Lecture Notes For CNS Prepared By SWARNALATA SAHOO

CHAPTER-1
Possible attacks on Computer

The need for security:

- The growing computer implies a need for automated tools for protecting files and other information.
- The use of network and communication facilities for carrying data between users and computer is also growing, so network security measures are needed to protect data during transmission.
- To avoid data threats.
- To avoid Denial of Service(DOS)
- To secure data from hackers. To safeguard our data from data analyzer.

Security Approaches:

(a) Trusted System:

- It is a computer system that can be trusted to a specified extend to enforce a specific policy.
- Trusted system where initially of primary interest to the military.
- However, these days the concept has spanned across various area most permanently in the banking and the financial community but the concept never caught on.
- Trusted system often use the term “REFERANCE MONITER” .This is an entity i.e. logical heart of the computer system.

(b)Security Models:

- Security models an organization can take several approaches to implement its security model and these approaches are:
  1. No Security:
     i. In this simplex case the approaches could be decision to implement no security at all.
  2. Security through Obsecurity:
     i. In this model, a system is secured simply because nobody knows about its existence and contents. This approach cannot

work for too long, as there are many ways an attacker can come to know about it.

3. Host Security:
   i. In this scheme, the security for each host is enforced individually.
4. Network Security:
   i. In this scheme, the focus is to control network access to various host and there services, rather than individually host security.

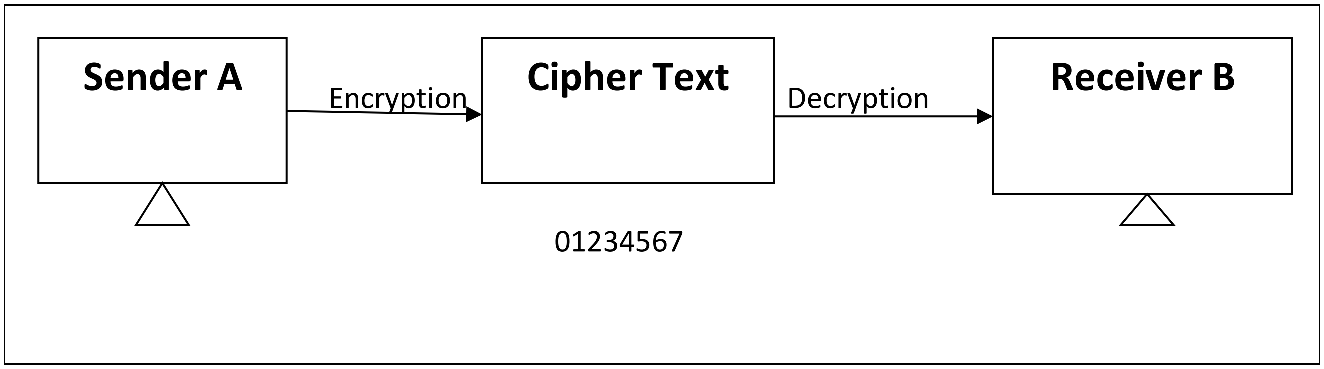
(c) Security Management Practices

- Good security management practices always talk of security policy being in place.
- Putting a security policy in place is actually quite and tough.
- A good security policy generally takes care of 4 key aspects:
  1. Affordability:
     (i) Cost and effort in security implementation.
  2. Functionality:
     (i) Mechanism of providing security.
  3. Cultural Issues:
     (i) Whether the policy gets well with people expectation, working style and believes.
  4. Legality:
     (i) Whether the policy meets the logical requirements.

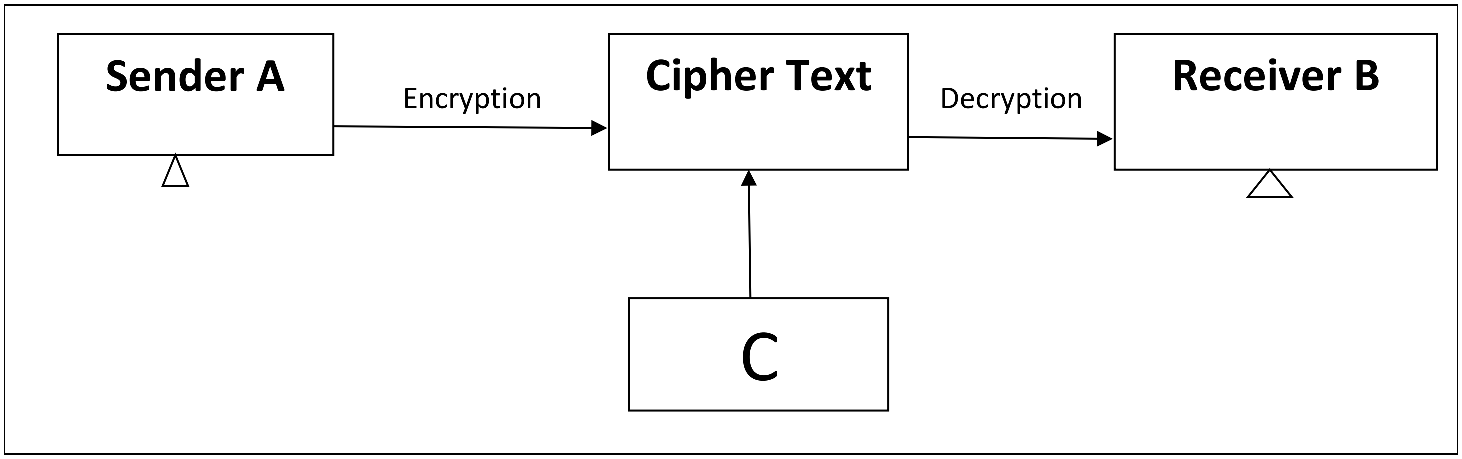
Principle of Security:

(a) Confidentiality:

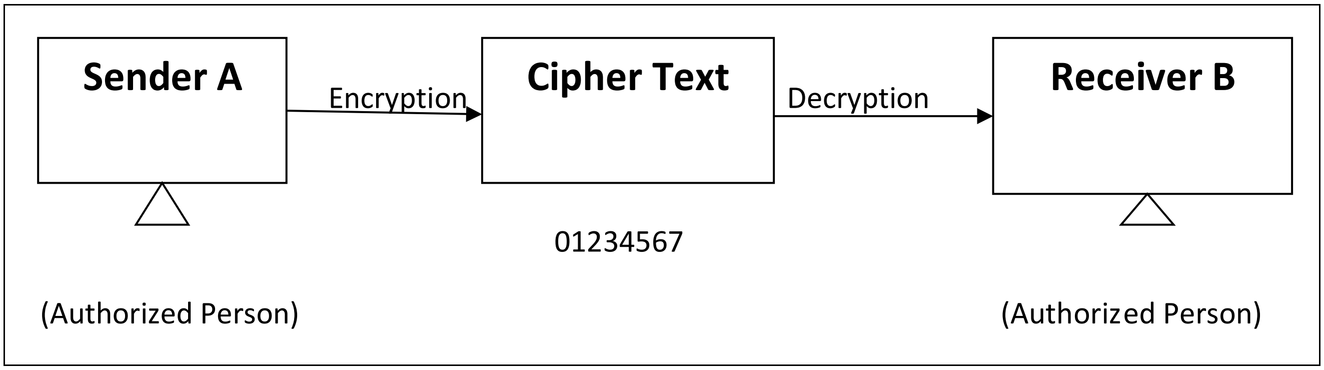
- Only sender, intended receiver should understand message contents.
  i) Sender encrypts the message
  ii) Receiver decrypts the message
- Third person cannot access to the system



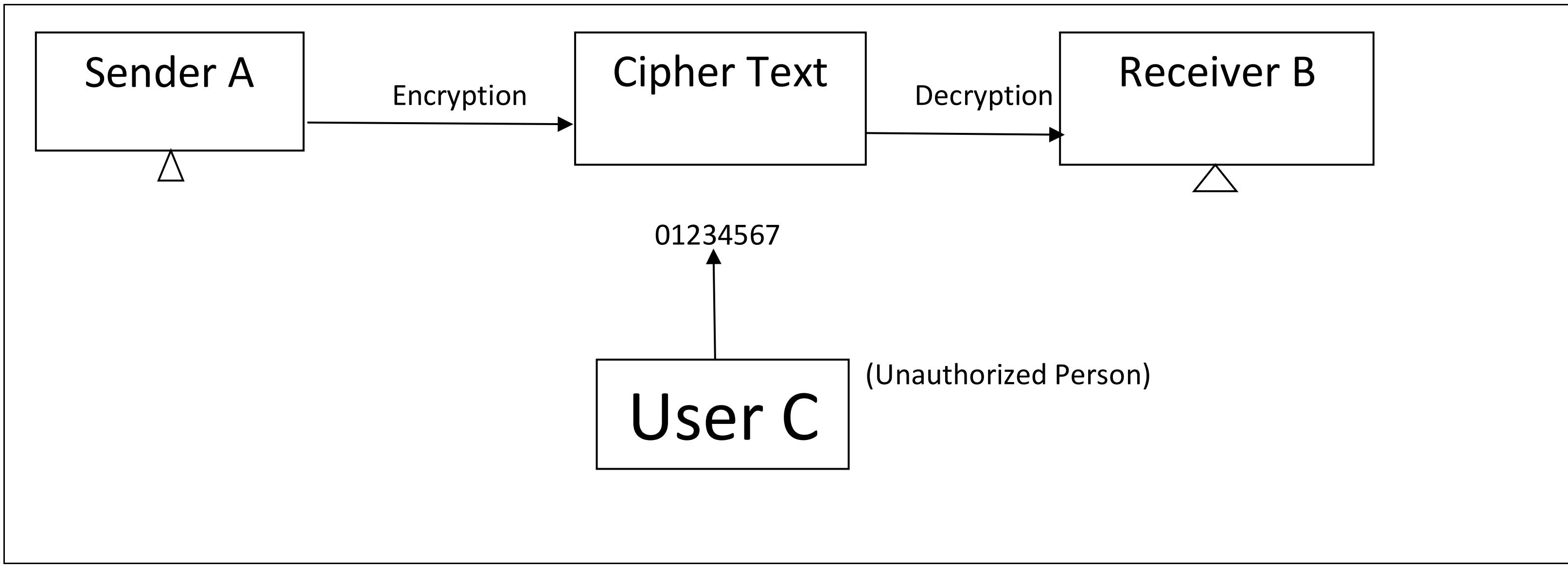
Loss of Confidentiality:



(b) Authentication:

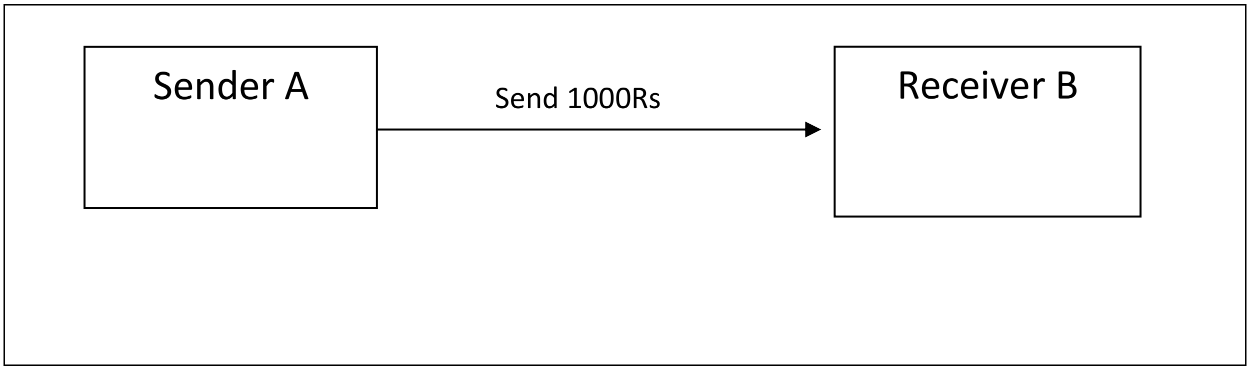


Loss of authentication:



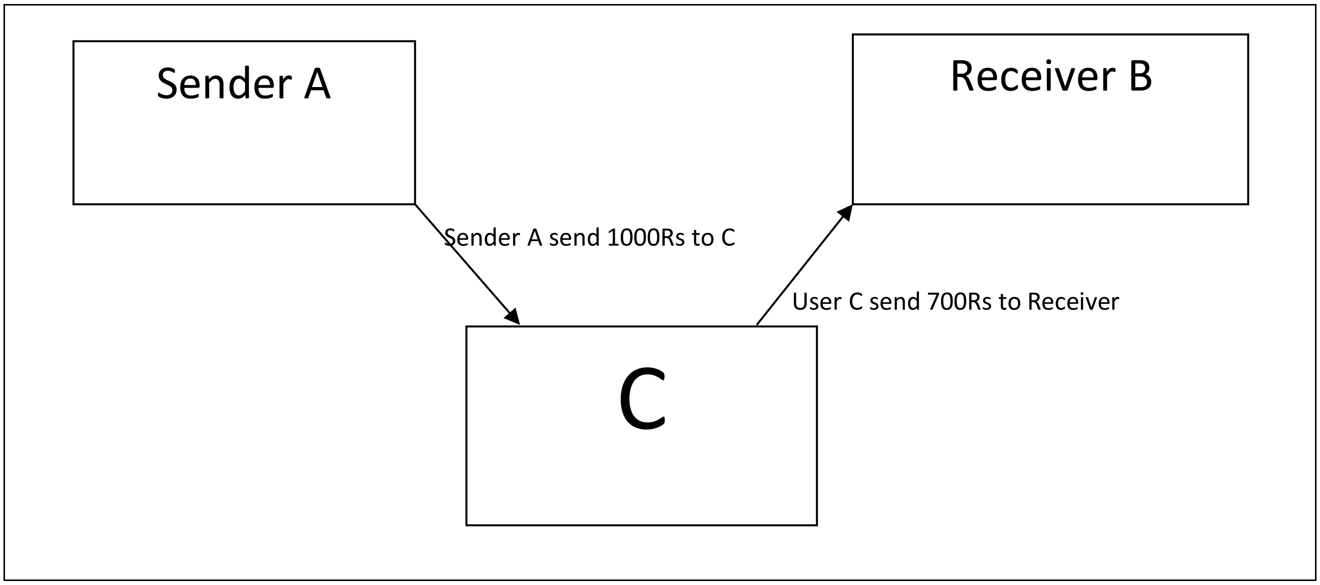
- Sender , receiver want to confirm the identity
- Both sender and receiver should be authorized to communicate the system.

(c) Message Integrity:

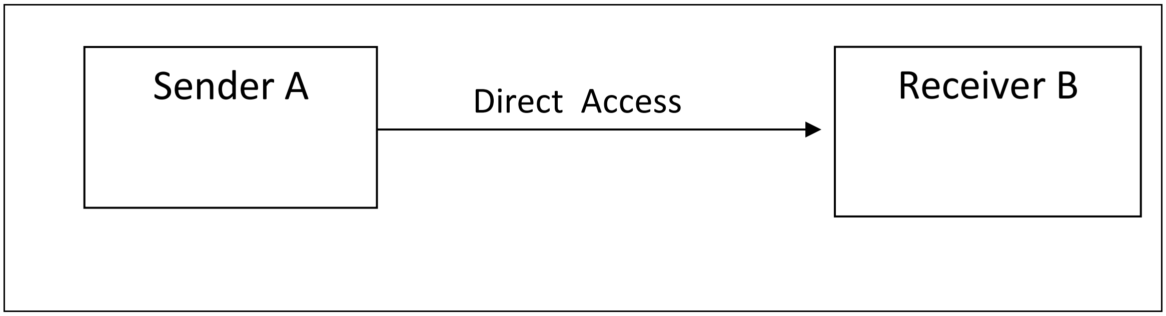


- Sender and receiver want to ensure message content not altered without detection.

Loss of Message Integrity:

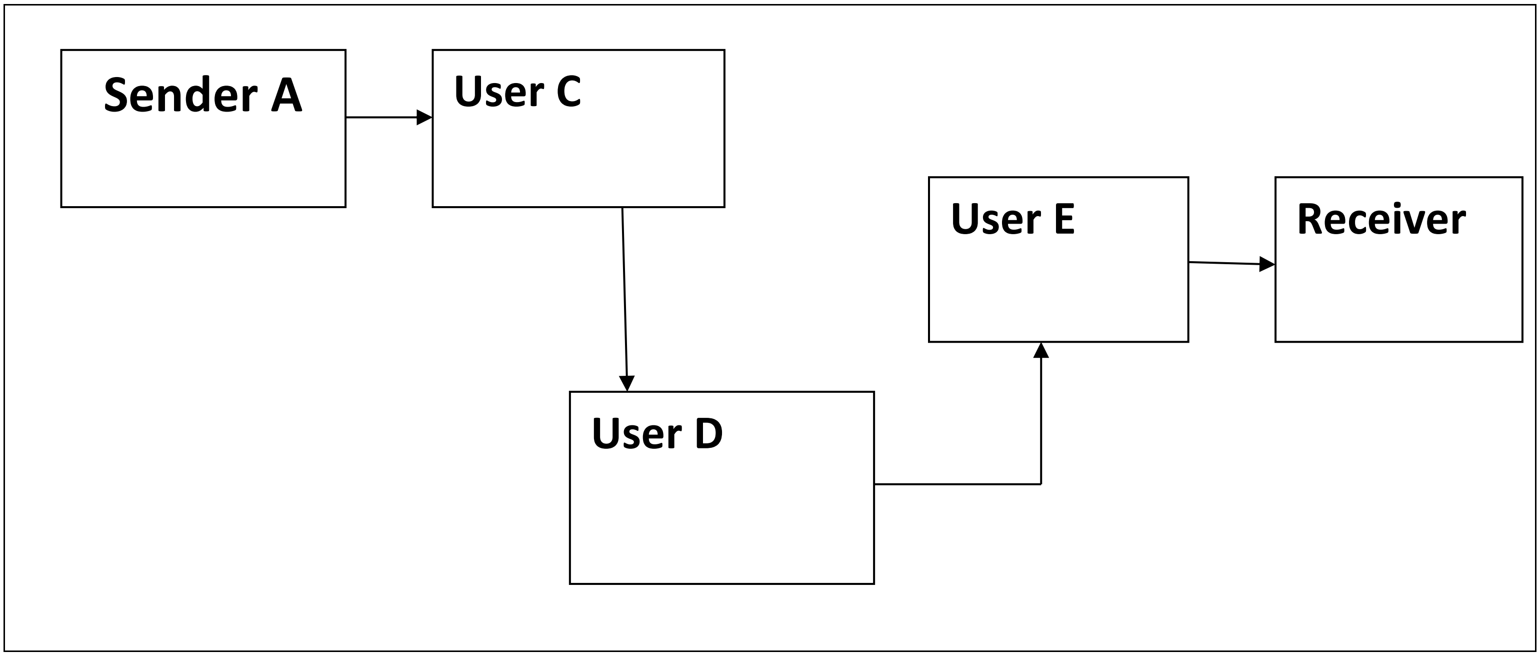


(d) Access and availability:



- Service must be accessible and available to the user.

Loss Of Access and Availability:



SECURITY SERVICES (GOALS):

(a) **Data Confidentiality:**

- It is designed to protect data from disclosure attack.
- The service as defined by X800 is very broad and encompasses confidentiality of the whole message or part of a message and also protection against traffic analysis.
- It is designed to prevent snooping and traffic analysis attack.

(b) <u>Data Integrity:</u>

- It is designed to protect data from modification, insertion, deletion and replaying by an adversary.
- It may protect the whole message or part of the message.

(c) <u>Authentication:</u>

- This service provides the authentication of the party at the other end of the line.
- In connection-oriented communication, it provides authentication of the sender or receiver during the connection establishment (peer entity authentication).
- In connectionless communication, it authenticates the source of data (data origin authentication) .

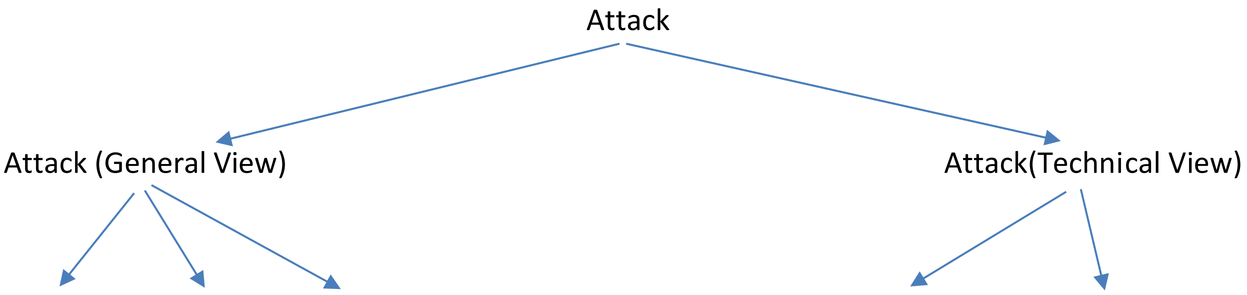
(d) <u>Access Control:</u>

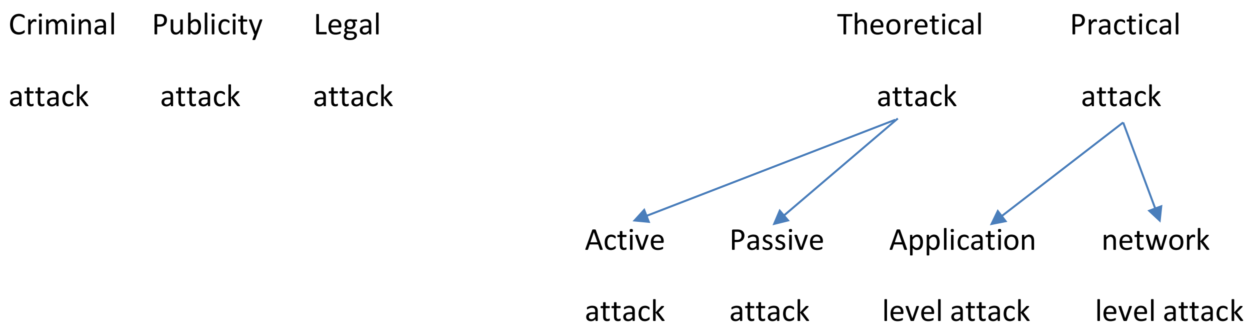
- It provides protection against unauthorized access to data.
- The term access in this definition is very broad and can involve reading, writing, modifying, executing programs and so on.

<u>(e) Non-Repudiation:</u>

- This service protects against repudiation by either the sender or the receiver of the data.
- In non-repudiation with proof of the origin, the receiver of the data can later prove the identity of the sender if denied.
- In non-repudiation with proof of delivery, the sender of data can later prove the data were delivered to the intended recipient.

<u>Types of Attack:</u>





Attack (General view)

Criminal attack: -

Criminal attacks are the simplest to understand their, the sole aim of the attackers is to maximize financial gain by attacking computer system.

These attacks are: -

1. Fraud – (OTP)
2. Scam – (duplicate side use)
3. Destruction – (account hack and block)
4. Identity theft
5. Intellectual identity theft
6. Brand theft – (nonbrand)

Publicity Attack: -

- It occurs because the attackers want to see their names appear on television, News channel and newspaper.

- History suggests that these types of attackers are usually not hardcore criminal, their people such as student in the universities or employees in large organization to seek publicity by adopting a novel approach of attacking computer system.

Legal Attack: -

- This form of attack is quite noble and unique.

- Here the attackers try to make the judge or the jury doubtful about the security of the computer system.

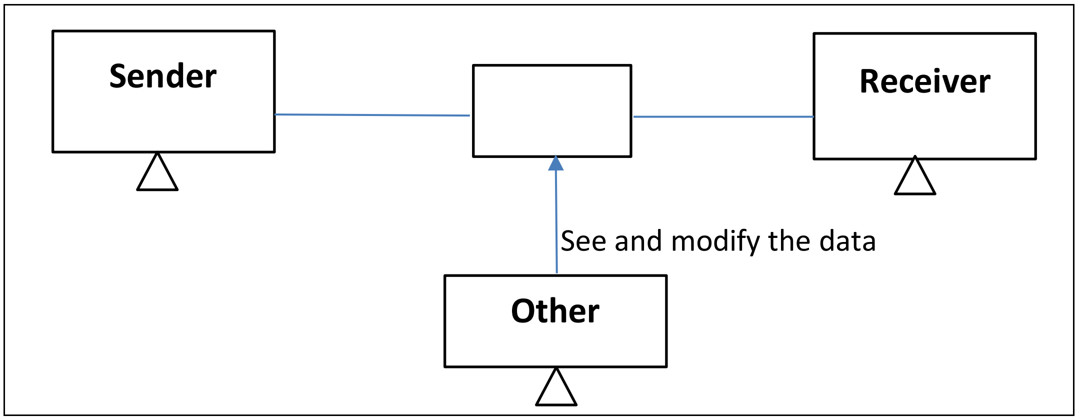
- These attackers attack the computer system and attack the party they manage to take the attacker to the court while the case is being fought.

Attack (Technical view): -

(a)Theoretical Attack: -

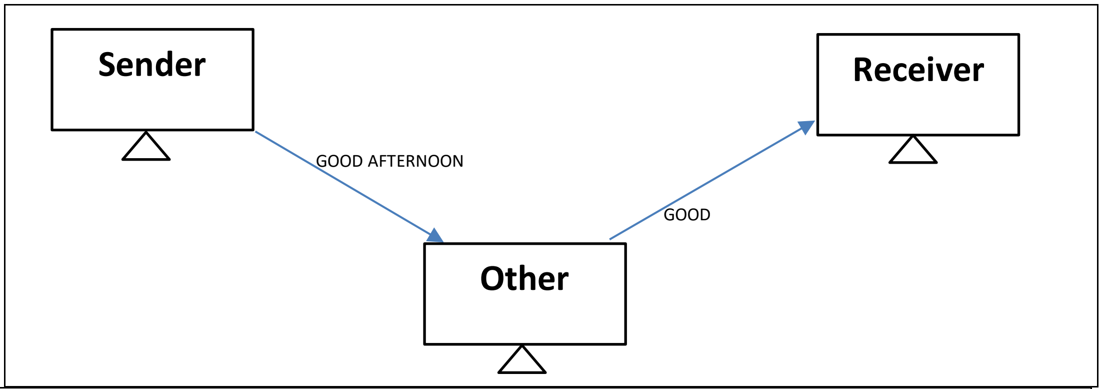
(1) Active Attack: -

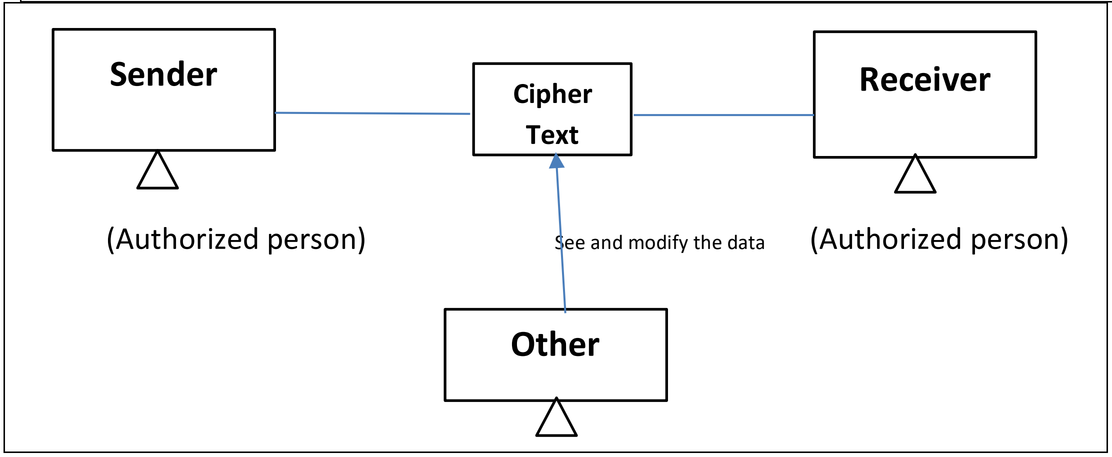
- In active attack the main aim of the attacker is just to obtain information.
- The attacker modifies the data to harm the system.
- Active attacks are 3 types: -
  - I. Interruption
  - II. Modification
  - III. Fabrication



(i)Interruption: -

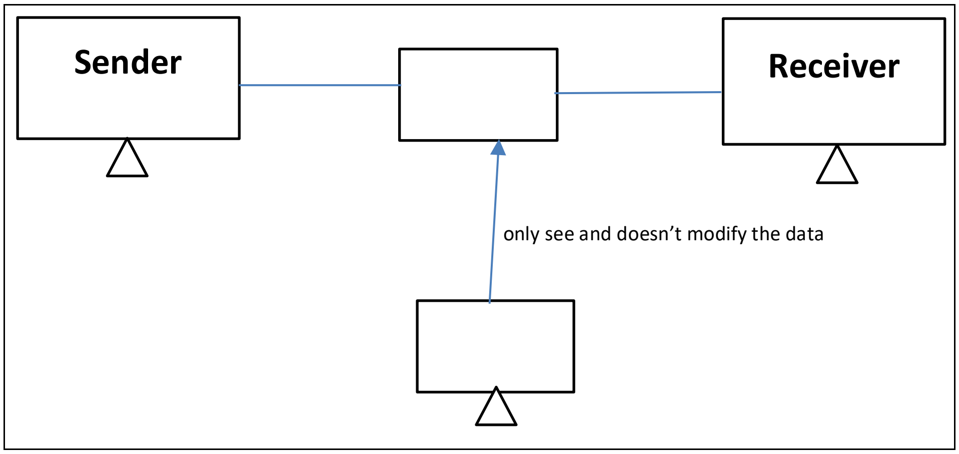
- Its means that an unauthorized Party has gain access to resource the party can be person or program or computer-based system.





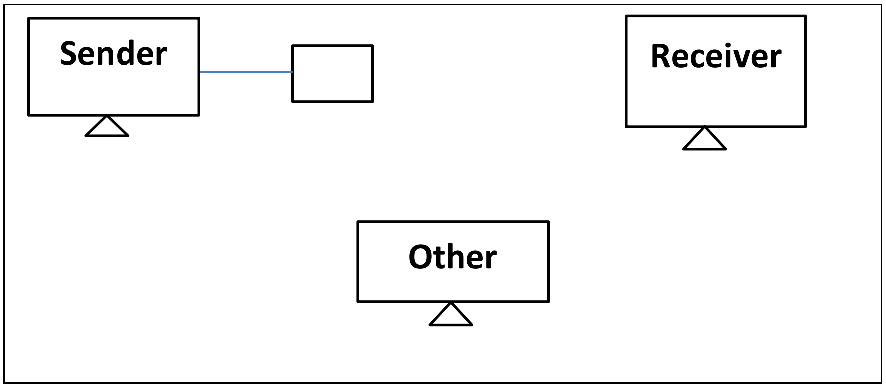
(ii)Modification: -

- Sender receiver want to ensure message contain change without detection.



(iii)Fabrication: -

- The resource become unavailable, lost or unusable.
- Ex-Fabrication are causing problems to hardware device or erasing programming data or operating system component.



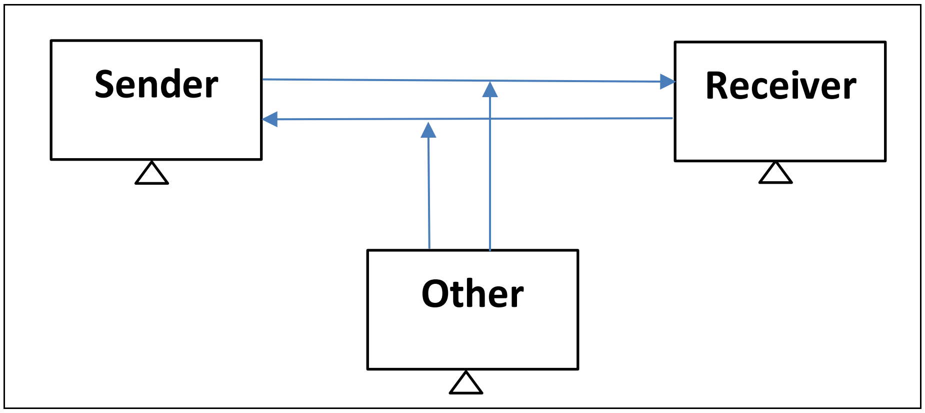
(b)Passive attack: -

- In passive attack the attacker's goal is just to obtain information. This attack does not modify the data or harm the system and system continue with its normal operation.

- There are 2 types of passive attack: -
  I. Release of message contents
  II. Traffic analysis

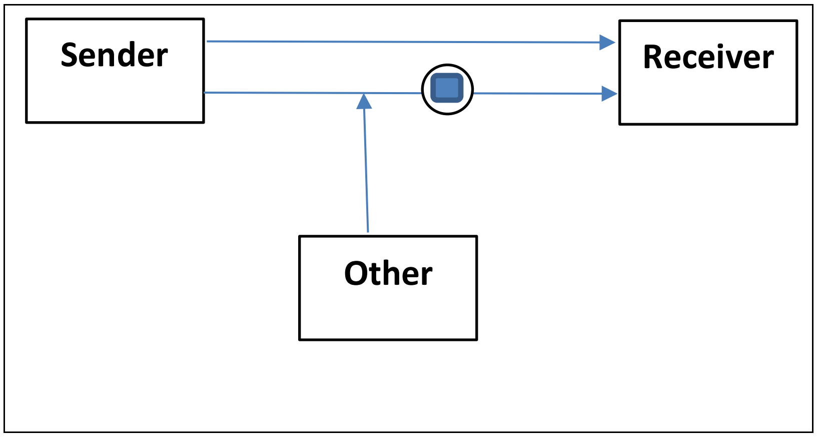
(i)Release of message contents: -

- Release of message content is quite simple to understand when we send confidential e-mail message to our friend, we desire that only third person able to access it.



(ii)Traffic analysis: -

- It is the process of inserting and examining message in order to deduce information from, patterns in communication.



Practical Attack: -

(i)Application-level attack: -

- These attacks happen at an application level in the sense that the attackers attempt to access, modify or prevent access to information of a particular application or to the application itself.
- Example: -
- Example of thin earth trying to obtain some one's credit card information on the internet or changing the contents of a message to change the amount in transaction.

(ii)Network level attack: -

- These attacks generally aim at reducing the capabilities of network by a number of possible means.
- This attack generally make an attempt to either slow down or completely bring to haults a computer.

Program that attacks: -

- A few programs that attack computer system to cause some damage or to create some confusion.
- Program that attack -

  i. Virus:-

  - A virus is a computer program that attaches itself to another legimate program and cause damage to the computer system or to the network.

ii.Worm:-

- A worm doesn’t perform any destructive actions and instead only consume system resource to bring it down.

iii. Trojan horse:-

- A trojan horse allows an attacker to obtain some confidential information about a computer an a network.

CHAPTER-2
Cryptography Concepts

Plain Text (Readable Text):

- Any communication in the language that we speak i.e., the human Language takes the form of plain text or clear text.
- A Clear text or plain text signifies a message that can be understand sender and the receiver and also by anyone else who gets an access to that message.

Cipher Text (Unreadable Text):

- when a plain text message codified using any suitable scheme, the resulting message is called as Cipher text.

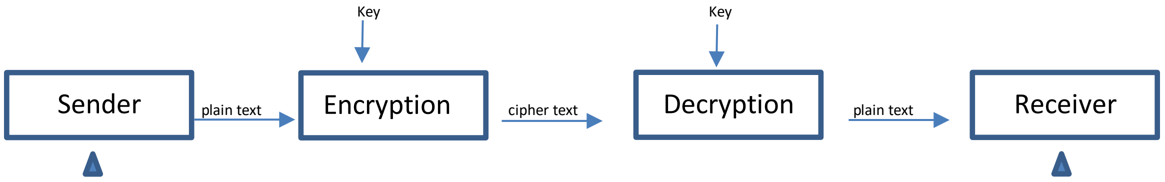
→ Encryption techniques is consisting of two techniques:

1. Substitution Technique.

2.Transposition Technique.

(I) Substitution Technique:

- In the substitution technique, the characters of plain text are replaced by other character or number or symbols.



Different types of substitution techniques are:

1) Caesar Cipher.

2) Modified Caesar Cipher

3) Mono- Alphabetic Cipher

4) Poly Alphabetic cipher

5) Playfair Cipher

1) Caesar Cipher:

- It was first proposed by Julius Caesar and termed as Caesar Cipher.
- It is a special case of substitution technique where in each alphabet, in a message is replaced by an alphabet 3 places down in the line.

Ex:

A B C D ← PT (Plain Text)

↓ ↓ ↓ ↓

D E F G ← CT (Cipher Text)

Ex:

C R I C K E T ← PT (Plain Text)

↓ ↓ ↓ ↓ ↓ ↓ ↓

F U L F N H W ← CT (Cipher Text)

2) Modified Caesar Cipher:

- It was first proposed by Julius Caesar and termed as Modified Caesar Cipher.
- It is a special case of substitution technique where in each alphabet in message is replaced by an alphabet 4 places down the line.

Ex:

C O M P U T E R S C I E N C E ← PT (Plain Text)

↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓ ↓

G S Q T Y X I V W G M I R G I ← CT (Cipher Text)

3) Mono Alphabetic Cipher:

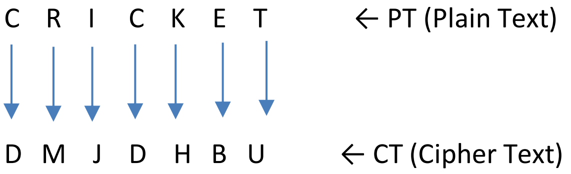
- It uses fixed substitution over entire message.
- It is also the “One to One” substitution Cipher Method.

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

↓ ↓

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

Ex:

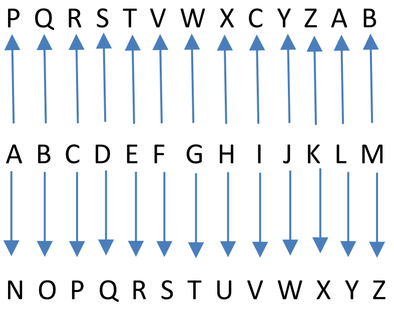


C R I C K E T ← PT (Plain Text)

D M J D H B U ← CT (Cipher Text)

4) Poly-Alphabetic Cipher

- a poly-alphabet cipher uses a of substitution at different position in the message.
- It is also the “One to Many” substitution Cipher method.

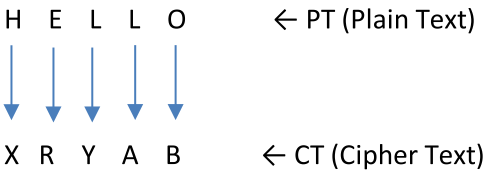


P Q R S T V W X C Y Z A B

A B C D E F G H I J K L M

N O P Q R S T U V W X Y Z

Ex:



H E L L O ← PT (Plain Text)

X R Y A B ← CT (Cipher Text)

5) Playfair Cipher:

- The Playfair cipher also called as Playfair square, is a cryptographic technique that is used for manual encryption of data. This scheme was invented by Charles Wheatstone in 1854.

Algorithm:

Stap 1: Choose keyword.

Step 2: Enter characters of keyword in 5×5 matrix, row wise from left to right.

Step 3: Fill remaining spaces in matrix with rest of English alphabet.

Step 4: Combine i and j in same cell.

Rules:

1) If both the alphabets are in the same row, replace them with alphabets to their immediate right.
2) If both the alphabets are in the same column, replace them with alphabets immediately below them.
3) If not in same row/column, replace them with alphabets in the same row respectively but at other pair of corners.

Note: The blank spaces in pair can be inserted by X or Z, and two same characters can not be pair.

Ex:

Keyword - Playfair Encryption

P	l	a	y	f
i/j	r	e	n	c
t	o	b	d	g
h	k	m	q	s
u	v	w	x	z

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

Ex:

PT → N A M E

CT → E Y W B

PT → B A L L O N

B A L X L O N X

CT → M E Y V R K D Y

(II) Transposition Technique:

- A transposition cipher is a method of encryption by which the position held by unit of plain text (which are commonly characters/ group of characters) are shifted according to a regular system. so that cipher text constitutes a permutation of plain text.
- Position plain text will be changed to convert the cipher text.

Ex:

PT→ N A M E

1 2 3 4 (position)

CT→ E M A N

4 3 2 1 (position)

- Available no. of permutations = n!

  where n = number of characters

- Here available no. of permutations = n! = 4! = 4*3*2*1 = 24

- The different types of transposition techniques are:
  1) Railfence Technique
  2) Simple Columnar Technique

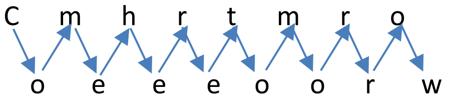
(1) Railfence Technique:

Step 1: write down the plain text message as sequence of diagonals.

Step 2: Read the text row by row.

Ex:

PT→ Come here tomorrow



CT→ Cmhrtmrooeeeooew

(2) Simple Columnar Technique:

Step 1: Write down the plain text message row by row in a rectangle of predefined size.

Step 2: Read the message column by column, however it need not be in the order of columns 1,2,3... etc. It can be any random order such as columns 2,3,1 etc

Step 3: The message, thus obtain is the cipher text message.

Ex:

PT→ Come home tomorrow

Column = 6

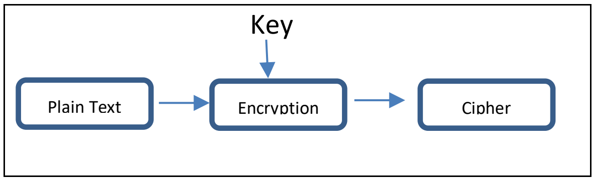
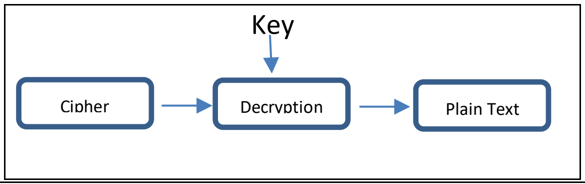
C_1	C_2	C_3	C_4	C_5	C_6
C	o	m	e	h	o
m	e	t	o	m	o
r	r	o	w		

- Columns will be switch to a random order.
- Let us decide the order of column as some random order say, 4 2 1 6 3 5 .

C_4 C_2 C_1 C_6 C_3 C_5

CT→ eow oer Cmr oo mto hm

Encryption and Decryption:

Encryption	Decryption
→ It is a process of converting from plain text to cipher text using a key. → It has automatic in nature, because whenever the data is transport/send between two machines, it is automatically encrypted. → In that process text will be considered as coded form (non-readable form). 	→ It is a process of converting from cipher text to plain text using a key. → It has automatic & manual in nature, because the receiver of data automatically converts them from the ports to original ports. In some case it is done manually as well. → In that process that will be considered as non-coded form (readable form) 

Key Encryption:

There two types of key encryptions:

i) Symmetric Key Encryption
ii) Asymmetric key encryption.

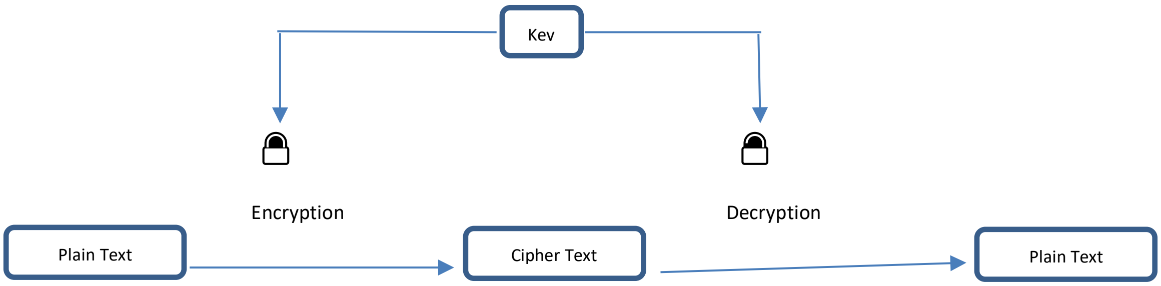
I) Symmetric Encryption

- In the case of symmetric key encryption, the same key is used for both encrypting and decrypting messages. Because the entire mechanism is dependent on keeping the key a shared secret- meaning that it need to be shared with the recipient in a secure way so that only they can use it to decrypt the message- it does not scale well.
- Symmetric encryption algorithm can use either block ciphers or stream ciphers, with block ciphers, a number of bits (in chunks) is encrypted as a single unit. For instance, AES uses a block size of 128 bits with options for three different kay lengths- 128, 192, or 256 bits.

Key Takeaways (points):

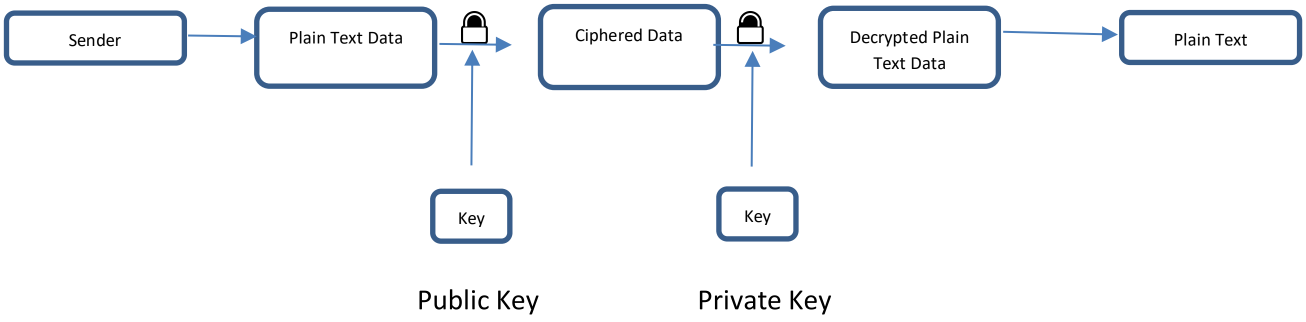
1. There's a single shared by that's used for encryption and decryption.

2. It doesn't scale very well because the secret key must not be lost or shared with unauthorized parties, on else they can read the message.



II) Asymmetric Key Encryption:.

- Asymmetric key encryption uses a pair of related keys- a public and a private key. The public key, which is accessible to everyone, is what's used to encrypt a plaintext message before sending it. To decrypt and read this message, you need to hold the private key. The public and the private Keys are mathematically related, but the private key cannot be derived from it .
- In asymmetric encryption (also known as public-key cryptography or public key encryption), the private key is only shared with the key's initiator since its security needs to be maintained.
- Because asymmetric key encryption is a more complicated process than its symmetric counterpart, the time required is greater. However, this type of encryption offers a higher level of security as compared to symmetric encryption since the private key is not meant to be shared and is kept a secret. It is also a considerably more scalable technique.



Key Takeaways (Points):

1) It involves the use of two mathematically related keys. The public key (the one that's known to everybody) and the private key (which is only known by you) are required for encrypting and decrypting the message. The private key cannot be derived from the public key.

2) The public key is used by others to encrypt the messages they send to you, but to decrypt and read those messages, one needs access to the private key.

Differentiator	Symmetric Key Encryption	Asymmetric Key Encryption
Symmetric Vs Asymmetric	Only one key is used, and the same key is used to encrypt and decrypt the message.	Two different cryptographic keys, called the public and the private keys, are used for encryption and decryption.
complexity & speed of Execution	It's a simple technique, and because of this, the encryption process can be carried out quickly.	It's a much more complicated process than symmetric key encryption, and the process is slower.
length of key	The length of the keys used, is typically 128 or 256 bits, based on the security Requirement.	The length of the key is much larger, e.g., the recommended RSA key size is 2048 bits or higher.
Usage	It's mostly used when large chunks of data need to be transferred	It's used in smaller transactions, primarily to authenticate and establish a secure communication channel prior to the actual data transfer.
Security	The secret key is shared, consequently the risk compromise is higher.	The private key is not shared, and the overall Process is more secure as compared to symmetric encryption.
Examples of Algorithms	Examples includes RC4, AES, DES, 3DES, etc.	Example includes RSA, Diffie-Hellman, ECC, etc.