Roll No. _____

Pandit Deendayal Energy University

(Formerly Pandit Deendayal Petroleum University)

Mid Semester Examination - September 2022

B. Tech. (Computer Science & Engineering)

Semester - V

Date: 27.09.2022

Course Name : Information Security | **Time: 2 hours**

Course Code : 20CP304T | **Max. Marks: 50**

Instructions:

1. Do not write anything other than your roll number on question paper.
2. Assume suitable data wherever essential and mention it clearly.
3. Writing appropriate units, nomenclature, and drawing neat sketches/schematics wherever required is an integral part of the answer.

Ques. No.	Description	Marks	CO Mapped	BL
Q. 1	Distinguish between the following: i. Passive and Active attacks ii. Data authentication and Data confidentiality iii. Substitution and Transposition cipher iv. Stream cipher and Block cipher v. Cryptography and Steganography	02*5	CO-1	L-2
Q. 2	i. State Fermat's Theorem. ii. Solve the following equations for **X** **X**≡ 2 (mod 5) **X**≡ 3 (mod 7) **X**≡ 10 (mod 11)	2+8	CO-2	L-3
Q. 3	i. Construct playfair matrix with the key "ELEPHANT" ii. Demonstrate the playfair cipher by showing encryption on the plain text: "GREEN BALLOON" using the key in Q.3 i. iii. Identify two disadvantages of playfair cipher. iv. Give example of an autokey system. Name the cipher which makes use of this system.	2+4+2+2	CO-3	L-4
Q. 4	i. Describe fiestel cipher structure (encryption only) with a neat sketch. ii. Discuss avalanche effect. Also name any two encryption algorithms that perform strong avalanche effect.	05*2	CO-3	L-2
	OR			
	Describe Advanced Encryption Standard.	10	CO-3	L-2
Q. 5	i. Explain meet-in-the-middle attack? In which encryption model do we encounter this attack? ii. Choose another encryption model that can be used to counter meet-in-the-middle attack. Discuss the encryption and decryption steps in the chosen model using a neat sketch.	05*2	CO-3	L-4
	OR			
	Describe 5 block cipher modes of operations. Compare the strength and weakness of all modes.	10	CO-3	L-4

Information Security (20CP3041)
Mid Semester Exam (27-09-2022)
Solution

Q1. Distinguish between

i) **Passive attack**

An attack, that attempts to learn or make use of information from the system but does not affect system resources

Eg:- Release of message contents, traffic analysis

Active Attack

An attack that attempts to alter system resources or affect their operation

Eg:- Masquerade, Replay, Modification of message, Denial of service

ii) **Data authentication**

It is the assurance that the communicating entity is the one that it claims to be.

For Eg:- Checking the authenticity of an email is nothing but checking whether it actually came from the person it says.

Data confidentiality

It is the protection of data from unauthorized disclosure

Eg:- In email service, maintaining confidentiality means that only the sender and the receiver should be able to read the message. The contents should be kept secret from every other person, except for those two.

iii) Substitution cipher

In this technique, letters of the plaintext are replaced by other letters or by numbers or symbols.

Eg:- Caesar cipher, Monoalphabetic cipher, Playfair cipher, Hill cipher, Polyalphabetic cipher, One pad cipher

Transposition cipher

In this technique, there is no substitution. Instead, the position of letters or symbols are changed in the plain text to generate the cipher text

Eg:- Rail fence technique, columnar transposition.

iv) Stream cipher

Stream cipher is one that encrypts a digital data stream one bit or one byte at a time.

Eg:- Autokeyed Vigenere cipher, Caesar cipher.

Block cipher

Block cipher is one ~~that~~ in which a block of plaintext is treated as a whole, and used to produce a ciphertext block of equal length.

Eg:- Feistel cipher, DES, AES.

v) Cryptography

- Cryptography means secret writing
- Only secret message is hidden,
- Structure of data is altered
- Supports confidentiality, authentication, data integrity, and non-repudiation

Steganography

- Steganography means covered writing.
- The fact that a secret communication is taking place is hidden
- Structure of data is not usually altered
- supports confidentiality and authentication

Q2. i) Fermat's theorem

Let 'p' be a prime no. & 'a' is a positive integer not divisible by 'p'

then, $\boxed{a^{p-1} \equiv 1 \pmod{p}}$

ii) $X \equiv 2 \pmod 5$

$X \equiv 3 \pmod 7$

$X \equiv 10 \pmod{11}$

$a_1 = 2, \quad a_2 = 3, \quad a_3 = 10$

$m_1 = 5, \quad m_2 = 7, \quad m_3 = 11$

$M = m_1 m_2 m_3 = 5 * 7 * 11 = 385$

$M_1 = \frac{M}{m_1} = \frac{385}{5} = 77$

$M_2 = \frac{M}{m_2} = \frac{385}{7} = 55$

$M_3 = \frac{M}{m_3} = \frac{385}{11} = 35$

$(\underbrace{M_1}_{77} * M_1^{-1}) \bmod \underbrace{m_1}_{5} = 1 \quad \Rightarrow M_1^{-1} = 3$

$(\underbrace{M_2}_{55} * M_2^{-1}) \bmod \underbrace{m_2}_{7} = 1 \quad \Rightarrow M_2^{-1} = 6$

$(\underbrace{M_3}_{35} * M_3^{-1}) \bmod \underbrace{m_3}_{11} = 1 \quad \Rightarrow M_3^{-1} = 6$

$X = (a_1 M_1 M_1^{-1} + a_2 M_2 M_2^{-1} + a_3 M_3 M_3^{-1}) \bmod M$

$= [2(77)(3) + 3(55)(6) + 10(35)(6)] \bmod 385$

$= 3552 \bmod 385 = \boxed{87}$ Ans

3. i) Playfair key matrix

ELEPHANT

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

ii) GREEN BALLOON

Break it into digrams :-

GR , EX , EN , BA, LX , LO, ON

Cipher text for the respective pair of plaintext :-

Plain text	→	Ciphes text
GR	→	IQ
EX	→	PV
EN	→	NF
BA	→	DP
LX	→	PW
LO	→	EQ
ON	→	VF

Thus, the generated cipher text is "IQPVNFDPPW EQVF"

iii) Disadvantage of playfair cipher

- It only encrypts english alphabets A to Z.
- It is a weak cipher as it can be cracked by knowing the frequency of english alphabets. It does not offer diffusion, ie. hiding of relationship between the plaintext and cipher text.

Q. 3. iv) Autokey system is where the plaintext is appended after the keyword (until the length of the key is same as the length of the plain text) to form the key.

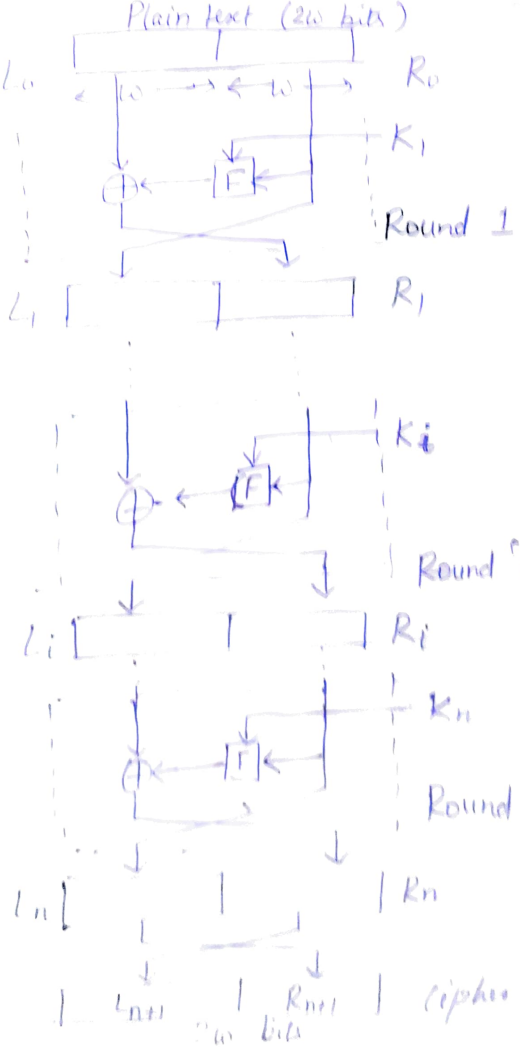
Eg: Keyword : DECEPTIVE

Plaintext : WEAREDISCOVEREDSAVEYOURSELF

Key : DECEPTIVEWEAREDISCOVEREDSA

Vigenere cipher makes use of this autokey system

Q4. i)



Encryption model of Feistel cipher structure

[illegible] effect is produced when a change in the plaintext or of the key produces a change in many bits of cipher text.

[illegible] property of any encryption algorithm.

e.g. Plain text : 0000000000000000000000000000000000000000

Cipher text : 4789FD476E82A5F1

Key : 22234512987ABB23

Plain text : 0000000000000000000000000000000000000001

Cipher text : 0A4ED5C15A63FEA3

Key : 22234512987ABB23

Although the two plaintext blocks differ only in the rightmost bit, the ciphertext block differs in 29 bits. This means that changing approximately 1.5% of the plaintext creates a change of approx. 45% in the ciphertext.

Data Encryption Standard (DES) and Advanced Encryption Standard (AES) perform strong avalanche effect.

OR

Q4. Advanced Encryption Standard

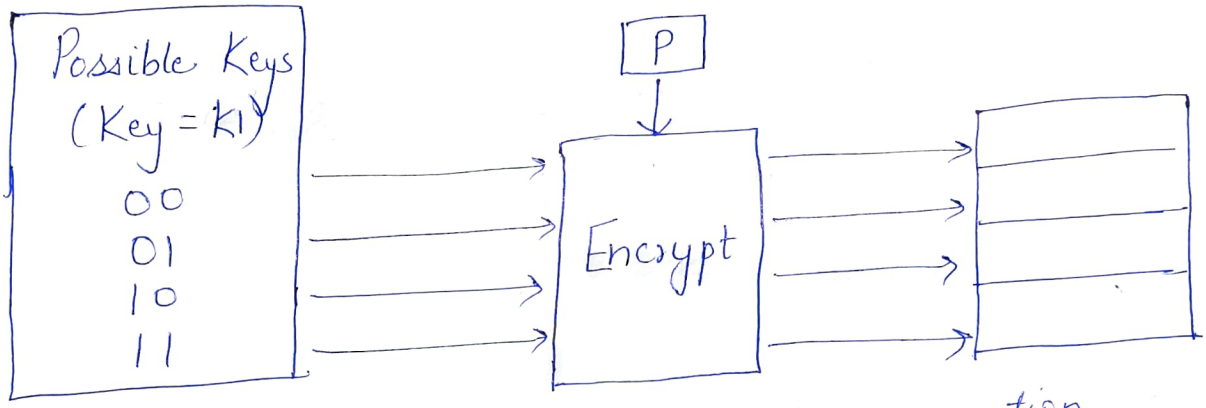
(Refer to "Cryptography and Network Security, Principles and Practice" by William Stallings, Ed. 7 (Chapter 6))

Q5. i) Meet in the middle attack involves encryption from one end, decryption from the other and matching the results in the middle.

Suppose cryptanalyst knows P and corresponding C. Now the aim is to obtain the values of K_1 and K_2.

Step 1

For all possible values (2^{56}) of key K_1, the cryptanalyst would encrypt the P by performing $E(K_1, P)$. The cryptanalyst would store output in a table.

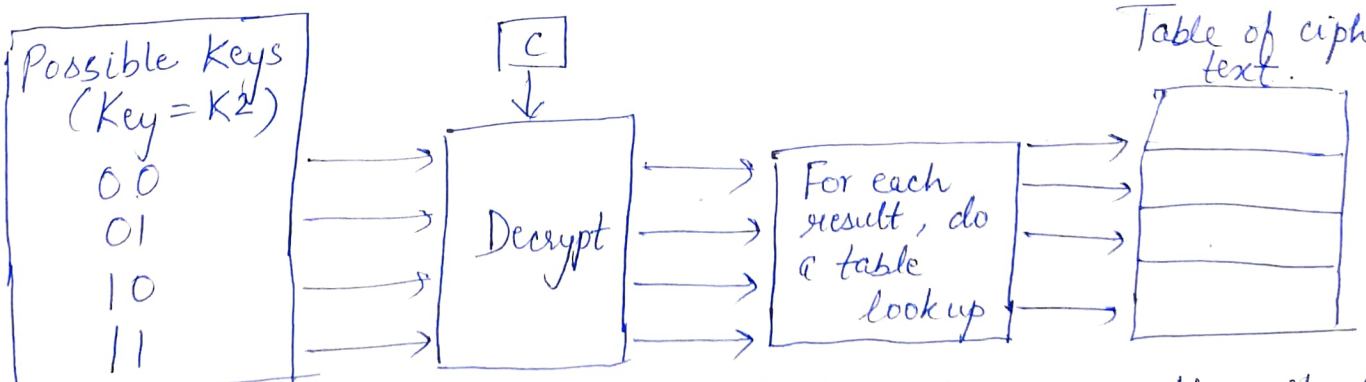


Cryptanalyst encryption operation

Step 2

Cryptanalyst decrypt the known C with all possible values of K_2.

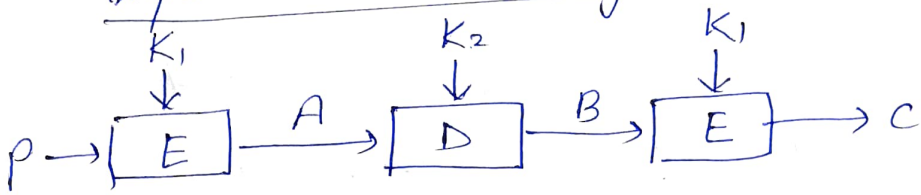
In each case, cryptanalyst will compare the resulting value with all values in the table of ciphertext



We encounter this attack in double data encryption standar

Q.5. ii) Triple Data Encryption Standard (DES) can be used to counter meet-in-the-middle attack.

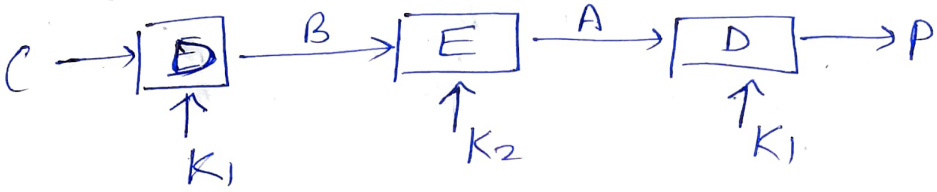
Triple DES with 2 keys



E: Encryption of DES
D: Decryption of DES

Encryption

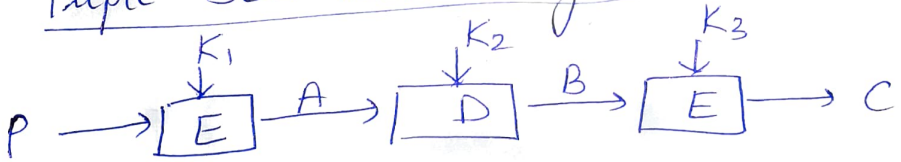
$$C = E(K_1, D(K_2, E(K_1, P)))$$



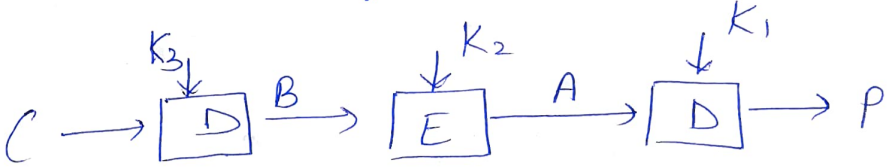
Decryption

$$P = D(K_1, E(K_2, D(K_1, C)))$$

Triple DES with 3 keys



Encryption



Decryption

$$C = E(K_3, D(K_2, E(K_1, P)))$$

$$P = D(K_1, E(K_2, D(K_3, C)))$$

OR

Q5. 5 block cipher modes of operations

[Refer to "Cryptography & Network Security, Principles & Practice" by William Stallings, Ed. 7 (Chapter 7)]