INDIAN INSTITUTE OF ENGINEERING SCIENCE AND TECHNOLOGY, SHIBPUR

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

B. TECH (CST), 6TH SEMESTER, MID TERM EXAMINATION, 2022

INFORMATION SECURITY AND CRYPTOGRAPHY [CS 3204]

Date: 10/03/2022

Name: Abhiroop Mukherjee

Examination Roll No.: 510519109

G Suite ID: 510519109.abhirup@students.iiests.ac.in

No. of Sheets uploaded: 11

(Q3)a) given 10 bit initial key → (10100 00010)

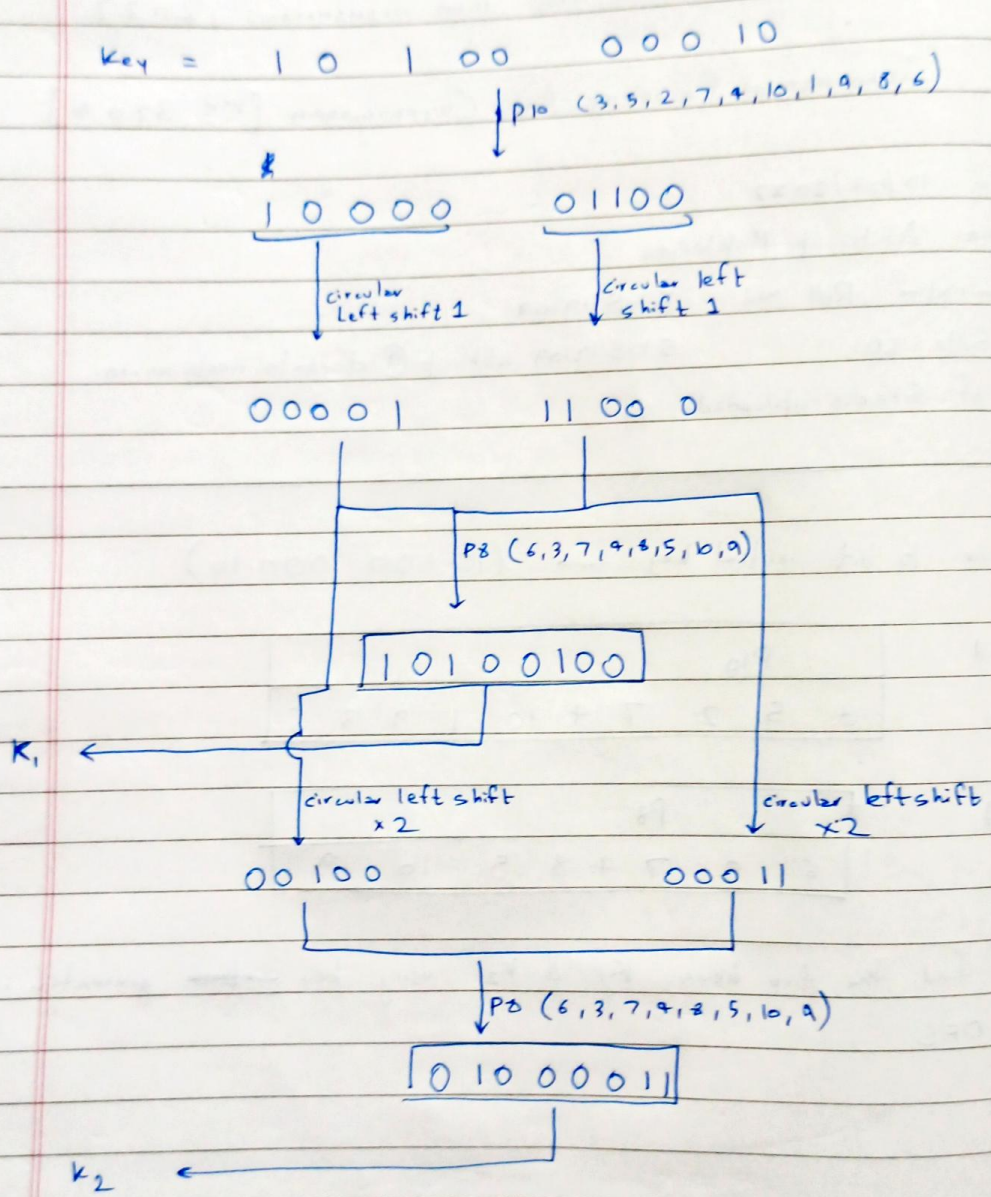
and

P10									
3	5	2	7	4	10	1	9	8	6

and

P8							
6	3	7	4	8	5	10	9

to find the two keys K_1 & K_2 using key ~~expansion~~ generation in S DES.

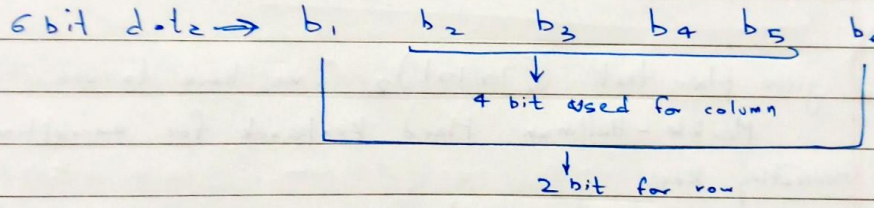

Key = 1 0 1 0 0 0 0 0 1 0
P10 (3, 5, 2, 7, 4, 10, 1, 9, 8, 6)
1 0 0 0 0
0 1 1 0 0
circular Left shift 1
circular left shift 1
0 0 0 0 1
1 1 0 0 0
P8 (6, 3, 7, 4, 8, 5, 10, 9)
1 0 1 0 0 1 0 0
K1
circular left shift x 2
circular left shift x2
0 0 1 0 0
0 0 0 1 1
P8 (6, 3, 7, 4, 8, 5, 10, 9)
1 0 1 0 0 0 1 1
K2

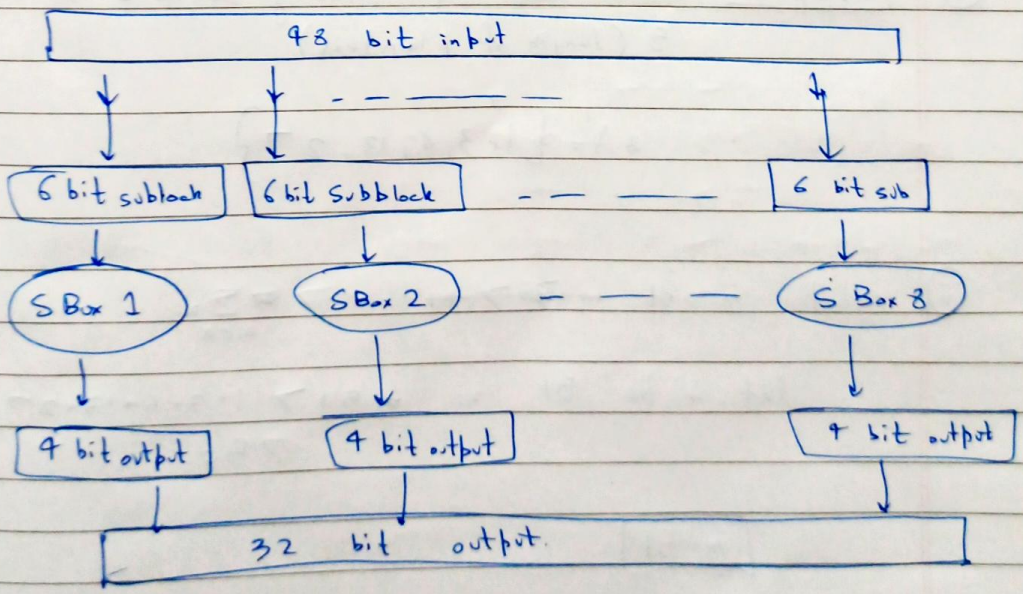
b) S Box Substitution in DES

→ here we use 8 S-Boxes of ~~si~~ with 4 rows & 16 columns ~~to get a bit~~ which takes 6 bit input & gives us 4 bit output.

i) ~~do~~ we ~~divide~~ divide 48 bit input to S-Box as eight 6 bit data.

ii) for each 6 bit data, we substitute them using coressponding Sbox as follows





(c) S Box Transformation (and the XOR done with key just before) is an important part of DES because of the following reasons

(i) The key is used in this phase, which is the first part about DES and is important for encryption

(ii) S Box Transformation is also a substitution part of DES which obfuscate every thing we get from XOR of data & key. This makes harder for key to get discovered.

Q4 given plain text $(10101)_2$, we have to use Merkle - Hellman Hard knapsack for encryption & decryption

(I) Generating Keys

(i) Assumption: We use super increasing sequence of length 5 (length of plain text)

$$A' = \{1, 3, 6, 13, 27\}$$

(ii) select m s.t. $m > \sum_{a_i \in A'} a_i$

let m be 51 as $51 > 1+3+6+13+27$

$$51 > 50$$

$\boxed{m = 51}$

(a)

(iii) select w s.t. $\gcd(m, w) = 1$

Factors of $51 = 3, 17$

lets take w as 7 $\rightarrow$ $\boxed{w = 7}$ as $\gcd(51, 7) = 1$

(iv) Find w^{-1}, multiplicative inverse of $w \pmod m$

$$w^{-1} = \frac{mn+1}{w}, \quad w^{-1} \text{ should be an integer}$$

$n=1 \rightarrow w^{-1} = \frac{51\times1+1}{7} = \frac{52}{7} \rightarrow$ fraction

$n=2 \rightarrow w^{-1} = \frac{51\times2+1}{7} = \frac{103}{7} \rightarrow$ fraction

$n=3 \rightarrow w^{-1} = \frac{51\times3+1}{7} = \frac{154}{7} = 22$

$\therefore \boxed{w^{-1} = 22}$

(v) generate public key

$$A = \left\{ \begin{array}{l} 7\times1 \pmod{51}, \\ 7\times3 \pmod{51}, \\ 7\times6 \pmod{51}, \\ 7\times13 \pmod{51}, \\ 7\times27 \pmod{51} \end{array} \right\} = \{7, 21, 42, 40, 36\}$$

(vi) Public key = A = {7, 21, 42, 40, 36}

Private key → [A^{-1} = {1, 3, 6, 13, 27}, m = 51, w = 7, w^{-1} = 22]

(II) Encryption of $(1010)_2$ using public key A

C (ciphertext) = ~~34~~ 7 + 0×21 + 1×42 + 0×40 + 1×36

= 7 + 42 + 36

= 85

C = 85 given to host (receiver)

(III) decryption of C using Private key.

(i) $(85 \times 22) \bmod 51 = 1870 \bmod 51 = 34$

(C, w^{-1}, m)

(ii)

	34 ≥ 27	→ ✓	→ 1
34 − 27 = 7	7 ≥ 13	→ ✗	→ 0
	7 ≥ 6	→ ✓	→ 1
7 − 6 = 1 →	1 ≥ 3	→ ✗	→ 0
	1 ≥ 1	→ ✓	→ 1

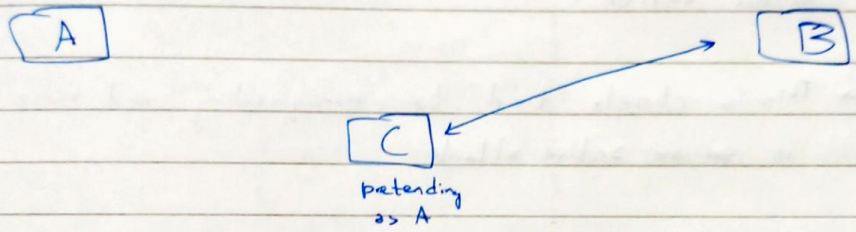
Plain text received = 1010

← same as plain text encrypted

6

(Q1) a) Masquerade

→ Masquerade is a type of active attack which takes place when one entity pretends to be other



Eg: suppose C captured A's authentication sequences. Later C might give those sequence to B & pretent to get inside B as A.

b) Fabrication Prevention

→ Fabrication can be prevented by :

1. Use of Authentication and Authorization Mechanism
2. Use of Digital Signatures to provide authenticity of data.
3. Use of Fire walls to allow only certain people.

(c) Packet Spoofing

→ Packet Spoofing is an attack where attacker sends packet with different source address (than it's own address). and hence try to pretend to be some other entity

→ This is closely tied to masquerading and hence is an active attack

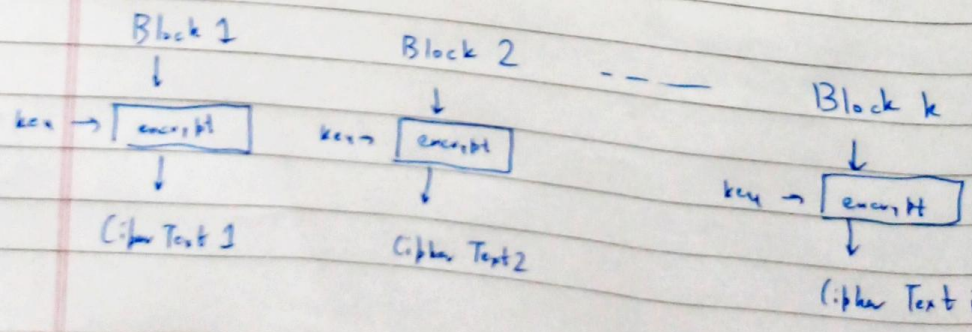
Q2) a) Algorithm mode

→ Algorithm mode defines the the details of the algorithm which will be used for encryption & decryption

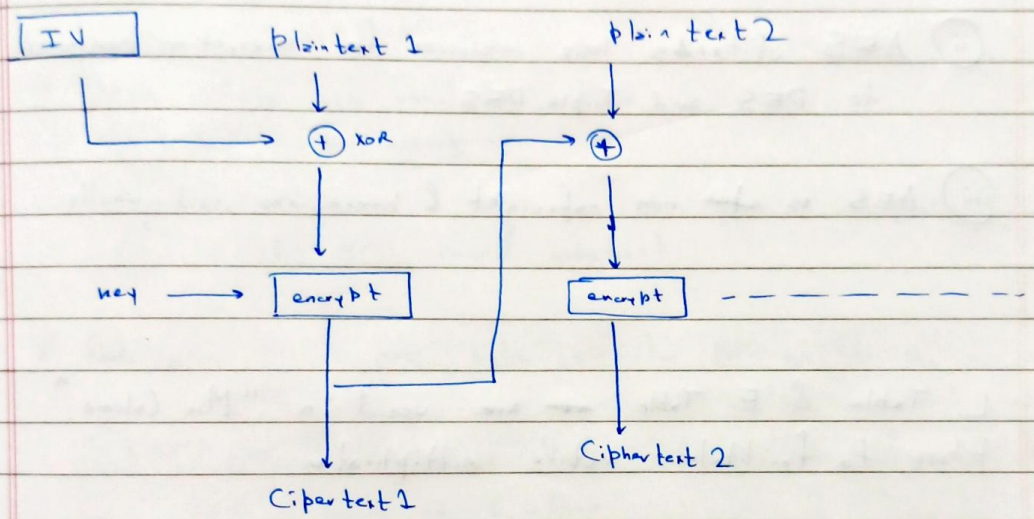
→ Defined after Algorithm Type is decided.

(b) → Electronic Code Book uses same key for decryption/encryption of data, hence the cipher text will have similar patterns as plain text

→ A cryptanalyst can easily indentify these patterns in cipher text & may crack the key of this algorithm



(c) Cipher Block Chaining (CBC) solves the problem by changing the key ~~everytime~~ for every block encryption as per the data being encrypted. This solves the same key problem of Electronic Code Book



Q5) a) AES became popular than DES because

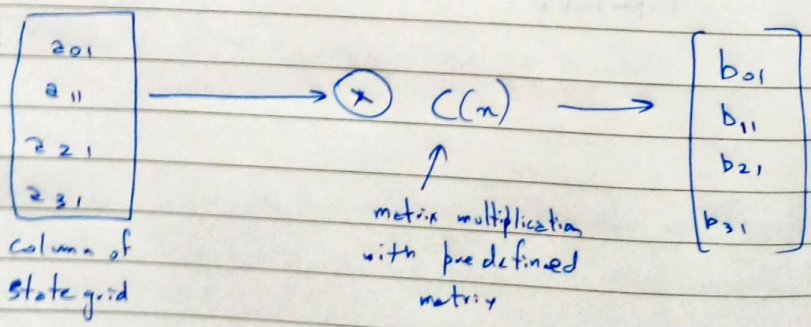
(i) AES is harder to crack than DES due to support for larger key size

(ii) AES utilizes less resources for encryption compared to DES and Triple DES.

(iii) AES is non copyright & hence was used globally.

b) L Table & E Table are used in "Mix Column" phase to facilitate matrix multiplication.

Eg:



→ L Table & E Table are basically a look up table which is used to transform result of matrix multiplication to resultant column.

(c) → In key expansion given 128 bit cipher key is stored in 4×4 byte matrix

→ 4 column of key matrix is expanded into 44 words resulting in 11 key rounds

→ These steps are used to achieve it

(i) Rot Word
(ii) Sub Word
(iii) XOR with round constant

★ Rot word → A one byte circular left shift on a word

Sub word → Performs a byte substitution on each byt using an S-Box

~~XOR~~ → round constant is fixed based on round no.