CNS

UNIT - I

Cryptographic attacks

→ It is any action that compromises the security of information of an organization (2 types - active, passive attacks)

i) Attacks based on confidentiality -

a) Snooping - This happens at confidentiality. It is mechanism where an unauthorized person interferes/intercepts between two authorized persons and try to steal the information

b) Traffic analysis - Here, the receiver will analyse the complete traffic, so that he can try to understand what type of information is being communicated.

ii) Attacks based on Integrity -

a) Modification - Here, the unauthorized person (or) 3rd person intercepting will try to modify the information being transmitted and uses it for his own benefits.

b) Masquerading - Here unauthorized person acts as if he is one among the sender and receiver and he ready and modify the data

c) Replaying - Here, same message will be sent again by 3rd person so that instruction given in message will be performed once again, so customer will be effected

d) Repudiation - Here, sender or receiver acts as 3rd person or hacker

eg - In online websites, when customer pays amount, sometimes receiver may intentionally says that amount is not received & asks to resend.

iii) Attacks based on Availability

Denial of service - when many requests are sent from Client at a time, the traffic jams, so that server cannot respond & denies the request. This is called denial of service

Passive attacks - Unauthorized person completely concentrates on just to obtain information inspite of harming sender or receiver

eg: snooping, traffic analysis

Active attacks - Here unauthorized person harms either sender or receiver

eg - Modification, masquerading, Replaying, Repudiation, Denial of service.

Services - The security services are the services that are required to implement network security. There are 5 types of services

i) Confidentiality ii) Data integrity
iii) Authentication iv) Access control
v) Non-Repudiation

i) Confidentiality - Ensures that information in computer system and transmitted information are accessible only for reading by authorized parties. Confidentiality is protection of transmitted data from passive attacks. There are 3 types - connection confidentiality, connectionless confidentiality & selective field confidentiality & traffic flow confidentiality.

ii)

iii)

ii) Data integrity - Ensures that only authorized parties are able to modify Computer system assests & transmitted information. Modification includes writing, changing status, deleting, creating & delaying or replaying of transmitted message.

iii) Authentication - This service is concerned with assuring that communication is Authentic. The assurance that the communicating entity is one that it claims to be. This ensures that origin of message is correctly identified with an assurance that the identity is not false

2 types - Peer entity authentication,
Data origin authentication

iv) Access control - Requires that access to information resources may be controlled by target system. Access control is the ability to limit & control access to host systems & applications via communication links. To achieve this, each entity trying to gain access must first be identified or authenticated

v) Non-Repudiation - Requires that neither the sender nor receiver of message be able to deny transmission. when message is sent, the receiver can prove that alleged sender in fact sent the message. Similarly, when message is received, sender can prove that alleged receiver in fact received the message

Security Mechanisms - These are the set of processes that deal with recovery from security attack. A mechanism might operate by itself or with others to provide particular service.

Types of Mechanisms

i) Encipherment - It refers to process of applying mathematical algorithm for converting data into form that is not intelligible i.e., not readable form. It is achieved by 2 techniques named cryptography and encipherment. Level of data encryption is dependent on algorithm used for encipherment

ii) Access control - This mechanism is used to stop unattended access to data which you are sending. It can be achieved by various

techniques such as applying passwords, using Firewall or just by adding PIN to data.

iii) Notarization - This involves use of trusted 3rd party in communication. It acts as mediator between sender & receiver so that if any chance of conflict is reduced. This mediator keeps record of requests made by sender to receiver for later denied.

iv) Data Integrity - This mechanism is used by appending value to data to which is created by data itself. It is similar to sending packet of information known to both sending & receiving parties & checked before and after data is received. When data is same while sending & receiving, data integrity is maintained.

v) Authentication exchange - This deals with identity to be known in communication: sender and receiver exchange information using same secret key.

vi) Digital signature - This is achieved by adding digital data that is not visible to eyes. It is form of electronic signature which is added by sender which is checked by receiver electronically. This mechanism is used to preserve data & protect against forgery.

vii) Traffic Padding - Here we insert some bogus data or bits into gaps in data stream through network to test so that hacker gets confused

viii) Routing control - This enables selection of particular physically secure routes for certain data & allows routing changes, especially when breach of security is suspected

Security Goals - In Network, while transmitting the data, it is highly vulnerable to attacks. the network security aims to ensure that the entire network is secure. Network security entails protecting usability, reliability, integrity and safety of network and data.

Effective network security defeats a variety of threats from entering or spreading on network

The primary goals of network security are Confidentiality, Integrity and Availability. These 3 pillars of Nlw security are often represented as CIA triangle

i) Confidentiality – It is roughly equivalent to privacy & avoids unauthorized disclosure of information. It involves the protection of data, providing access for those who are allowed to see it while disallowing others from learning anything about content. It prevents essential information from reaching wrong people while making sure that right people get it.

Data encryption is good example.

ii) Integrity – It refers to the methods for ensuring that data is real, accurate and safeguarded from unauthorized user modification. It is the property that information has not be altered in an unauthorized way and source of information is genuine

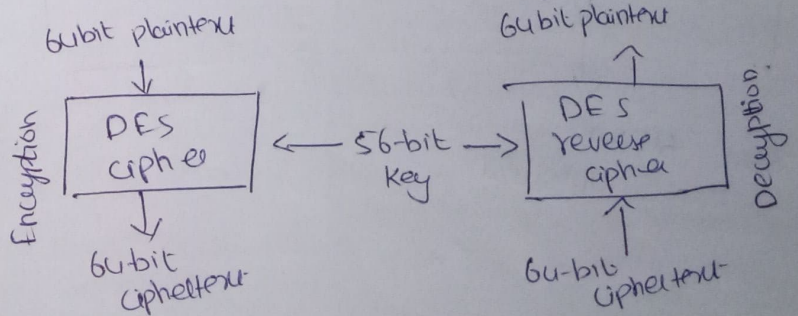
(iii) Availability – It is the property in which information is accessible and modifiable in a timely fashion by those authorized to do so. It is the guarantee of reliable and constant access to our sensitive data by authorized people.

UNIT-II

DES Algorithm

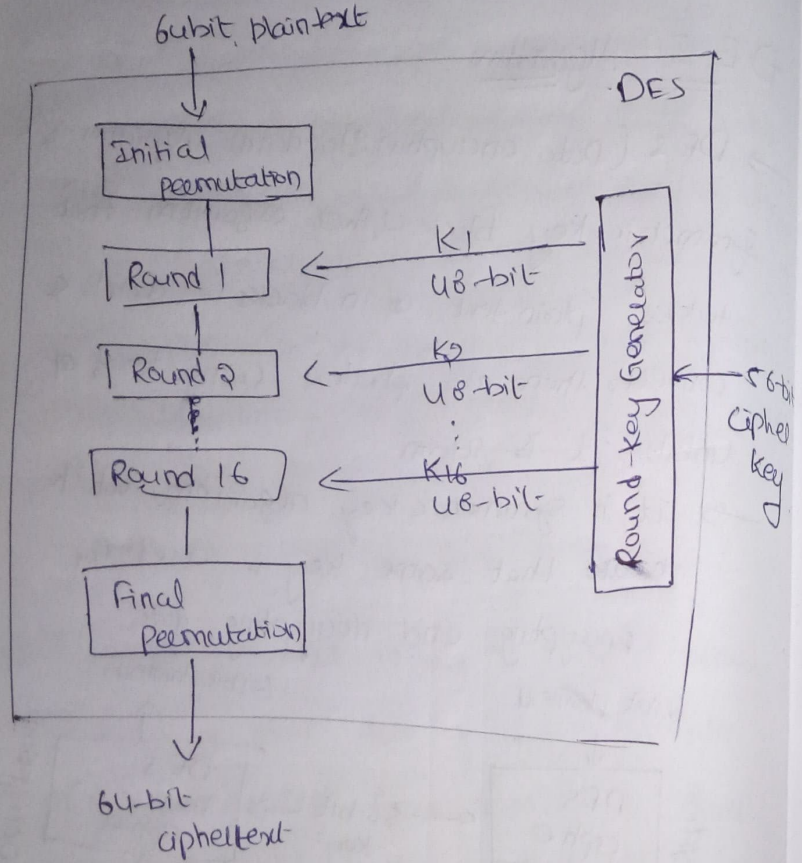
→ DES (Data encryption standard) algorithm is a symmetric-key block cipher algorithm that takes plain text of in blocks of 64bits & converts them into ciphertext using keys of 48bits. ~~It is symm~~

→ It is symmetric key algorithm, which means that same key is used for encrypting and decrypting data.



→ At encryption site, DES takes 64-bit plaintext & creates 64bit ciphertext, at the decryption site, DES takes 64-bit ciphertext & creates 64-bit block of plaintext The same 56-bit cipher key is used for both encryption and decryption

General structure of DES



Algorithm steps

1) The process begins with 64-bit plaintext block getting handed over to an initial permutation (IP) function

2) The initial permutation is performed on plain text

3) Next, IP creates 2 halves of permuted block, referred to as left plain text (LPT) and Right plaintext (RPT).

4) Each LPT and RPT goes through 16 Rounds of encryption process
The encryption process is further broken down into five stages
a) Key transformation
b) Expansion permutation
c) S-Box permutation
d) P-Box permutation
e) XOR and swap
For decryption, we use same algorithm, and we reverse the order of 16 round keys.

5) Finally, LPT and RPT are rejoined and a Final Permutation (FP) is performed on newly combined block

6) The result of this process produces desired 64-bit - cipher text

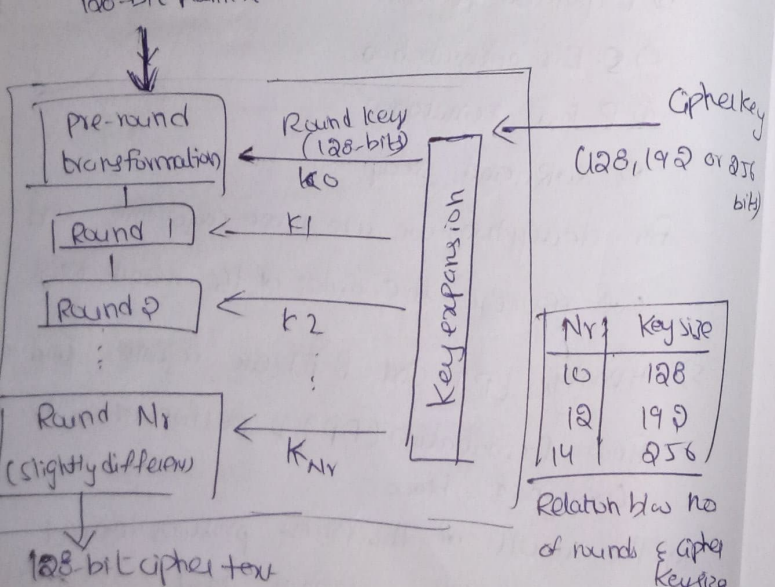
AES algorithm –

→ Advanced Encryption Standard (AES) algorithm is a symmetric block cipher algorithm and is most widely adopted symmetric encryption algorithm

→ AES includes three block ciphers AES-128, AES-192 and AES-256

→ There are 10 rounds in 128-bit keys, 12 rounds in 192-bit keys and 14 rounds in 256-bit keys each of these rounds uses different 128-bit round key, which is calculated from original AES key

AES encryption cipher

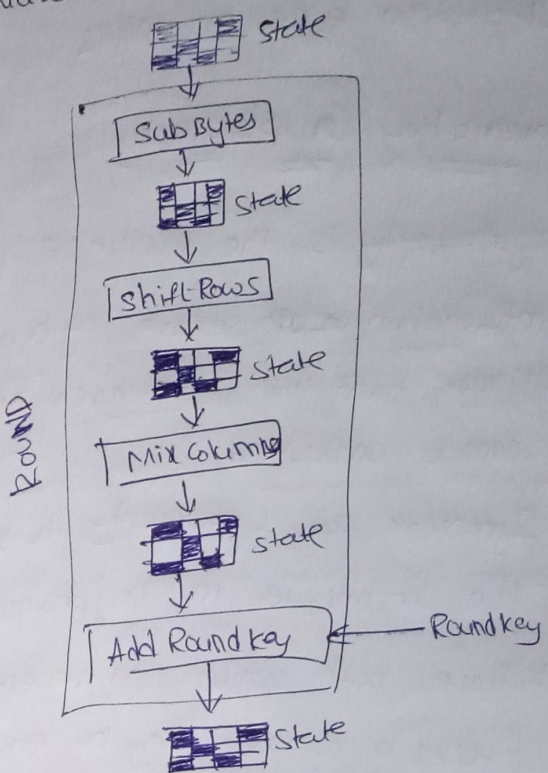


Nr	Key size
10	128
12	192
14	256

Relation b/w no of rounds & cipher key size

Encryption process

structure of each round at encryption site



→ Each round, except last uses four transformations that are invertible. The last round has only 3 transformations

→ Each transformation takes state and creates another state to be used for next transformation or next round.

→ The pre-round section uses only one transformation (AddRoundKey).

→ At decryption site, the inverse transformations are used: Inv SubByte, Inv ShiftRows, Inv MixColumns, AddRoundKey (this is self-invertible)

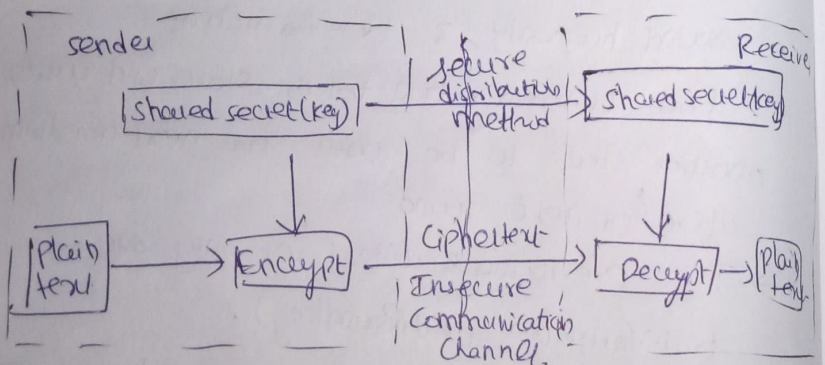
→ AES is stronger and faster than Triple-DES and it provides full specification & design details

Symmetric key Cryptography

→ Cryptography is the science of keeping information secure by transforming it into form that unintended recipients cannot understand

→ Symmetric key cryptography is one of the techniques in cryptography

→ Here, both sender and receiver uses a common key to encrypt and decrypt the message.



The message exchange involves following steps

→ Before starting communication, sender & receiver shares secret key

→ This secret key is shared through some external means

→ At sender side, sender encrypts message using his copy of key

→ The cipher text is then sent to receiver over the communication channel

→ At receiver side, receiver decrypts cipher text using his copy of key.

→ After decryption, the message is converts back into readable format.

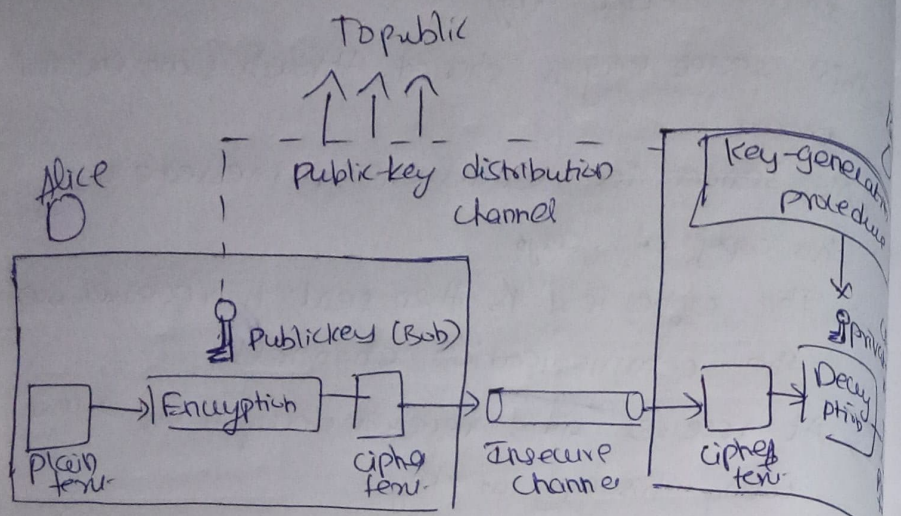
UNIT-III

Asymmetric key Cryptography

→ In Asymmetric key cryptography, we use 2 different keys, one for encryption and another for decryption

we use terms like private key and public key for better understanding

→ The following figure show the general idea of asymmetric-key cryptosystem



→ Here, the burden of providing security is mostly on receiver (Bob).

→ Bob need to create 2 keys - 1 private & 1 public.

→ Bob is responsible for distributing public key to community. This can be done through public-key distribution channel. This channel must provide authentication & integrity.

→ Bob & alice cannot use same set of keys of 2-way communication. Each entity in community should create their own public & private keys.

→ In above fig, it shows that Alice can use Bob's public key to send encrypted messages to Bob. If Bob wants to respond, Alice needs to establish her own private & public keys.

→ After encrypting the plain text into cipher text, that text is transmitted over the insecure channel.

→ Here Bob needs to have his private key inorder to decrypt the cipher text which was previously encrypted using Bob's public key.

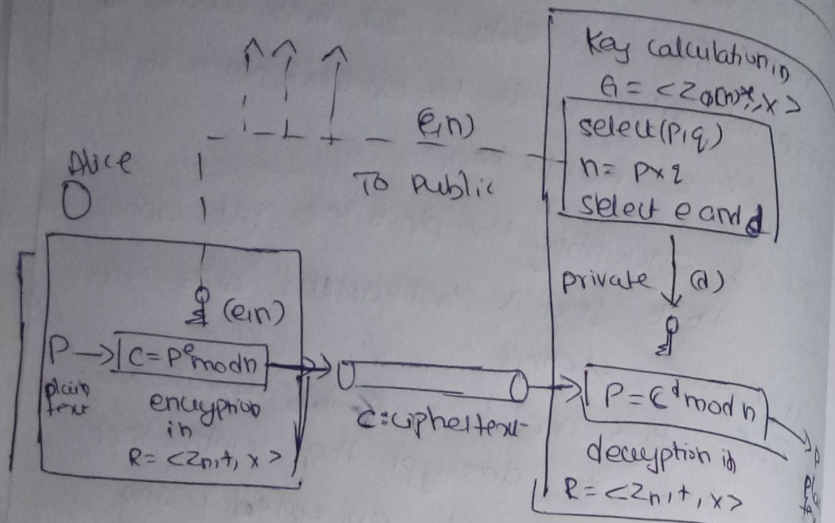
→ By using Bob's private key, Bob can convert the cipher text ie, he can decrypt the text into original plaintext.

RSA Algorithm

→ RSA algorithm is public key encryption technique and is considered as most secure way of encryption.

→ It was invented by Rivest, Shamir and Adleman in year 1978, & hence named as RSA algorithm.

General idea behind procedure used in



Steps in RSA algorithm

1) Generate RSA modulus

→ The initial procedure begins with selection of 2 prime numbers p & q & then calculating their product n,

$n = p * q$

n - specified large number

2) Desired Number (e) - Consider number e as desired number which should be greater than 1 & less than (p-1) & (q-1) which is not common factor of p-1 & q-1 except 1.

3) Public key - Specified pair of number n & e forms RSA public key & it is made public

4) Private key - Private key d is calculated from p, q & e as

$e^d = 1 \bmod (p-1)(q-1)$

Encryption formula - consider sender, who sends plain text message to someone whose public key is (n, e). To encrypt plain text message, we use this formula -

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

Decryption formula - Considering receiver C has private key d, the modulus will be calculated as

$$P = C^d \bmod n$$