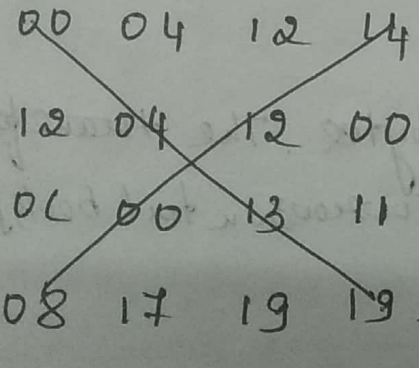
→ Append 2 dummy characters at the end.

AES USES A MATRIX ZZ.

16 | 18
1-2

16 | 23
1-

00 04 12 14 12 04 12 00 0C 00 13 11 08 17 19 19



(State matrix is filled column by column)

$$\begin{bmatrix} 00 & 12 & 0C & 08 \\ 04 & 04 & 00 & 17 \\ 12 & 12 & 13 & 19 \\ 14 & 00 & 11 & 19 \end{bmatrix}$$

SubBytes

AES uses 2 invertible transformations

→ SubBytes
→ Inv SubBytes.

→ SubBytes

The first transformation, SubBytes, is used @ the encryption site.

To substitute byte, we interpret the byte as 2 hexa-decimal digits.

left digit → row right digit → column.

The 2 hexadecimal digits at the junction of the row & column are the new byte.

In SubBytes transformation Transformations is done one byte @ a time.

The contents of each byte is changed, but arrangement of the bytes remains the same.

In this process, each byte is transformed independently. There are 16 distinct byte-to-byte transformations.

→ Inv SubBytes.

It is the inverse of SubBytes. The transformation is done using the table 7.2 [Refer Forouzan text book].

Permutation.

→ Shiftrows. → (Byte exchange transformation)

Another transformation found in a round is shifting. which permutes the bytes.

[In DES it is done by bit level but in AES it is done by byte level].

In encryption the transformation is called "Shiftrows", where as in decryption it is called "Inv shiftrows".

In encryption, shifting is done @ the left. The no of shifts depends on the row. not of the state matrix.

Row 0: No shift.

Row 1: 1-byte shift.

Row 2: 2 byte shift.

Row 3: 3 byte shift to the left.

In decryption, shifting is done @ the right.

Mixing

Mixing transformation changes the contents of each byte by taking 4 bytes at a time & combining them to recreate a 4 new bytes.

To guarantee that each new byte is different the combination process first multiplies each bytes with a different constant & then mixes them.

Mixing can be provided by matrix multiplication.

Column matrix × Square matrix = Column matrix.

Add round key

proceeds one column at a time. Similar to Mix columns.

Add round key adds a round key word with each state column matrix.

Operation in Add round key is matrix addition.

XORing of each column of state matrix with a corresponding key.