USN | | | | | | | | | | |

Internal Assessment Test 1- Oct. 2022

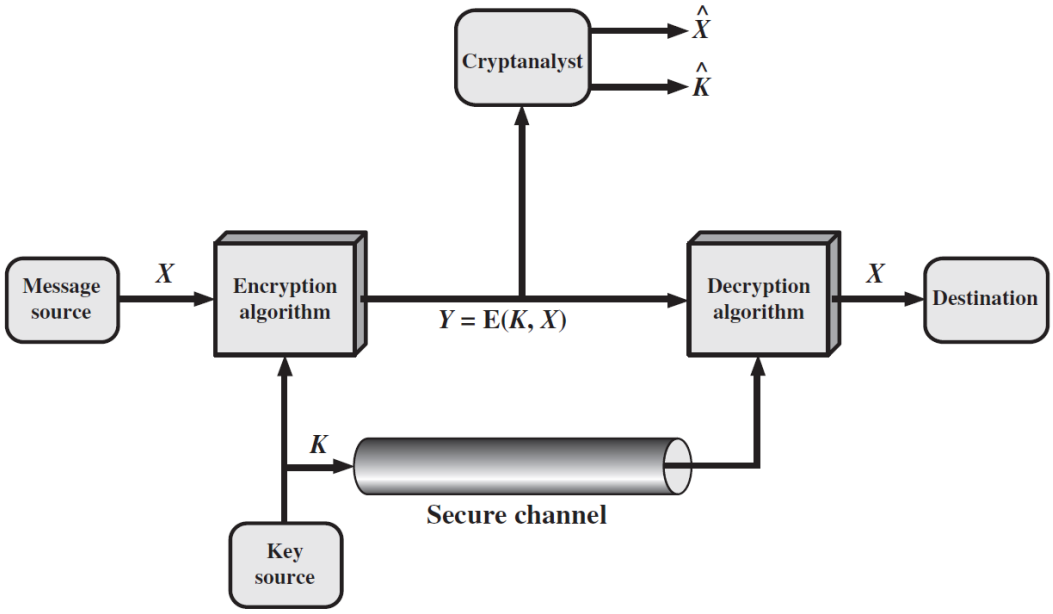
Sub:	Cryptography					Sub Code:	18CS744	Branch:	CSE
Date:	26/10/2022	Duration:	90 mins	Max Marks:	50	Sem/Sec:	C		OBE

	Answer any FIVE FULL questions	MARKS	CO	RBT
1	What are crypto systems? Explain symmetric and asymmetric models of crypto systems.	[10]	CO1	L2
2 .	When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code: KXJEY UREBE ZWEHE WRYTU HEYFS KREHE GOYFI WTTTU OLKSY CAJPO BOTEI ZONTX BYBNT GONEY CUZWR GDSON SXBOU YWRHE BAAHY USEDQ The key used was ***royal new zealand navy***. Decrypt the message.	[10]	CO1	L3
3	Encrypt the message "This is a hidden message" using the Hill cipher with the key $\begin{bmatrix}9 & 4\\5 & 7\end{bmatrix}$ a. Show your calculations and the result. b. Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext.	[10]	CO1	L3
4	a). Differentiate between Stream ciphers and Block ciphers.	[06]	CO2	L2
	b). What is Avalanche effect? Explain The properties of Confusion and Diffusion in Cryptography.	[04]	CO2	L2
5.	Design Feistel cipher model for encryption and decryption process	[10]	CO2	L2
6	In an RSA cryptosystem, a participant uses two prime numbers p=3 and q=11 to generate his public and private keys. If the private key is 7, then how will the text „COMPUTER" be encrypted using the public key?	[10]	CO2	L3

Solutions:

1. A cryptosystem is an implementation of cryptographic techniques and their accompanying infrastructure to provide information security services.

Private Key Cryptosystem: Uses a single key for encryption and decryption purpose. The following diagram depicts infrastructure of the private key cryptosystem.



A source produces a message in plaintext, $X = [X1, X2, c, XM]$. The M elements of X are letters in some finite alphabet. Traditionally, the alphabet usually consisted of the 26 capital letters. Nowadays, the binary alphabet {0, 1} is typically used. For encryption, a key of the form $K = [K1, K2, c, KJ]$ is generated. If the key is generated at the message source, then it must also be provided to the destination by means of some secure channel. Alternatively, a third party could generate the key and securely deliver it to both source and destination. With the message X and the encryption key K as input, the encryption algorithm forms the ciphertext $Y = [Y1, Y2, c, YN]$.

This notation indicates that Y is produced by using encryption algorithm E as a function of the plaintext X, with the specific function determined by the value of the key K. The intended receiver, in possession of the key, is able to invert the transformation: $X = D(K, Y)$.

Public Key Cryptosystem:

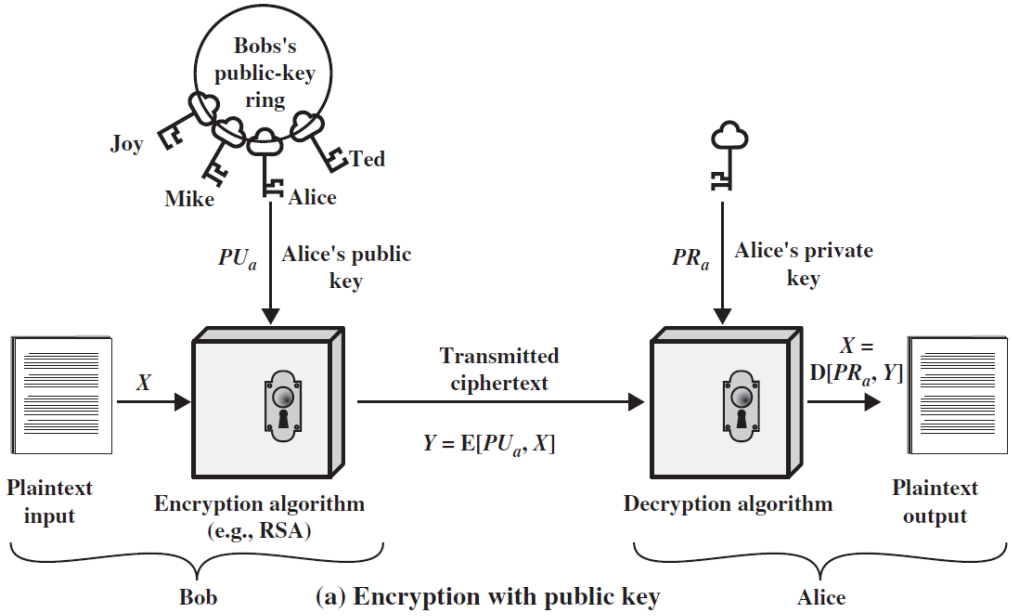
Asymmetric algorithms rely on one key for encryption and a different but related key for decryption. These algorithms have the following important characteristic.

- It is computationally infeasible to determine the decryption key.
- Either of the two related keys can be used for encryption, with the other used for decryption.
- A public-key encryption scheme has five ingredients

1. Plaintext: This is the readable message or data that is fed into the algorithm as input.
2. Encryption algorithm: The encryption algorithm performs various transformations on the plaintext.
3. Public and private keys: This is a pair of keys that have been selected so that if one is used for encryption, the other is used for decryption. The exact transformations performed by the algorithm depend on the public or private key that is provided as input.
4. Ciphertext: This is the scrambled message produced as output. It depends on the plaintext and the key. For a given message, two different keys will produce two different ciphertexts.

5. Decryption algorithm: This algorithm accepts the ciphertext and the matching key and produces the original plaintext.

Following diagram depicts the public key cryptosystem.



- Each user generates a pair of keys to be used for the encryption and decryption of messages.
- Each user places one of the two keys in a public register or other file. This is the public key. The companion key is kept private.
- If Bob wishes to send a confidential message to Alice, Bob encrypts the message using Alice's public key.
- When Alice receives the message, she decrypts it using her private key. No other recipient can decrypt the message because only Alice knows Alice's private key.

With this approach, all participants have access to public keys, and private keys are generated locally by each participant and therefore need never be distributed. As long as a user's private key remains protected and secret, incoming communication is secure. At any time, a system can change its private key and publish the companion public key to replace its old public key.

Q2. When the PT-109 American patrol boat, under the command of Lieutenant John F. Kennedy, was sunk by a Japanese destroyer, a message was received at an Australian wireless station in Playfair code:

KXJEY UREBE ZWEHE WRYTU HEYFS

KREHE GOYFI WTTTU OLKSY CAJPO

BOTEI ZONTX BYBNT GONEY CUZWR

GDSON SXBOU YWRHE BAAHY USEDQ

The key used was ***royal new zealand navy***. Decrypt the message.

Solution:

PT BOAT ONE OWE NINE LOST IN ACTION IN BLACKETT STRAIT TWO MILES SW MERESU COVE X CREW OF TWELVE X REQUEST ANY INFORMATION

Q3. Encrypt the message “This is a hidden message” using the Hill cipher with the key

$$\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$$

a. Show your calculations and the result.

b. Show the calculations for the corresponding decryption of the cipher text to recover the original plaintext.

Solution:

3 $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

0	1	2	3	4	5	6	7	8	9	10	11	
A	B	C	D	E	F	G	H	I	J	K	L	
12	13	14	15	16	17	18	19	20	21	22	23	
M	N	O	P	Q	R	S	T	U	V	W	X	
24	25											
Y	Z											

Encryption

This is a hidden message

$$C_1 = [19\ 7] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = \begin{bmatrix} 171+35 & 76+49 \end{bmatrix}$$

$$= [206 \quad 125] \bmod 26$$

$$= [24 \quad 21]$$

$$= [Y \quad V]$$

$$C_2 = [8\ 18] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [72+90 \quad 32+126]$$

$$= [162 \quad 158] \bmod 26$$

$C_3 = [9 \ 13] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [10 \ 2] = [K \ C]$

$C_4 = [0 \ 7] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [0+35 \ 0+49]$

$= [35 \ 49]$

$= [9 \ 23]$

$= [J \ X]$

$C_5 = [8 \ 3] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [72+15 \ 32+21]$

$= [87 \ 33] \ \text{mod } 26$

$= [9 \ 7]$

$= [J \ H]$

$C_6 = [3 \ 4] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [27+20 \ 12+28]$

$= [47 \ 40] \ \text{mod } 26$

$= [21 \ 14]$

$= [V \ O]$

$C_7 = [13 \ 12] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [117+60 \ 52+84]$

$= [170 \ 136] \ \text{mod } 26$

$= [14 \ 6]$

$= [O \ G]$

$C_8 = [4 \ 18] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [36+90 \quad 16+126]$

$= [126 \quad 142]$

$= [22 \quad 12]$

$= [w \quad m]$

$C_9 = [18 \ 0] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [162 \quad 72]$

$= [6 \quad 20]$

$= [G \quad U]$

$C_{10} = [6 \ 4] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} = [54+20 \quad 24+28]$

$= [74 \quad 52]$

$= [22 \quad 0]$

$= [w \quad A]$.

Plain text : "This is a hidden message

Cipher text : 4V KC JX JH VO OG WM GU WA.

Q4.

a). Differentiate between Stream ciphers and Block ciphers.

Block Cipher	Stream Cipher
Processing or encoding of the plain text is done as a fixed length block one by one. A block for example could be 64 or 128 bits in size.	Processing or encoding of plain text is done bit by bit. The block size here is simply one bit.
The same key is used to encrypt each of the blocks	A different key is used to encrypt each of the bits.
A Pad added to short length blocks	Bits are processed one by one in as in a chain
Uses Symmetric Encryption and is NOT used in asymmetric encryption	High speed and low hardware complexity
Confusion factor: The key to the cipher text relationship could be really very complicated.	Key is often combined with an initialization vector
Diffusion Factor: output depends on the input in a very complex method.	Long period with no repetition
Most block ciphers are based on Feistel cipher in structure	Statistically random
Looks more like an extremely large substitution and Using the idea of a product cipher	Depends on a large key and Large liner complexity
More secure in most cases	Equally secure if properly designed
Usually more complex and slower in operation	Usually very simple and much faster
Examples of Block Cipher are: Lucifer / DES,IDEA, RC5, Blowfish etc.	Examples of Stream Cipher are: FISH, RC4, ISAAC, SEAL, SNOW etc.

b). What is Avalanche effect? Explain The properties of Confusion and Diffusion in Cryptography.

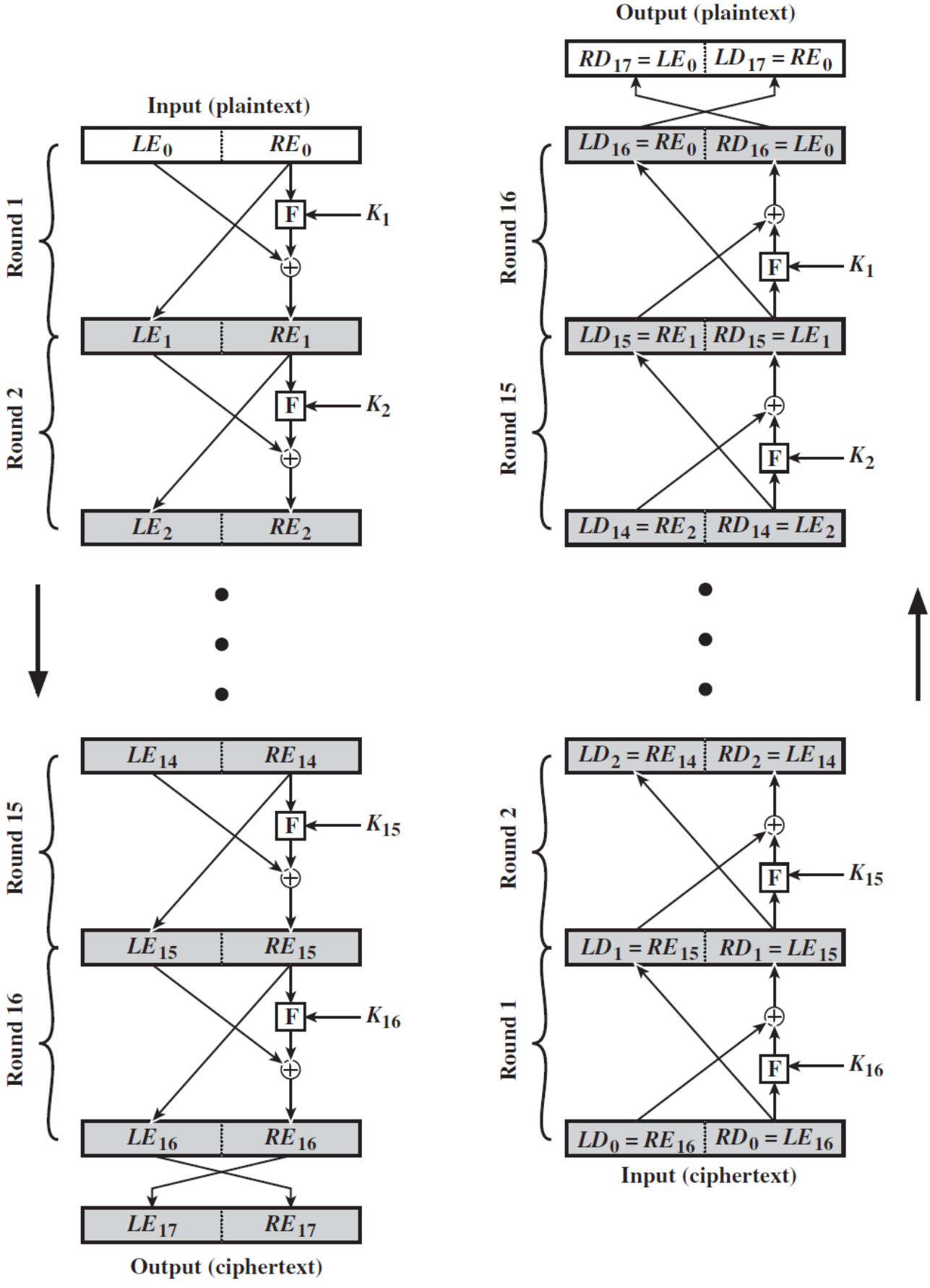
A desirable property of any encryption algorithm is that a small change in either the plaintext or the key should produce a significant change in the ciphertext. In particular, a change in one bit of the plaintext or one bit of the key should produce a change in many bits of the ciphertext. This is referred to as **the avalanche effect**. If the change were small, this might provide a way to reduce the size of the plaintext or key space to be searched.

The property of confusion hides the relationship between the ciphertext and the key. This property makes it difficult to find the key from the ciphertext and if a single bit in a key is changed, the calculation of most or all of the bits in the ciphertext will be affected.

Confusion increases the ambiguity of ciphertext and it is used by both block and stream ciphers. Diffusion means that if we change a single bit of the plaintext, then about half of the bits in the ciphertext should change, and similarly, if we change one bit of the ciphertext, then about half of the plaintext bits should change. This is equivalent to the expectation that encryption schemes exhibit an avalanche effect.

Q5. Design Feistel cipher model for encryption and decryption process

The Data Encryption Standard is a symmetric-key algorithm for the encryption of digital data. Developed in the early 1970s at IBM and based on an earlier design by Horst Feistel.



The left-hand side of Figure depicts the structure proposed by Feistel. The inputs to the encryption algorithm are a plaintext block of length 2*w* bits and a key *K*. The plaintext block is divided into two halves, *L*0 and *R*0. The two halves of the data pass through *n* rounds of processing and then combine to produce the ciphertext block. Each round *i* has as inputs *Li*-1 and *Ri*-1 derived from the previous round, as well as a subkey *Ki* derived from the overall *K*. In general, the subkeys *Ki* are different from *K* and from each other. In Figure, 16 rounds are used, although any number of rounds could be implemented.

All rounds have the same structure. A **substitution** is performed on the left half of the data. This is done by applying a *round function* F to the right half of the data and then taking the exclusive-OR of the output of that function and the left half of the data. The round function has the same general structure for each round but is parameterized by the round subkey *Ki*. Another way to express this is to say that F is a function of right-half block of *w* bits and a subkey of *y* bits, which produces an output value of length w bits: *F*(*REi*, *Ki*+1). Following this substitution, a **permutation** is performed that consists of the interchange of the two halves of the data.

Q6. In an RSA cryptosystem, a participant uses two prime numbers p=3 and q=11 to generate his public and private keys. If the private key is 7, then how will the text „COMPUTER" be encrypted using the public key?

Concept:

RSA Algorithm:

Step 1: Calculate value of n = p × q, where p and q are prime no.'s

Step 2: calculate Ø(n) = (p-1) × (q-1)

Step 3: consider d as a private key such that Ø(n) and d have no common factors. i.e greatest common divisor (Ø(n) , d) = 1

Step 4: consider e as a public key such that (e × d) mod Ø(n) = 1.

Step 5: Ciphertext = message i.e. m^e mod n.

Step 6: message= cipher text i.e. c^d mod n.

Calculation:

Given prime numbers, p =3, q = 11

n= 3 x 11 =33

Ø(n) = (3-1) × (11-1) = 2 x 10 =20

greatest common divisor (20, d) =1

d = Private Key = 7

Given prime numbers, p =3, q = 11

n= 3 x 11 =33

Ø(n) = (3-1) × (11-1) = 2 x 10 =20

greatest common divisor (20, d) =1

d = Private Key = 7

As per question d =7.

(e × d) mod Ø(n) = 1

(e x 7) mod 20 = 1

So, e x 7= 20 x 1+1

e= $\frac{21}{7}$ = 3 possible.

,e = public Key=3 =encrypt key

So n = 33 ,e = 3 , d = 7, Ø(n) = 20

Plan text = COMPUTER

Plan text = COMPUTER

Ciphertext = m^e mod n.

Ciphertext for C = 3^3 mod 33 = 27

Ciphertext for O = 15^3 mod 33 = 9

Ciphertext for M = 13^3 mod 33 = 19

Ciphertext for P = 16^3 mod 33 = 4

Ciphertext for U = 21^3 mod 33 = 21

Ciphertext for T = 20^3 mod 33 = 14

Ciphertext for E = 5^3 mod 33 = 26

Ciphertext for R = 18^3 mod 33 = 24

Hence the correct answer is 27 9 19 4 21 14 26 24.