Cryptographic Techniques (Unit-5)

Nithya Mam, CSPC53 Networks

Cryptography – secured writing, how data is going to be transmitted securely.

Transmitter – has its own data, and it needs to be transmitted across some medium. (Assume that the transmission media is not same).

After the original message is transmitted, the transmitter must perform the encryption operation. Input is the plain text (original message needed to be transmitted), which is given to the encryption function. The function gives output as the cipher text (encrypted text) unknown to 3rd parties.

The receiver must do the reverse operation – decryption. Input: cipher text and output: plain text. Thus, data is securely transmitted.

Issues with this secure transmission: Encryption and decryption algorithm must be known to both parties and these algorithms use several keys. In some techniques the keys need to be distributed in advance. How to generate and distribute the key to ensure higher security – key generation, key distribution and key management are very hard to do.

Symmetric Cryptographic Techniques: Only one secret key is shared between the source and destination. If this key is known to a 3rd party, then data transmission will not be secure. The same secret key is used in the encryption and decryption algorithms.

Asymmetric Cryptographic Techniques: Two keys are present – public key and private key. The public key is known to all, while the private key is only known to the individual. The public key is used by the encryption algorithm, while the private key is used by the decryption algorithm. Each node in the network has its own set of public and private key pairs.

Traditional Cryptographic Techniques: Character oriented symmetric cryptographic technique, not used currently.

Modern Cipher Cryptographic Techniques: (bit oriented)

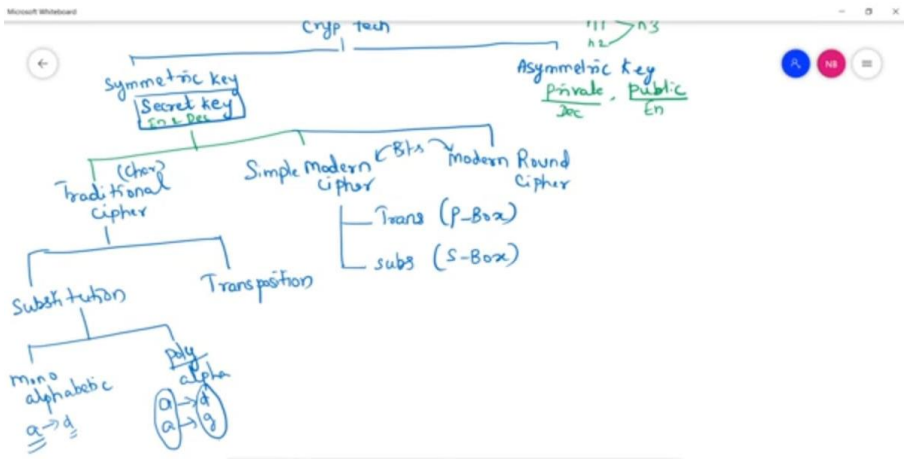
Modern Round Cipher Cryptographic Techniques: (bit oriented) frequently used.

Substitution: Substitute one character with another character.

Transposition: No changing of characters, but position of the characters is altered. Eg: ABCD becomes CBDA.

Monoalphabetic Substitution: Each occurrence of a character ‘x’ is replaced by a distinct character ‘y’.

Polyalphabetic Substitution: a -> d, next time a -> g.



MONOALPHABETIC SUBSTITUTION

Encryption

Plain Text: TEXT, Key = 3, then Cipher Text: WHAW (move right by 3 characters)

Decryption

Cipher Text: WHAW, Key = 3, then Plain Text: TEXT

C = E(P) function = (P+K) mod 26 [because here Z will map to C]

P = D(C) function = (C-K) mod 26

PT -> az, key = 3, then CT -> dc [(0+3) % 26=3 and (25+3) % 26 = 2]

CT -> dc, key = 3, then PT -> az [(3-3) % 26=0 and (2-3) % 26 = 25]

POLYALPHABETIC SUBSTITUTION

	a	*b*	*c*	*d*	…	…	*y*	*z*
a	a	b	c	d	…	…	y	z
b	b	c	d	e	…	…	z	a
c	c	d	e	f	…	…	a	b
d	d	e	f	g	…	…	b	c
…	…	…	…	…	…	…	…	…
…	…	…	…	…	…	…	…	…
y	y	z	a	b	…	…	w	x
z	z	a	b	c	…	…	x	y

Encryption: k = b c x y (column) and plain text = a b c d b c (row)

PT	a	b	c	d	b	c
Key	*b*	*c*	*x*	*y*	*b*	*c*
CT	b	d	*z*	b	c	e

Decryption: in the key column, search for occurrence of the cipher text – the plain text is the corresponding text in the row

Transposition: Permutations of the words are formed (rearrangement). Key controls the method of rearrangement.

Encryption: Plain Text: COMPUTERNETWORKS, key = 4312

1	2	3	4		4	3	1	2
C	O	M	P		P	M	C	O
U	T	E	R		R	E	U	T
N	E	T	W		W	T	N	E
O	R	K	S		S	K	O	R

Cipher Text: PMCOREUTWTNESKOR (read row by row)

Decryption: Arrange in columns and sort the columns number wise, and then again read row-wise.

SIMPLE MODERN CIPHER [p-box]

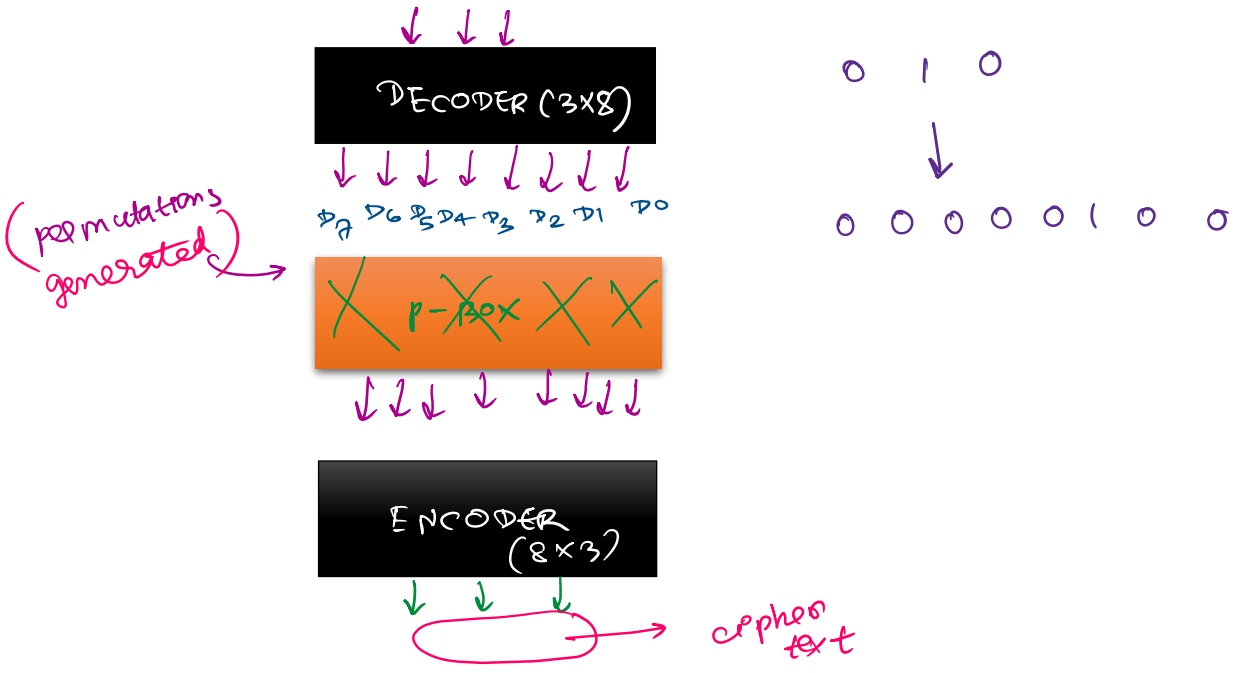
Permutation is again done, and position of bits is changed according to the key.

Encryption: Plain Text: 100011, key = 245163, Cipher Text: 001110

Decryption: Sort the cipher text based on the key to get the plain text.

S-BOX MODERN CIPHER (using encoder and decoder)

Decoder: n bit input gives 2^n output bits. Eg 3x8 decoder.
Encoder: 2^n input bits give n bit output. Eg 8x3 encoder.



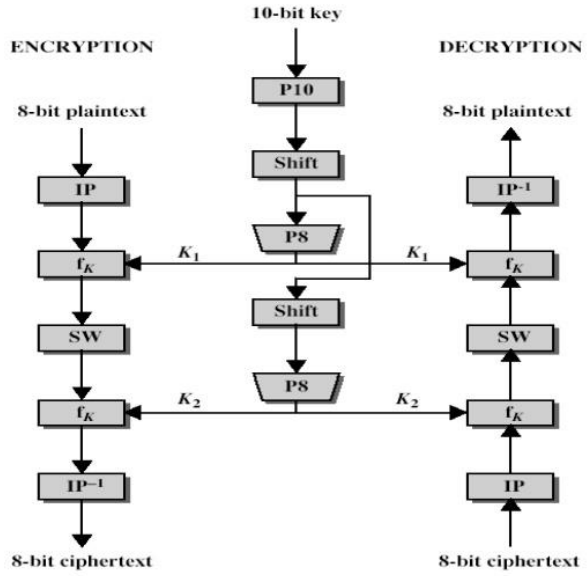
p-box and s-box are not frequently used as a single technique as it can be easily compromised. It is used in modern round cipher as a part of the whole cryptographic process.

MODERN ROUND CIPHER

1. DES (Data Encryption Standard)

2. AES (Advanced Encryption Standard)

S-DES is a simplified DES algorithm used for simplified study purposes.



DES: 64-bit plain text + 5 bit key, f(k) needs to be done 16 times

S-DES: 8-bit plain text, f(k) needs to be done 2 times.

AES: 128-bit plain text + (128, 256 or 192) bit key

IP: Initial Permutation, *f(k)*: Permutation + Substitution

The 10-bit key generates 2 keys – k1 and k2

SW: Switching, data from 2 halves are switched (interchanged).

Then again f(k) is done with a different key, then inverse initial permutation is done.

Key Generation

10-bit key is given to a permutation of size 10, and some circular shifting operation is done. Then it is given to Permutation P8.

Size of input and output permutations remains the same (10 bits) in encryption and decryption. But in the middle, 10 bit becomes 8 bit in P8 (therefore the box shape is a bit different).

The shifted output is k1. This is again shifted and permuted to get k2.

Equations

k1 = P8(shift(P10(key)))

k2 = P8(shift(shift(P10(key))))

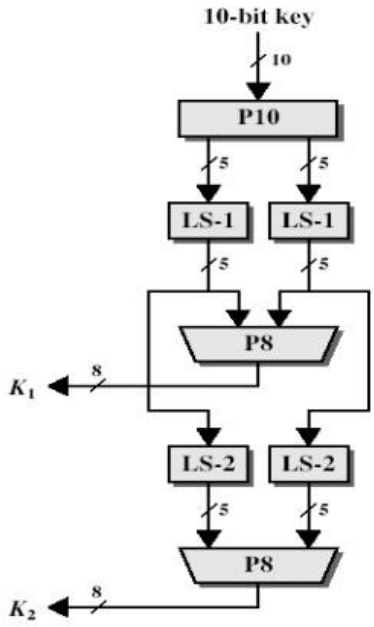
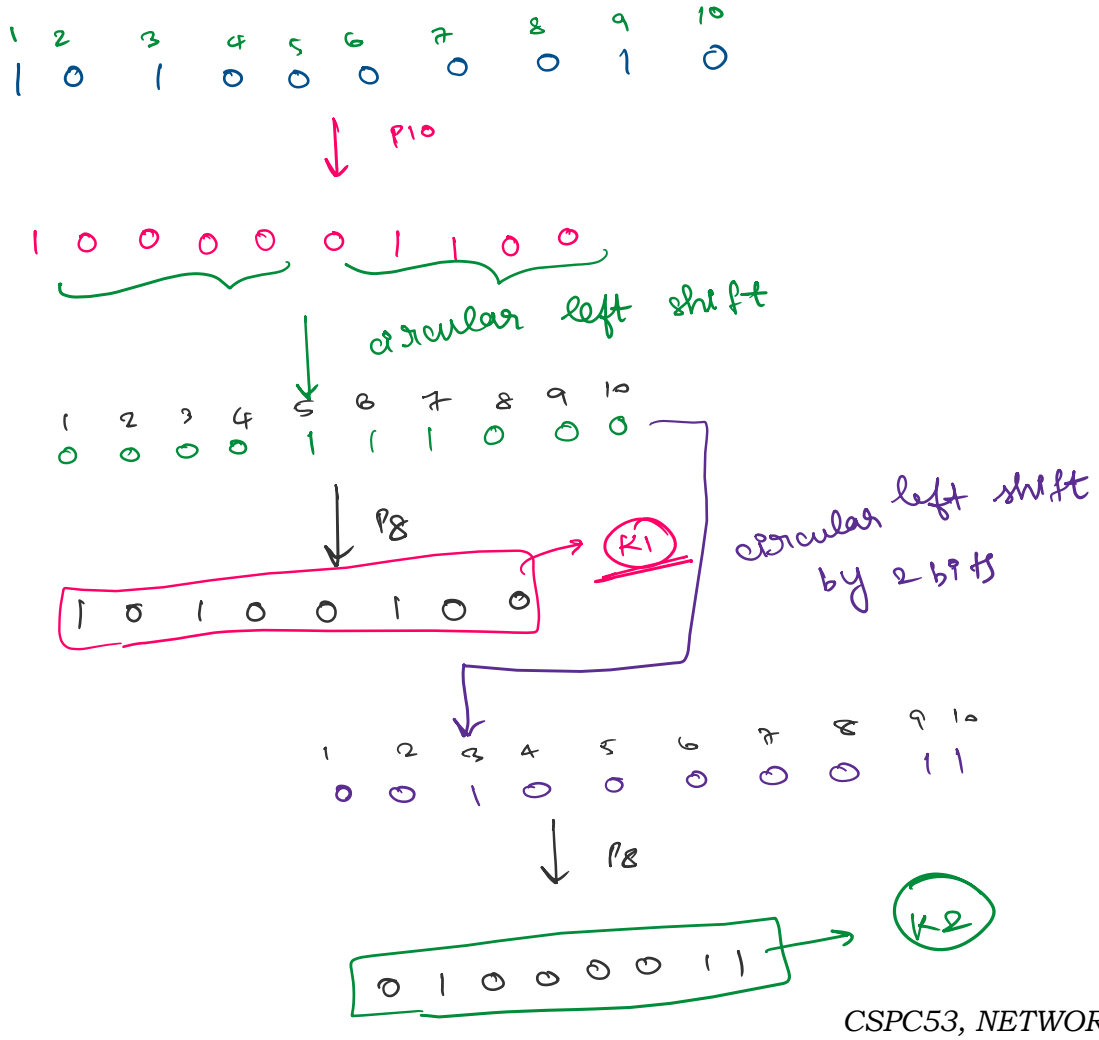
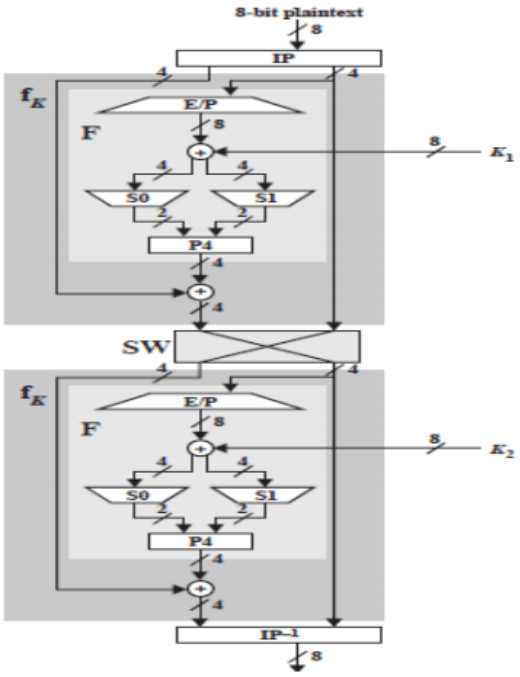


Figure: key generation for S-DES

Question: P10 is given as 3 5 2 7 4 10 1 9 8 6 and P8 is given as 6 3 7 4 8 5 10 9. Key is 1010000010. Find k1 and k2.





Initial Permutation: 2 6 3 1 4 8 5 7, Inverse Initial Permutation: 4 1 3 5 7 2 8 6

Expansion Permutation: 4 1 2 3 2 3 4 1

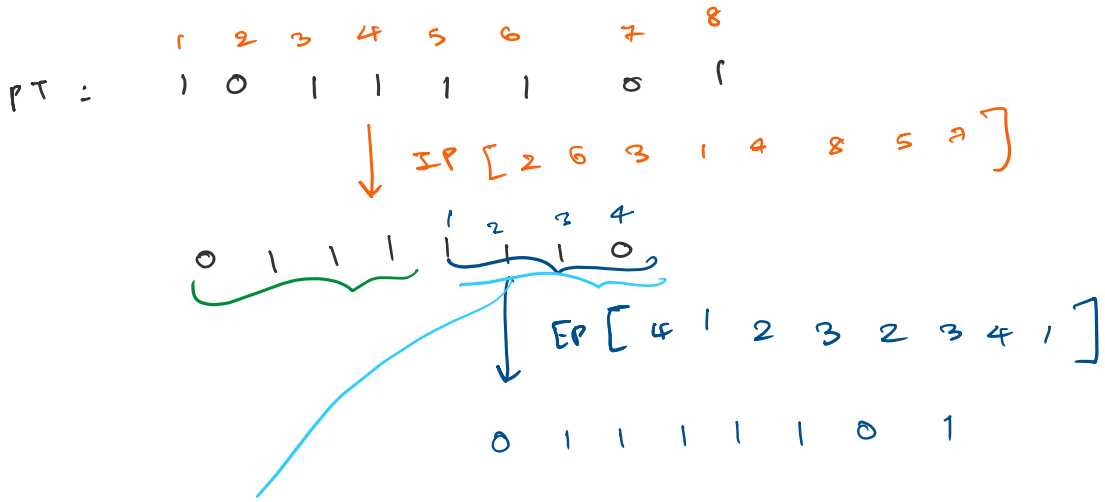
S0	1	0	3	2	S1	0	1	2	3
	3	2	1	0		2	0	1	3
	0	2	1	3		3	0	1	0
	3	1	3	2		2	1	0	3

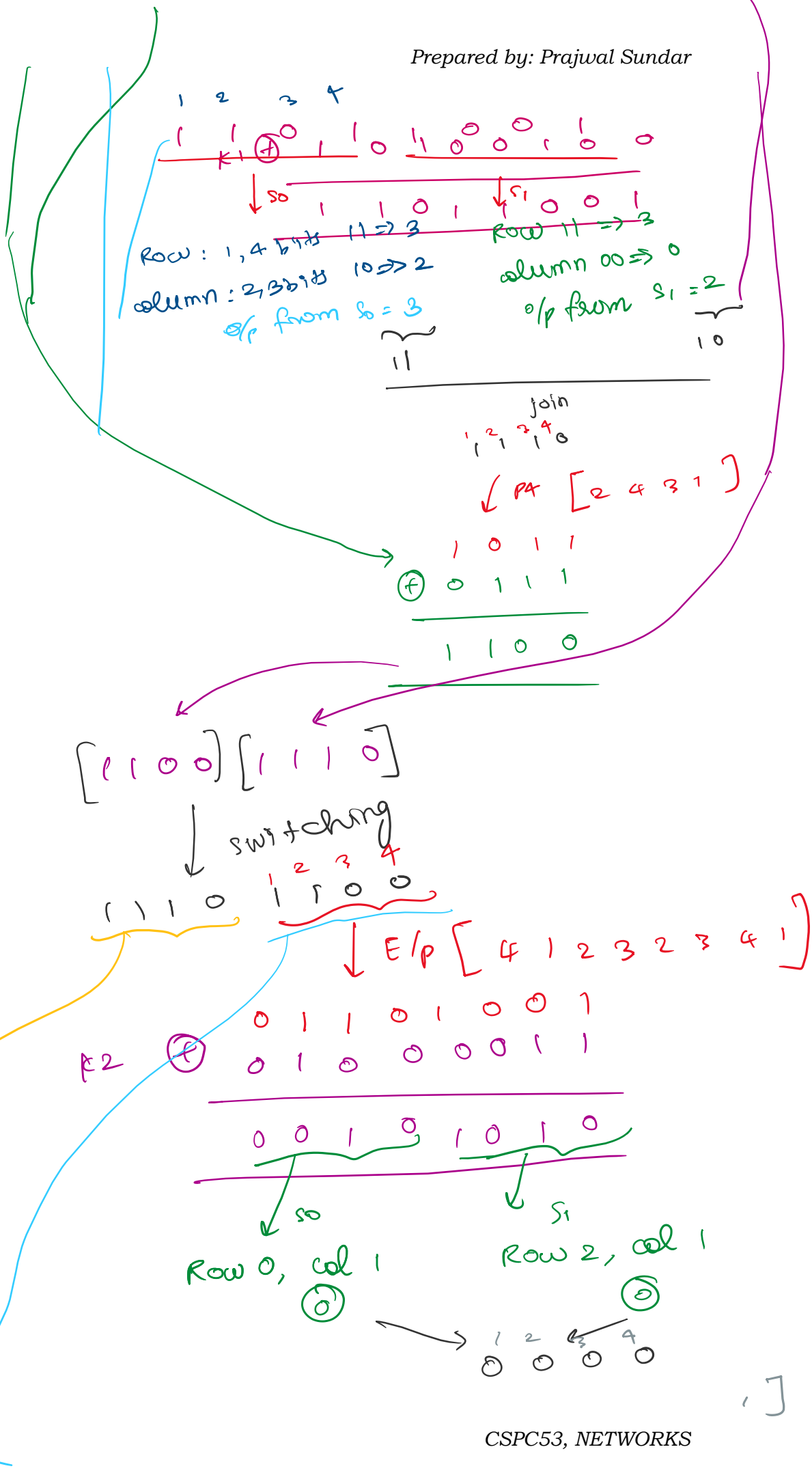
P4: 2 4 3 1

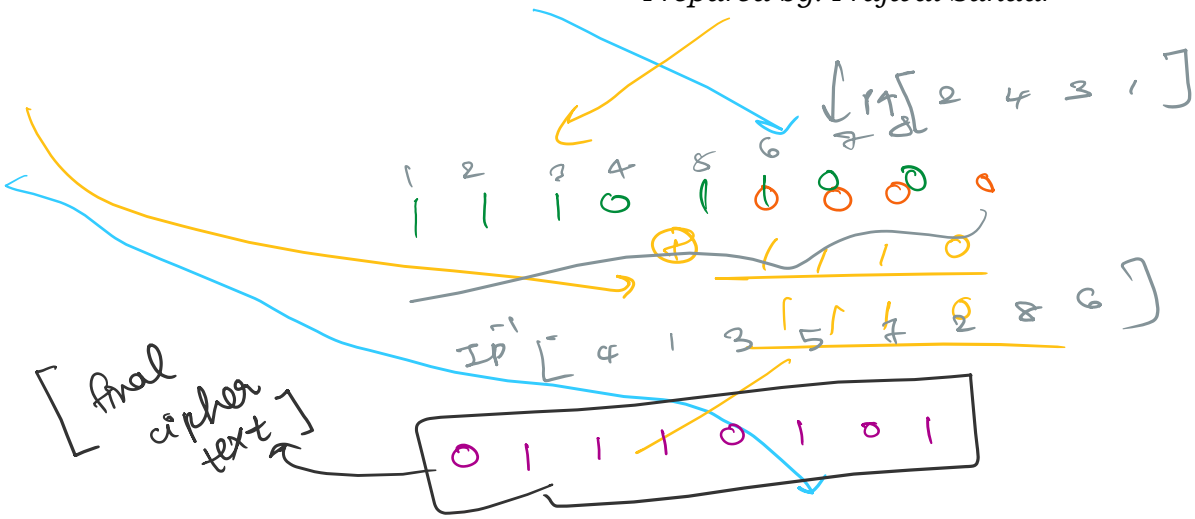
k1 (calculated from key generation): 1 0 1 0 0 1 0 0.

k2 (calculated from key generation): 0 1 0 0 0 0 1 1.

Plain Text: 1 0 1 1 1 1 0 1 -> encrypt this data using simple DES encryption technique.




1 2 3 4
1 1 0 1 1 0 0 1 0
K1
f
S0
S1
Row : 1, 4 bits 11 => 3
column : 2, 3 bits 10 => 2
o/p from S0 = 3
11
Row 11 => 3
column 00 => 0
o/p from S1 = 2
10
join
1 2 3 4
1 1 1 0
PA [2 4 3 1]
1 0 1 1
f
0 1 1 1
1 1 0 0
[1 1 0 0] [1 1 1 0]
switching
1 2 3 4
1 1 1 0 1 1 0 0
E/p [4 1 2 3 2 3 4 1]
0 1 1 0 1 0 0 1
K2
f
0 1 0 0 0 0 1 1
0 0 1 0 1 0 1 0
S0
S1
Row 0, col 1
Row 2, col 1
1 2 4
0 0 0 0



Asymmetric Cryptographic Techniques: RSA Algorithm, Diffie-hellman algorithm