Network Security
Unit-1

Need of Security

- To protect the data

Principles of Security

- Confidentiality.

  Only the sender and the intended receiver should access the message. Loss of confidentiality results in ***interception***.
- Authentication.

  It helps establish proof of identities. Absence of authentication leads to ***fabrication***.
- Integrity.

  The contents of the message should remain same when the receiver receives it. Loss of integrity leads to ***modification***.
- Non- Repudiation.

  Does not allow the sender to refute the claim of not sending that message.
- Access Control.

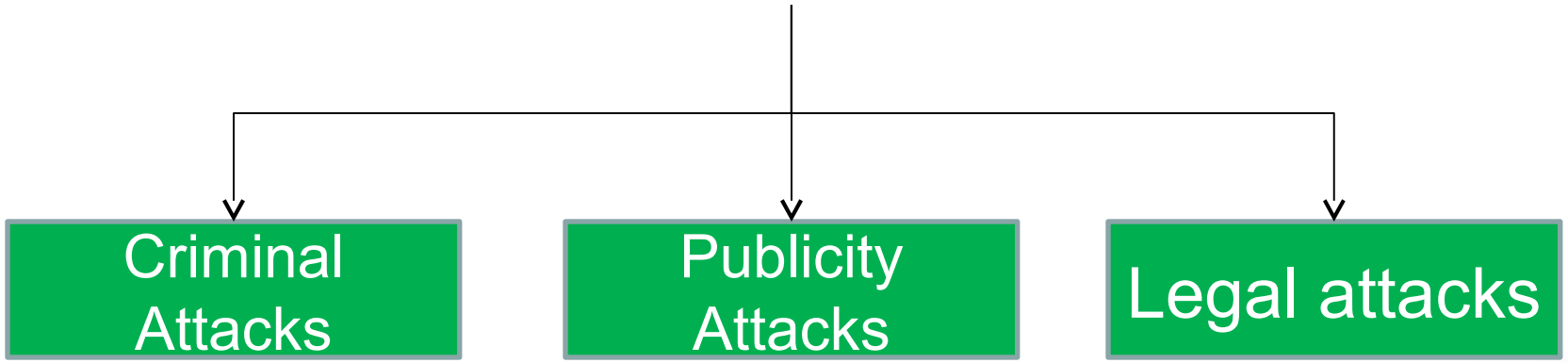
  Who should be able to access **what**. It is broadly related to two areas: role management and rule management.
- Availability.

  Resources should be available to all authenticated persons who need them. ***Interruption*** puts the availability of resources in danger.

Types of Attacks

- Attacks can be classified with respect to 2 views:
- Common person’s view
- Technical view

Common person's view

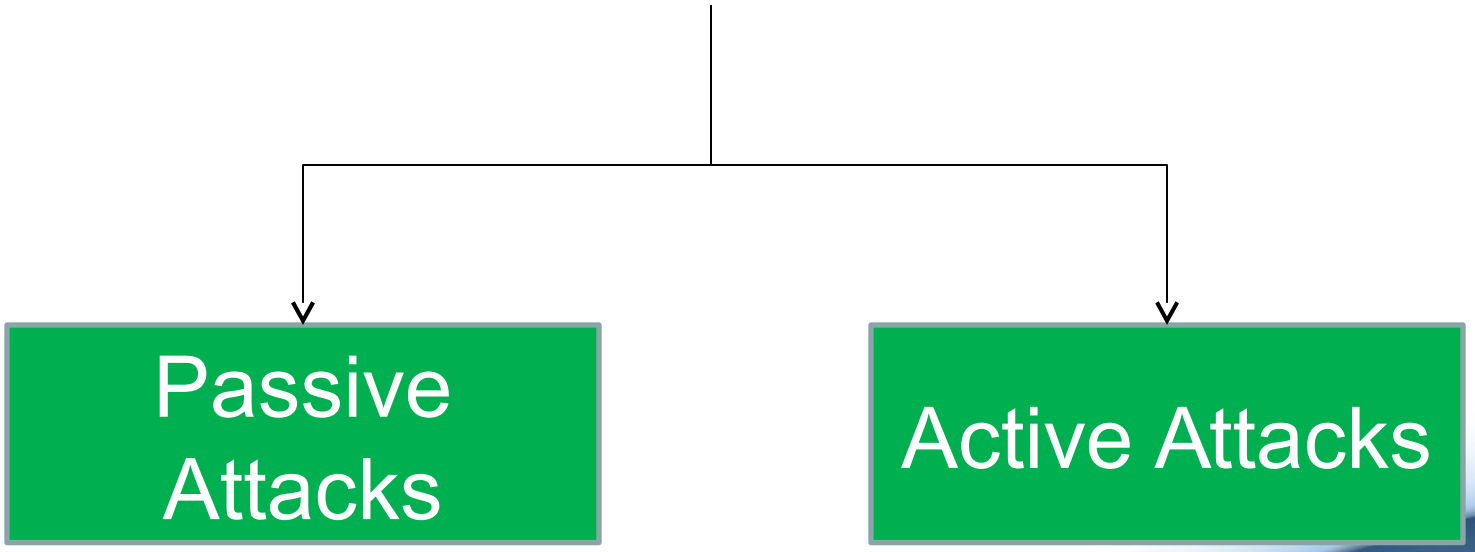


Done for financial gain
(for eg: fraud, scams, destruction, identity theft, intellectual property theft, brand theft)

Done for publicity

Makes the court doubtful about the security of system

Technical View



Passive Attacks

- Passive Attacks are those wherein the attacker indulges in ***monitoring the data which is in transit***.
- The attacker does not attempt to modify the data.
- That's why they are ***hard to detect***. Only prevention can be done rather than detection or corrective steps.

Passive Attacks do not involve any modification to the contents of an original message .

Again divided into 2 sub categories:-

1.) Release of message contents

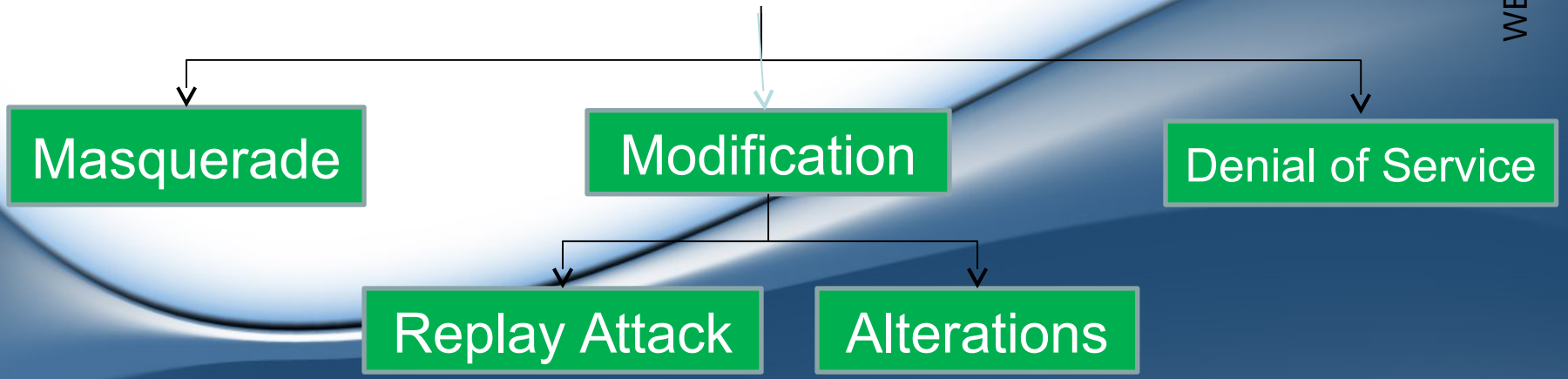
2.) Traffic Analysis.

Active Attacks

- The active attacks are based on the ***modification of the original message*** in some particular manner or on creation of a false message.
- These attacks cannot be prevented easily.
- However efforts can be taken to detect them and recover from them.

In Active Attacks the contents of the original message are modified in some way.

These attacks can be in the form of :-



- Practically these attacks are performed at:
- Application level
- Network level

Cryptography

- ***Cryptography is the art of achieving security by encoding messages to make them non- readable.***
- **Cryptanalysis**: is the technique of making the non-readable format into readable format. It is just like breaking the code.
- **Cryptanalyst**: A person who performs cryptanalysis.
- **Cryptology**: is the combination of cryptography and cryptanalysis.

- Important terms used in cryptography:
- **Plain text**

  The original message which can be easily read is called as plain text.
- **Cipher text**

  A coded message which is not understood by everyone (except the intended receiver) is known as cipher text.
- **Encryption or Encoding or Encode**

  The process of converting plain text into cipher text is called as encoding.
- **Decryption or Decoding or Decode**

  The process of converting cipher text into plain text is called as decoding.
- **Key**

  A key is a character or a group of characters used to encrypt or decrypt the plain text. A key is generally developed/created from the plain text.

Some techniques of encoding

- Substitution technique

  Where the individual letters of the original message are substituted by any other alphabet.
- Transposition Technique

  Where the individual letters of the original message are just rearranged.

Substitution Techniques

- **Caesar Cipher**:

  The Characters of the plain text message are replaced by alphabets 3 places down the order

ATTACK	ON	TAJ
DWWDFN	RQ	WDM

- **Mono-alphabetic Cipher**
- Each character is replaced with alphabet with no order. For e.g. each A can be replaced by any letter from B to Z or even A and so on.
- Here the no. of attempts are as 26x25x24x23x22…… or $4x10^{26}$ possibilities.

ATTACK	ON	TAJ
SRRSUP	AN	RSD

- **Polygram Substitution Cipher**:
- Here rather than replacing each letter, each word of the message is substituted.
- Replacement happens block by block

ATTACK
GJJGPM

ATTACKER
YHZOGCIV

- **Poly alphabetic Substitution Cipher**:
- It uses multiple one-character keys.
- Each key encrypts one letter of plain text
- 1st letter- 1st key, 2nd letter-2nd key ……..
- After all keys are used, they are recycled.
- Examples : Vigenere cipher, Beaufort cipher

Example:

PLAIN TEXT

KEY

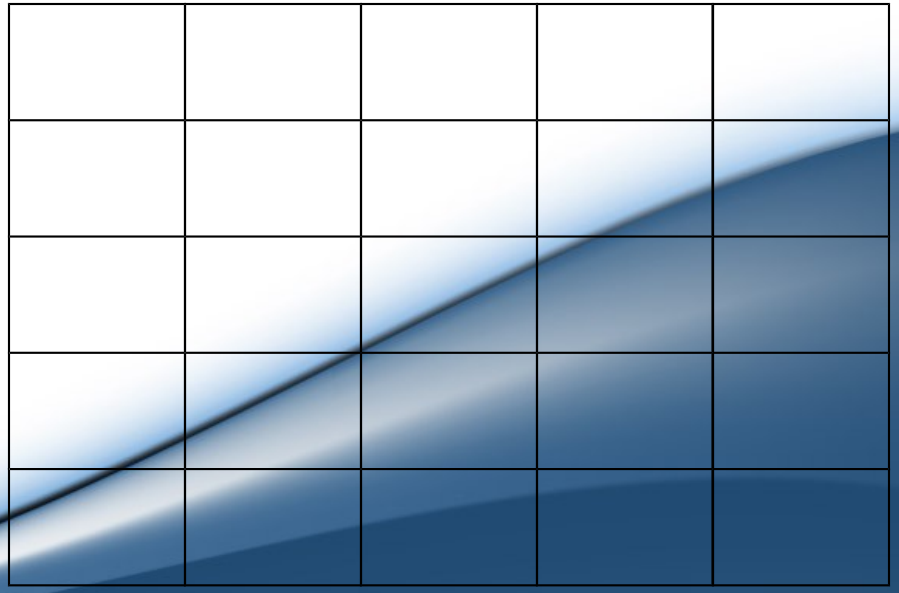
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T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

- **Playfair Cipher**:
- Developed by Charles Wheatstone but named after his friend
- This scheme uses two main process:
- **Step:1 Creation and population of matrix.**
- **Step:2 Encryption process**

Step:1 Creation and population of matrix (using key)

- Choose a word, sentence or characters as a keyword.
- Create a 5x5 matrix. Fill the keyword in the matrix excluding the duplicates.
- After filling the matrix, if there are still some blank space then fill them with other letters excluding the ones which you have already filled.

Let us say, the keyword is "**NUCLEAR ATTACK**"



Let us say, our original message is “BOMB PLACE IN EUROPE”

Step:2 The encryption process
-> break the message into pair of 2 letters as:

BO MB PL AC EI NE UR OP EX
TQ QR XK TN BQ UN RF PQ LY

Use the matrix with respect to rules.

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

Step:2 Encryption Process

- Before initiating the encryption, break the plain text in pair of 2 letters.
- If both the alphabets are same or 1 letter is remaining, add X after the first alphabet.
- After the initial process, take the pairs for encryption.
- If the letters of the pair appear in same row of the matrix then substitute them with their immediate right letter. If the letter of the plain text is itself the rightmost, then wrap it up with the left letter
- If the letters of the pair appear in same column of the matrix then substitute them with their immediate below letter. If the letter of the plain text is itself below, then wrap it up with the top letter
- If the letter of the pair are not in same row or column then define a rectangle with the original pair and substitute them with other corners of the rectangle.

- **Hill Cipher:**
- Invented by Lester Hill in 1929.
- Treat each letter with a number like A=0, B=1, C=2……

Let us say, our original message is “TAJ”

As per the rule, T=19 A=0 J=9

Convert into matrix form as $\begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix}$

Now ***multiply the plain text matrix with any number as keys***. The multiplying matrix should be of *n* x *n* where n is the number of rows of original matrix.

$$\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix} \times \begin{bmatrix} 19 \\ 0 \\ 9 \end{bmatrix} = \begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix}$$

Now compute ***mod 26*** on resultant matrix i.e. take the remainder after dividing by 26.

$$\begin{bmatrix} 123 \\ 337 \\ 515 \end{bmatrix} \bmod 26 = \begin{bmatrix} 19 \\ 25 \\ 21 \end{bmatrix}$$

Now translating numbers into alphabets, we get:

19=T 25= Z 21=V

Therefore our cipher text is ***TZV***

To decrypt hill cipher, follow the steps:

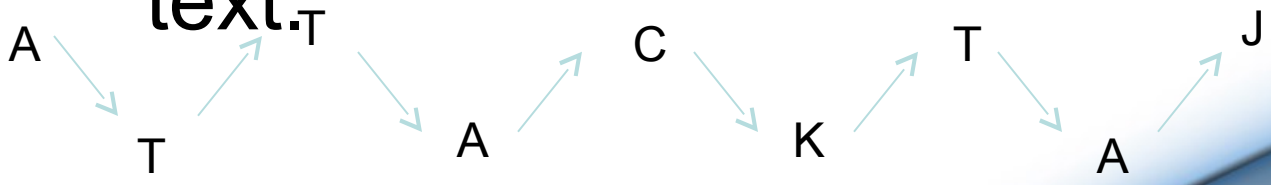
1.) take cipher text matrix and multiply it by inverse of original key matrix

2.) Again perform mod by 26.

Thus we get our original text.

Transposition techniques

- **Rail – fence technique**
- It involves writing plain text as a sequence of diagonals and then reading it row by row to produce cipher text.



Cipher Text : ATCTJTAKA

Original Message: ATTACK TAJ

- **Simple Columnar Transposition Technique**:
- Write the plain text message row by row in a rectangle of pre-defined size
- Read the message column by column but the sequence of columns can be any order.

Original Text : ATTACK ON EUROPE

Col 1	Col 2	Col 3	Col 4	Col 5	Col 6
A	T	T	A	C	K
O	N	E	U	R	O
P	E				

Columns are read in 2,4,6,1,5,3 order
TNEAUKOAOPCRTE

- **Simple Columnar Transposition Technique with multiple rounds**:
- It is same as earlier one but repeated again upto 1 to 3 times as desired.

- **Vernam Cipher (one time pad):**
- It uses a one-time pad, which is discarded after a single use and therefore is suitable only for short messages.
- Treat each plain text alphabet with numbers as A=0, B=1, C=2……

Original Message: ATTACK TAJ

Plain text		A	T	T	A	C	K	T	A	J
		0	19	19	0	2	10	19	0	9
	+									
One Time Pad		N	B	D	E	P	S	F	Z	L
(substitute with		13	1	3	4	15	18	5	25	11
any letters which										
are used only ones)										
Initial Total		13	20	22	4	17	28	24	25	20
Substrcat 26,										
If >25		13	20	22	4	17	2	24	25	20
Substitute		N	U	W	E	R	C	Y	Z	U

- **Book Cipher**
- Similar to Vernem cipher.
- Instead it uses characters of books to substitute.
- Remaining all the work is same

Encryption & Decryption

- **Encryption or Encoding or Encode**

  The process of converting plain text into cipher text is called as encoding.

- **Decryption or Decoding or Decode**

  The process of converting cipher text into plain text is called as decoding.

The important aspects of **Encryption & Decryption** process are:

- **Algorithm**

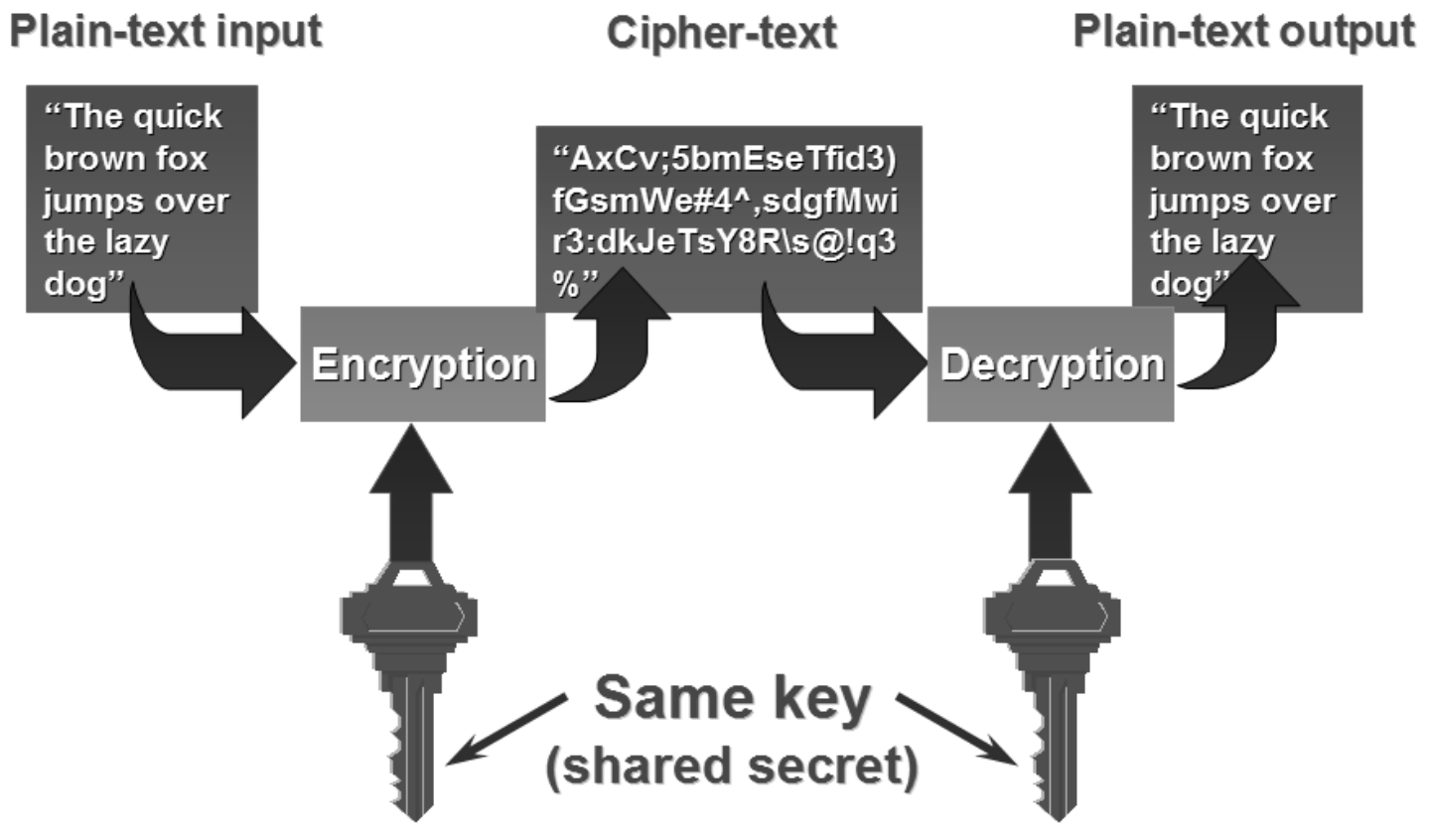
  The technique/ method used to encrypt or decrypt. Algorithm is generally not kept secret.

- **Key**

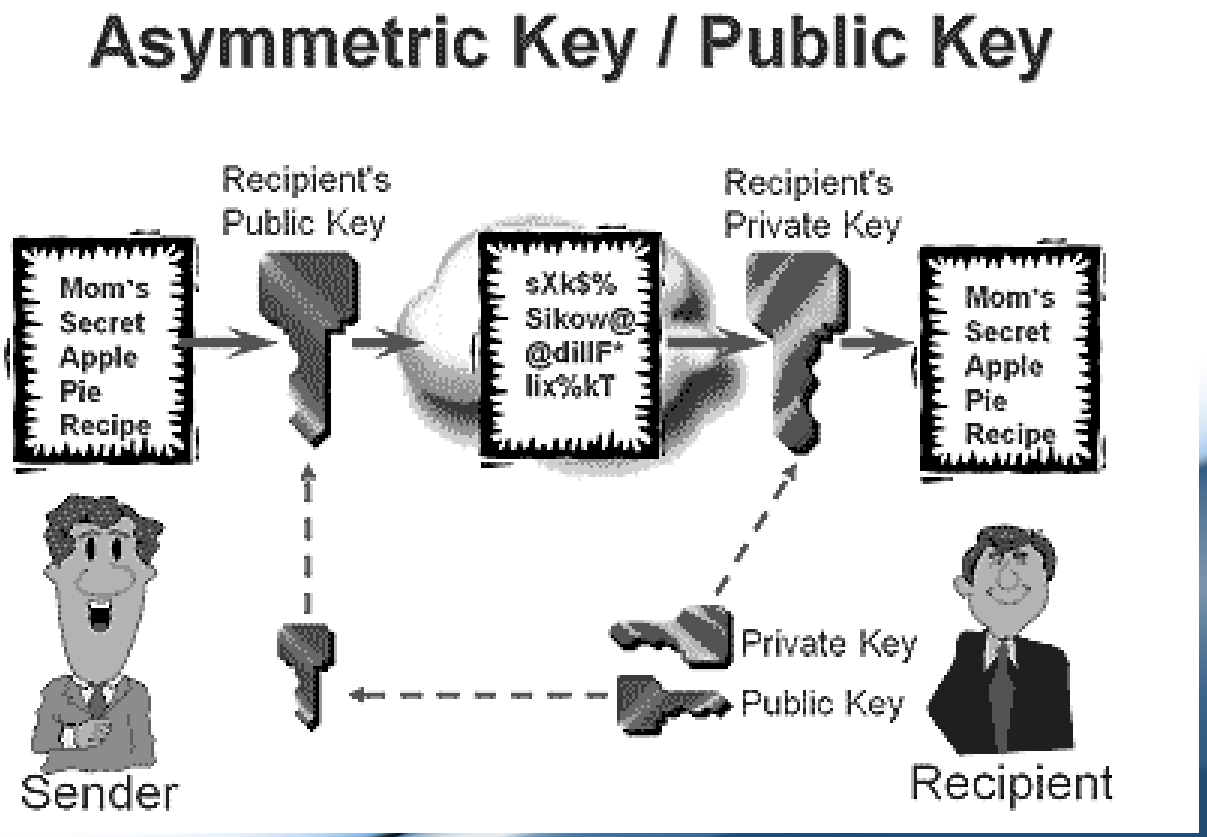
  A key is a character or a group of characters used to encrypt or decrypt the plain text. A key is generally kept secret.

- Depending on what keys are used, there are two types of cryptography mechanisms:-
- **Symmetric Key Cryptography**
- **Asymmetric Key Cryptography**

Symmetric Key Cryptography



Asymmetric Key Cryptography



Possible types of Attack

Attack	Things known to the attacker	Things the attacker wants to find out
Cipher-text only	• Cipher text of several messages, all of which are encrypted with the same encryption key. • Algorithm used	• Plain text messages corresponding to these cipher text messages • Key used for encryption
Known cipher text	• Cipher text of several messages, all of which are encrypted with the same encryption key. • Plain text messages corresponding to above cipher text messages • Algorithm used	• Key used for encryption • Algorithm to decrypt cipher text with the same key
Chosen plain text	• Cipher text and associated plain text messages • Chooses the plain text to be encrypted	• Key used for encryption • Algorithm to decrypt cipher text with the same key
Chosen cipher text	**•Cipher text of several messages to be decrypted •Corresponding plain text messages**	**Key used for encryption**

Key Range

- A **key range** a number of attempts to crack a key.
- For eg: for a brute force attack with a mono alphabetic algorithm, there are 0 to 100 billion attempts to crack a key. Thus a **key range becomes from 0 to 100 billion**.

Key Size

- The concept of key range leads us to the principle of **key size**.
- As money is measured in rupees, dollars; the strength of key is measured in key size.
- We measure **key size in bits** representing in binary system.
- If a key is of 1 bit, then the possibilities are 0 or 1.
- If a key is of 2 bit, then the possibilities are 00,01,10,11.
- If a key is of 3 bit, then the possibilities are 000,001,010,011, 101,111, 100, 110.
- Generally, a key is preferred as 56-bit key or 64-bit key or 128-bit key.

Steganography

- Steganography is a technique that facilities hiding of a message that is to be kept secret inside other messages.
- Initially, sender used techniques like invisible ink, tiny pin punctures on specific characters, minute variations between handwritten characters, pencil marks on handwritten characters etc.
- Now a days, sender hide secret messages within graphic images

Thank You