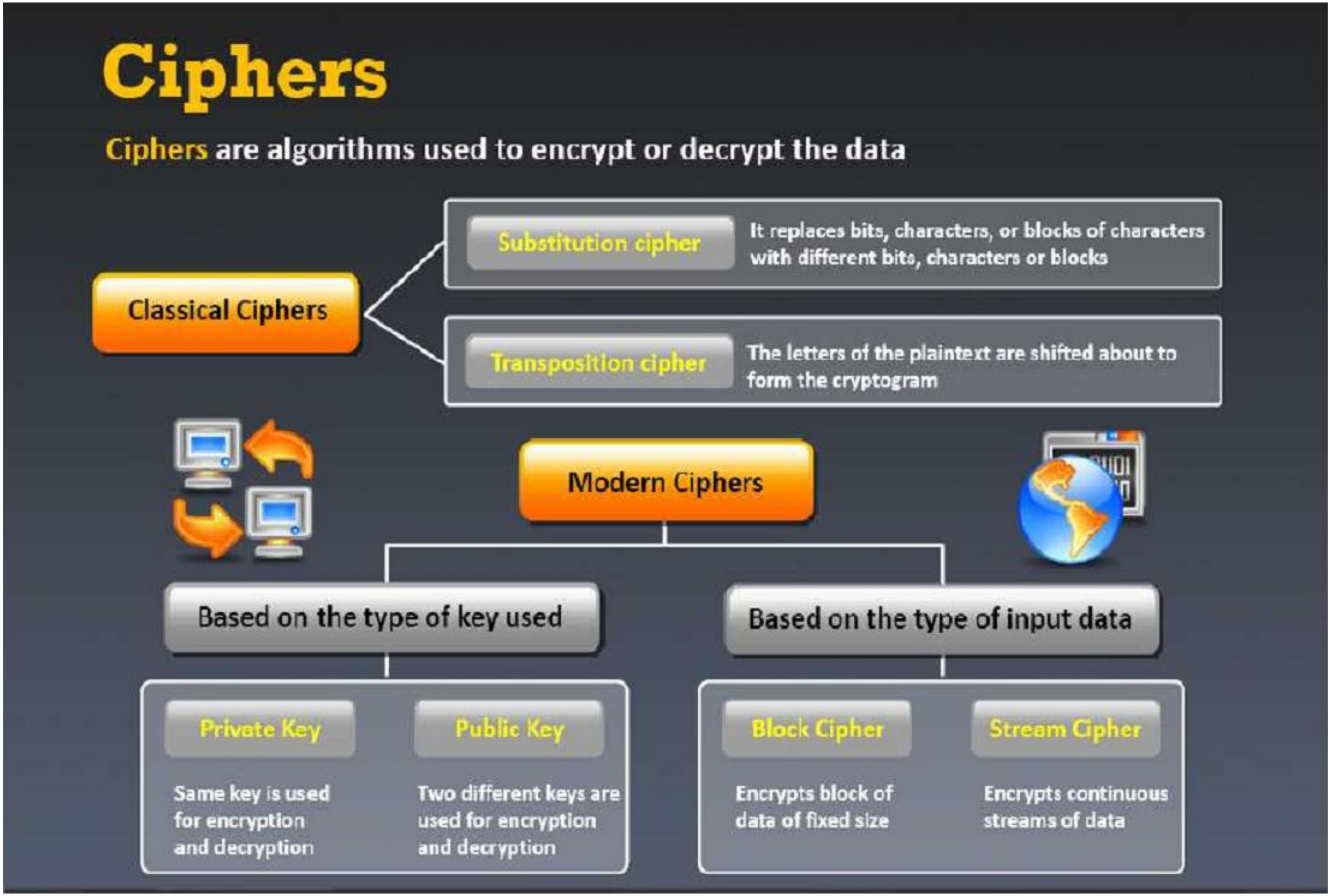
INFORMATION NETWORK SECURITY

Dr/ Amr Wageeh

Lecture 2

CONTENTS


Ciphers
Ciphers are algorithms used to encrypt or decrypt the data
Classical Ciphers
Substitution cipher
It replaces bits, characters, or blocks of characters with different bits, characters or blocks
Transposition cipher
The letters of the plaintext are shifted about to form the cryptogram
Modern Ciphers
Based on the type of key used
Based on the type of input data
Private Key
Same key is used for encryption and decryption
Public Key
Two different keys are used for encryption and decryption
Block Cipher
Encrypts block of data of fixed size
Stream Cipher
Encrypts continuous streams of data

CLASSICAL SYMMETRIC ENCRYPTION

- Plaintext is viewed as a sequence of elements (e.g. bits or characters).
- **Substitution cipher:** replacing each element of the plaintext with another element.
- **Transposition (or permutation) cipher:** rearranging the order of the elements of the plaintext.

SUBSTITUTION CIPHERS

- A substitution cipher replaces one symbol with another.
- If the symbols in the plaintext are alphabetic characters, we replace one character with another.

A substitution cipher replaces one symbol with another.

- The simplest substitution cipher is a shift cipher (additive cipher).

CAESAR CIPHER

- Use the additive cipher with encryption key k= 3 to encrypt the message "hello".

- Solution: apply the encryption algorithm to the plaintext, character by character:

Plaintext: h	→	Shift 3 characters down	→	ciphertext: k
Plaintext: e	→	Shift 3 characters down	→	ciphertext: h
Plaintext: l	→	Shift 3 characters down	→	ciphertext: o
Plaintext: l	→	Shift 3 characters down	→	ciphertext: o
Plaintext: o	→	Shift 3 characters down	→	ciphertext: r

The ciphertext is therefore "khoor".

CAESAR CIPHER

- Mathematically, map letters to numbers:

a	b	c	d	e	f	g	h	i	j	k	l	m
0	1	2	3	4	5	6	7	8	9	10	11	12

n	o	p	q	r	s	t	u	v	w	x	y	z
13	14	15	16	17	18	19	20	21	22	23	24	25

- Then the general Caesar cipher is:

$$c = \mathrm{E}_K(p) = (p + k) \bmod 26$$

$$p = \mathrm{D}_K(c) = (c - k) \bmod 26$$

PROBLEMS OF CAESAR CIPHER:

KEY	PHHW	PH	DIWHU	WKH	WRJD	SDUWB
1	oggv	og	chvgt	vjg	vqic	rctva
2	nffu	nf	bgufs	uif	uphb	qbsuz
3	meet	me	after	the	toga	party
4	ldds	ld	zesdq	sgd	snfz	ozqsx
5	kccr	kc	ydrcp	rfc	rmey	nyprw
6	jbbq	jb	xcqbo	qeb	qldx	mxoqv
7	iaap	ia	wbpan	pda	pkcw	lwnpu
8	hzzo	hz	vaozm	ocz	ojbv	kvmot
9	gyyn	gy	uznyl	nby	niau	julns
10	fxxm	fx	tymxk	max	mhzt	itkmr
11	ewwl	ew	sxlwj	lzw	lgys	hsjlq
12	dvvk	dv	rwkvi	kyv	kfxr	grikp
13	cuuj	cu	qvjuh	jxu	jewq	fqhjo
14	btti	bt	puitg	iwt	idvp	epgin
15	assh	as	othsf	hvs	hcuo	dofhm
16	zrrg	zr	nsgre	gur	gbtn	cnegl
17	yqqf	yq	mrfqd	ftq	fasm	bmdfk
18	xppe	xp	lqepc	esp	ezrl	alcej
19	wood	wo	kpdob	dro	dyqk	zkbdi
20	vnnc	vn	jocna	cqn	cxpj	yjach
21	ummb	um	inbmz	bpm	bwoi	xizbg
22	tlla	tl	hmaly	aol	avnh	whyaf
23	skkz	sk	glzkx	znk	zumg	vgxze
24	rjjy	rj	fkyjw	ymj	ytlf	ufwyd
25	qiix	qi	ejxiv	xli	xske	tevxc

PROBLEMS OF CAESAR CIPHER:

- If it is known that a given cipher text is a Caesar cipher, then a brute-force cryptanalysis is easily performed: simply try all the 25 possible keys.
- The last figure shows the results of applying this strategy to the example cipher text.
- In this case, the plaintext leaps out as occupying the third line.
- The language of the plaintext is known and easily recognizable.

2.MONOALPHABETIC SUBSTITUTION CIPHER

- Shuffle/scramble the letters and map each plaintext letter to a different random ciphertext letter:

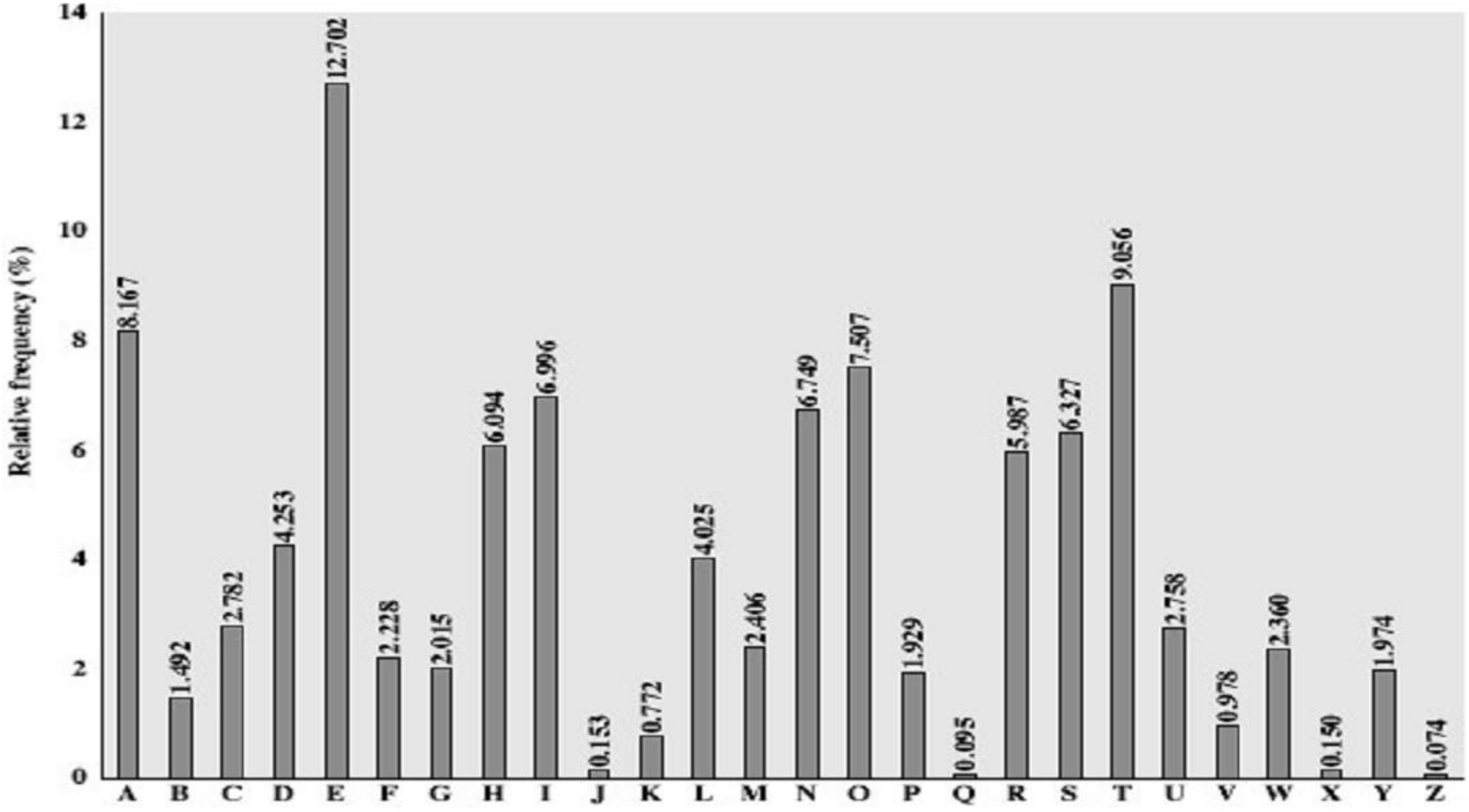
Plaintext	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Ciphertext	D	K	V	Q	F	I	B	J	W	P	E	S	C	X	H	T	M	Y	A	U	O	L	R	G	Z	N

- Plaintext: ifwewishtoreplaceletters
- Ciphertext: WIRFRWAJUHYFTSDVFSFUUFYA

LANGUAGE STATISTICS AND CRYPTANALYSIS

- Now have a total of 26! = 4 x 10^26 keys.
- with so many keys, might think is secure, but would be !!!WRONG!!!
- Problem is language characteristics.
- Human languages are not random.
- Letters are not equally frequently used.
- In English, E is by far the most common letter, followed by T, ……
- Other letters like Z, J, K, Q, X are fairly rare.

Classic Encryption Cryptanalysis using Letter Frequencies



3.POLYALPHABETIC CIPHERS

- These techniques have the following features in common:

1. A set of related monoalphabetic substitution rules is used.
2. A key determines which particular rule is chosen for a given transformation.

VIGENÈRE CIPHER

- The Vigenere cipher uses this table together with a keyword to encipher a message.
- For example, suppose we wish to encipher the plaintext message:

I WILL COME TOMORROW

- Using the keyword BEE. We begin by writing the keyword, repeated as many times as necessary, above the plaintext message.

VIGENÈRE CIPHER

- To derive the ciphertext using the tableau, for each letter in the plaintext, one finds the intersection of the row given by the corresponding keyword letter and the column given by the plaintext letter itself to pick out the ciphertext letter.
- Plaintext: IWILLCOMETOMORROW
- Keyword: BEEBEEBEEBEEBEEBE
- Ciphertext: JAMMRGPQIUSQPVVPA

	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

VIGENÈRE CIPHER

- A general equation of the encryption process is:

$$C_i = (p_i + k_{i \bmod m}) \bmod 26$$

- Similarly, a general equation of the decryption process is:

$$p_i = (C_i - k_{i \bmod m}) \bmod 26$$

ON TIME PAD (UNBREAKABLE CIPHER)

- It is a Vigenere cipher with key length equal to the of the plaintext.
- The key must be chosen in a completely random way and can only be used once.
- It produces random output that bears no statistical relationship to the plaintext.
- The one time pad is the only cryptosystem that exhibits what is referred to as perfect secrecy.

ON TIME PAD (UNBREAKABLE CIPHER)

- Messages encrypted with keys based on randomness have the advantage that there is theoretically no way to break the code by analyzing a succession of messages.
- Each encryption is unique and bears no relation to the next encryption, making it impossible to detect a pattern.
- But with a one-time pad, the decrypting party must have access to the same key used to encrypt the message; this raises the issue of how to get the key to the decrypting party safely, or how to keep both keys secure.

ON TIME PAD

- A One Time Pad (OTP) is the only potentially unbreakable encryption method. Plain text encrypted using an OTP cannot be retrieved without the encrypting key. However, there are several key conditions that must be met by the user of a one time pad cipher, or the cipher can be compromised.

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
0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25

E	4	K	10
N	13	E	4
I	8	Y	24
G	6	W	22
M	12	O	
A	0	R	

plain text: ENIGMA

keyword: KEYWORD

OTP LIMITATIONS

- There is the practical problem of making large quantities of random keys.
- Even more daunting is the problem of key distribution and protection.

CONTENTS

MODERN SYMMETRIC-KEY CIPHERS

- Since traditional ciphers are **no longer secure**, modern symmetric-key ciphers have been developed during the last few decades.
- **Modern ciphers** normally use a combination of substitution, transposition and some other complex transformations to create a ciphertext from a plaintext.
- Modern ciphers are bit-oriented (instead of character oriented).
- The plaintext, ciphertext and the key are **strings of bits**.

Data Encryption Standard (DES)

DATA ENCRYPTION STANDARD (DES)

- DES is a block cipher.
- (Plaintext and Ciphertext size= 64 bits)
- Master Key of size 64 bits.
- The efficient length of the key is 56 bits.
- Brute force attack will try 2^{56} possible key.
- 16 Round.
- 16 subkeys of length 48 bits.

Simplified DES
(S-DES)

SIMPLIFIED DES

- S-DES is a block cipher.
- (Plaintext and Ciphertext size= 8 bits)
- Master Key of size 10 bits.
- Brute force attack will try 2^{10} possible key.
- 2 Round.
- 2 subkeys of length 8 bits.

Important Functions:

IMPORTANT FUNCTIONS:

XOR:

$$C = A \oplus B$$

$$0 = 1 \oplus 1$$

Inverse:

$$A = C \oplus B$$

$$1 = 0 \oplus 1$$

Permutation:

P=[2 3 1 4]

If I/p of P: 1101

O/p of P: 1011

Inverse:

P^{-1}=[3 1 2 4]

If I/p of P^{-1}: 1011

O/p of P^{-1}: 1101

IMPORTANT FUNCTIONS:

E/P Expansion and Permutation:

E/P=[2 3 1 4 4 1 2 3]

If I/p of E/P: 1101

O/p of E/P: 10111110

Inverse:

E/P^{-1}=[3 1 2 4]

Or E/P^{-1}=[6 7 8 5]

Or E/P^{-1}=[3 7 2 5]

Or E/P^{-1}=[6 1 8 4]

If I/p of E/P^{-1}: 10111110

O/p of E/P^{-1}: 1101

IMPORTANT FUNCTIONS:

Permutation Choice:

PC=[4 5 7 10 2 3 6 9]

If I/p of PC: 0111111110

O/p of PC:11101111

Inverse:

PC^{-1}=[x 5 6 1 2 7 3 x 8 4]

If I/p of PC^{-1}: 11101111

O/p of PC^{-1}: x111111x10

IMPORTANT FUNCTIONS:

Left Shift (LS-n):

Ex. LS-2:

If I/p of LS-2 is: 1101

O/p of LS-2 is:

1101

1011

0111

Inverse (Right) Shift (RS-n):

Ex. RS-2:

If I/p of RS-2 is: 0111

O/p of RS-2 is:

0111

1011

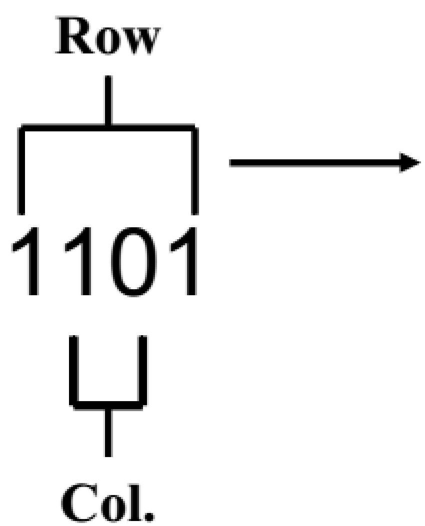
1101

IMPORTANT FUNCTIONS:

S-Boxes:

If i/p of S-box is: 1101

The o/p of S-box is: 11



$$S0 = \begin{array}{c} \\ 0 \\ 1 \\ 2 \\ 3 \end{array} \begin{array}{c} \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$$

IMPORTANT FUNCTIONS:

S-Boxes:

It is a nonlinear function

If o/p of S-box is: 11

The i/p of S-box is:

0100

0001

1110

1001

1101

$$S0 = \begin{array}{c c} & \begin{array}{cccc} 0 & 1 & 2 & 3 \end{array} \\ \begin{array}{c} 0 \\ 1 \\ 2 \\ 3 \end{array} & \begin{bmatrix} 1 & 0 & 3 & 2 \\ 3 & 2 & 1 & 0 \\ 0 & 2 & 1 & 3 \\ 3 & 1 & 3 & 2 \end{bmatrix} \end{array}$$

IMPORTANT FUNCTIONS:

- Concatenation (||):

If A=00 and B= 10

C= A || B

C= 0010