K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109

FIRST INTERNAL TEST QUESTION PAPER-2023-24 EVEN SEMESTER

SET A

USN										

Degree : B.E
Branch : Electronics & Communication Engg.
Course Title : Cryptography
Duration : 60 Minutes

Semester : VI A& B
Course Code : 21EC642
Date : 29th MAY 2024
Max Marks : 20

Note: Answer ONE full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
	PART-A			
1(a)	Explain the extended Euclid's algorithm for determining the multiplicative of two positive integers. **Solve** the GCD of **(24140,16762)**	4	CO1	K3
(b)	State the axioms of Field and **Solve** additive & multiplicative table for GF(2^2) give primitive polynomial as(x^2+x+1)	4	CO1	K3
(c)	Construct additive and multiplicative table for Z_7 and **Solve** all additive and multiplicative inverse elements	4	CO1	K3
	OR			
2(a)	Explain the Euclid's algorithm & find GCD of a number and **Solve** the multiplicative inverse of **1234 mod 4321**	4	CO1	K3
(b)	Check whether (X^3+X^2+1) is irreducible and **Solve** multiplicative invers for (X^3+X^2+1) mod (X^2+X+1)	4	CO1	K3
(c)	Construct mod8 additive and multiplicative table and **Solve** all additive and multiplicative inverse elements.	4	CO1	K3
	PART-B			
3(a)	**Make use of** Symmetrical encryption model and explain it with a neat diagram and define Substitution Technique and Transposition technique.	4	CO2	K3
(b)	Make use of Playfair algorithm and **solve** cipher text for **"TECHNOLOGY"** with keyword **"ATTACK"**	4	CO2	K3
	OR			
4(a)	Encrypt the plain text MONDAY using Hill cipher with key [J E F H] and **Solve** inverse of the Key matrix.	4	CO2	K3
(b)	**Make use of** Playfair algorithm and Explain it with an example.	4	CO2	K3

Name & Signature of Course In charge:

Name & Signature of Module Coordinator

HOD ECE

Principal

Selected

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
I SESSIONAL TEST QUESTION PAPER 2023-24 ODD SEMESTER
SCHEME AND SOLUTION for SET A

Degree: B.E **Semester: VI A & B**
Branch: E&CE **Course Code: 21EC642**
Course Title : Cryptography **Max Marks: 20**

1 a

The Euclidean Algorithm for finding GCD(A,B) is as follows:
If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.
If B = 0 then GCD(A,B)=A, since the GCD(A,0)=A, and we can stop.
Write A in quotient remainder form (A = B·Q + R)
Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) = GCD(B,R) — 2M

GCD(24140, 16762) = GCD (16762, 7378) = GCD (7378, 2006) =
GCD (2006, 1360) = GCD (1360, 646) = GCD (646, 68) = GCD (68, 34) =
GCD (34, 0) = 34 — 2M

4M

1b

Properties of Field
Satisfies all the properties of group like closure, associative, Identity, Inverse and commutative property and also satisfies properties of Ring like closure, associative, Identity,distributive and also satisfies Inverse property.

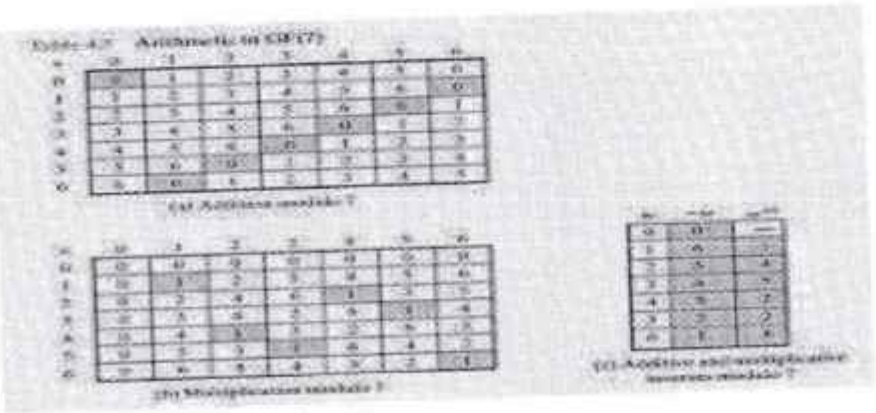
Additive & Multiplicative table for GF(2^2) give primitive polynomial as($\mathbf{x^2+x+1}$)
Set elements are (0,1,X,X+1)
Additive inverse of

Elements	Additive Inverse	Multiplicative Inverse
0	0	0
1	1	1
X	X	X+1
X+1	X+1	X

4M

1c

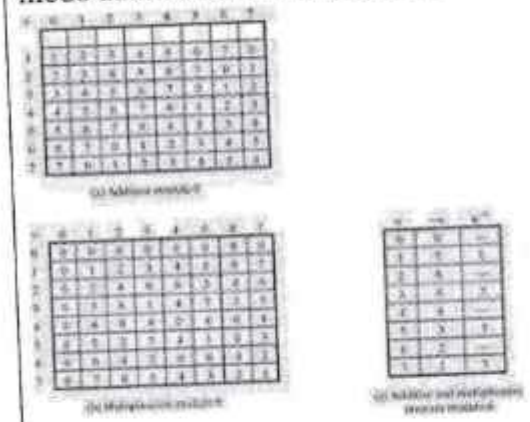
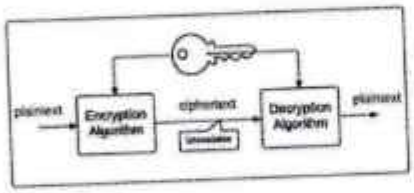
Additive and multiplicative table for $\mathbf{Z_7}$



4M

2a.

The explanation of Euclid's algorithm 1M

	Multiplicative inverse of 1234 mod 4321= 3239 3M	4M
2b	Yes (X^3+X^2+1) is irreducible and The multiplicative invers for $(X^3+X+1)^{-1} \bmod (X^2+X+1)$ is [x+1] $(X^2+X+1)^{-1} \bmod (X^3+X+1) = x^2$	
2c.	mod8 additive and multiplicative 	4M
3a.	Symmetrical encryption model  Diagram &Explanation 3M	4M
3b.	Define for Substitution & Transposition Techniques: 1M PLAY FAIR cipher with the key **ATTACK** encrypt the message **"TECHNOLOGY** **4M**	4M
4a	$K^{-1} = \begin{matrix} 9 & 2 \\ 1 & 15 \end{matrix}$	4M
4b.	Explanation Playfair algorithm with an example	4M

Signature of Course in-charge **Signature of Module Coordinator** **Signature of HOD ECE**

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109

FIRST INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER

SET B

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

Degree : B.E
Branch : Electronics & Communication Engg.
Course Title : Cryptography
Duration : 60 Minutes

Semester : VI A& B
Course Code : 21EC642
Date : 29th MAY 2024
Max Marks : 20

Note: Answer ONE full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
	PART-A			
1(a)	Mention all modular arithmetic properties & obtain additive & multiplicative table for Mod5 and **Solve** all additive & multiplicative inverse for the same	4	CO1	K3
(b)	**Solve** GCD [a(x),b(x)] for $\mathbf{a(x) = x^6+x^5+x^4+x^3+x^2+x+1}$ and $\mathbf{b(x) = x^4+x^2+x+1}$ **and write** all modular arithmetic properties	4	CO1	K3
(c)	Construct additive and multiplicative table for GF(7) and **Solve** all additive and multiplicative inverse elements	4	CO1	K3
	OR			
2(a)	**Solve** the multiplicative inverse of $\mathbf{a(x) = x^8+x^4+x^3+x+1}$ and $\mathbf{b(x) = x^7+x+1}$	4	CO1	K3
(b)	Check whether $(X^4+X^3+X^2+1)$ is irreducible and **Solve** multiplicative invers for (X^3+X+1) mod (X^2+X+1)	4	CO1	K3
(c)	Construct Z_8 additive and multiplicative table and **Solve** all additive and multiplicative inverse elements.	4	CO1	K3
	PART-B			
3(a)	**Make use of** Symmetric Crypto system and explain it with a neat diagram and define reducible and irreducible polynomial.	4	CO2	K3
(c)	**Make use of** playfair cipher ,Encrypt the plain text **"ELECTRONICS"** with a key **INDIA** also mention all the rules for encryption.	4	CO2	K3
	OR			
4(a)	Encrypt the plain text MONDAY using Hill cipher with key $\mathbf{K}=\begin{pmatrix} 2 & 3 \\ 1 & 22 \end{pmatrix}$ and **Solve** inverse of the Key matrix	4	CO2	K3
(b)	**Make use of** Playfair cipher with the key **largest** encrypt the message **"Must see you today"**	4	CO2	K3

Name & Signature of Course In charge:

Name & Signature of Module Coordinator

HOD ECE

Principal

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
I SESSIONAL TEST QUESTION PAPER 2023-24 ODD SEMESTER
SCHEME AND SOLUTION for SET B

Degree: B.E **Semester: VI A & B**
Branch: E&CE **Course Code: 21EC642**
Course Title : Cryptography **Max Marks: 20**

1 a Mod 5 — 4M

Additive modulo 5

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

multiplication modulo 5

X	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

1b GCD **a**
$a(x) = x^6+x^5+x^4+x^3+x^2+x+1$ and 3M
$b(x) = x^4+x^2+x+1$
is **$\underline{x^3+x^2+1}$** 4M

Modular Properties :
(a+b) modn= amodn + bmodn 1M
(a-b) modn= amodn - bmodn
(a*b) modn= amodn * bmodn

1c Additive and multiplicative table for x^3+x+1

	*	000	001	010	011	100	101	110	111
		0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
000	0	0	0	0	0	0	0	0	0
001	1	0	1	x	x+1	x^2	x^2+1	x^2+x	x^2+x+1
010	x	0	x	x^2	x^2+x	x+1	1	x^2+x+1	x^2+1
011	x+1	0	x+1	x^2+x	x^2+1	x^2+x+1	x^2	1	x
100	x^2	0	x^2	x+1	x^2+x+1	x^2+x	x	x^2+1	1
101	x^2+1	0	x^2+1	1	x^2	x	x^2+x+1	x+1	x^2+x
110	x^2+x	0	x^2+x	x^2+x+1	1	x^2+1	x+1	x	x^2
111	x^2+x+1	0	x^2+x+1	x^2+1	x	1	x^2+x	x^2	x+1

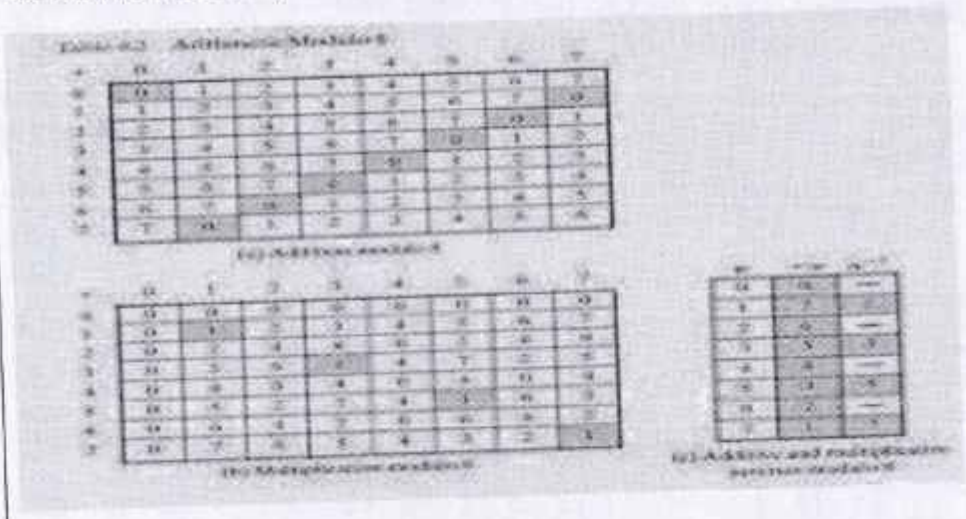
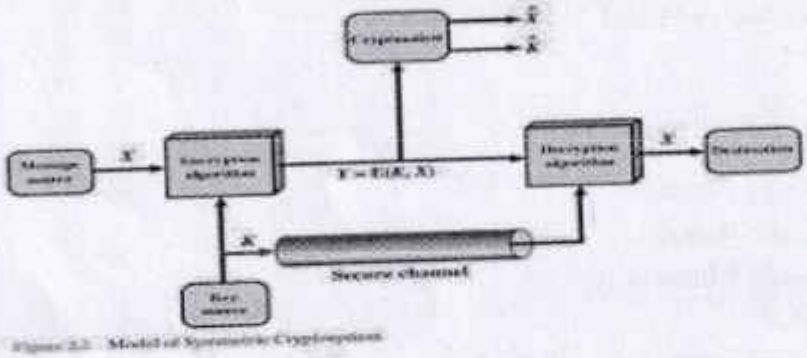
2a. Multiplicative Inverse for **$a(x) = x^8+x^4+x^3+x+1$** is and 4M

$b(x) = x^7+x+1$ is x^7

2b No $(X^4+X^3+X^2+1)$ is not irreducible and

The multiplicative invers for (X^3+X+1) mod (X^2+X+1)

X and X+1

2c.	Z_8 additive and multiplicative table 	4M
3a.	model of Symmetric Crypto system 	4M
3b.	**INDIA** **EL EC TR ON IC SX** LR FE US LA CK XD	4M
4a	plain text MONDAY using Hill cipher with key **K= 2 3** **1 22** **k − 1** $\begin{pmatrix} 24 & 5 \\ 19 & 14 \end{pmatrix}$	
4b.	PlayFair cipher with the key **largest** encrypt the message "**Must see you today**" **MU ST SE E Y OU TO DA YX** **UZ TB DL GZ PN AW TE ZY**	4M 4M

Signature of Course in-charge **Signature of Module Coordinator** **Signature of HOD ECE**

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
SECOND INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER
SET A

Degree	:	B.E	USN		
Branch	:	Electronics & Communication Engg.	Semester	:	VI A& B
Course Title	:	Cryptography	Course Code	:	21EC642
Duration	:	60 Minutes	Date	:	29th June 2024
			Max Marks	:	20

Note: Answer ONE full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
	PART-A			
1(a)	**Explain** with a neat diagram the operation performed in 1st & 10th round of AES algorithm.	4	CO3	K2
(b)	State & prove Fermat's theorem and **Solve** $3^{990} \bmod 91$ & $3^{999} \bmod 10$ using it	4	CO3	K3
(c)	With a neat diagram **explain** round operation in DES encryption	4	CO3	K2
	OR			
2(a)	With a neat diagram of DES encryption & decryption process and **explain** the working principle for the same.	4	CO3	K2
(b)	Explain Key expansion technique in AES algorithm & Define Euler's theorem and **Solve** Totient function for 37 & 600	4	CO3	K3
(c)	Explain the parameters of Feistel structure and design Feistel network for encryption & decryption.	4	CO3	K2
	PART-B			
(a)	Encrypt the plain text 'PAYMOREMONEY' using Hill cipher algorithm and **Solve** the cipher text. Given Key K= $\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$	4	CO2	K3
(b)	With a neat block diagram explain the Principles of Public-Key Cryptosystems with authentication & **Solve** cipher text and plain text using the RSA algorithm given P=5, Q=11, e=3 and encrypt the message M=EC and decrypt the same.	4	CO4	K3
	OR			
(a)	**Make use of** Substitution and Transposition technique definition with an example also define Diffusion and Confusion technique. **solve** the Encrypt the plain text **AUTHENTICATION** using Rail fence method & Key technique given KEY as 4132	4	CO2	K3
(b)	**Make use of** the concepts of Public key explain Principles of Public-Key Cryptosystems with authentication and secrecy with a neat diagram. & Explain RSA algorithm	4	CO4	K3

Name & Signature of Course In charge:

Name & Signature of Module Coordinator

HOD ECE

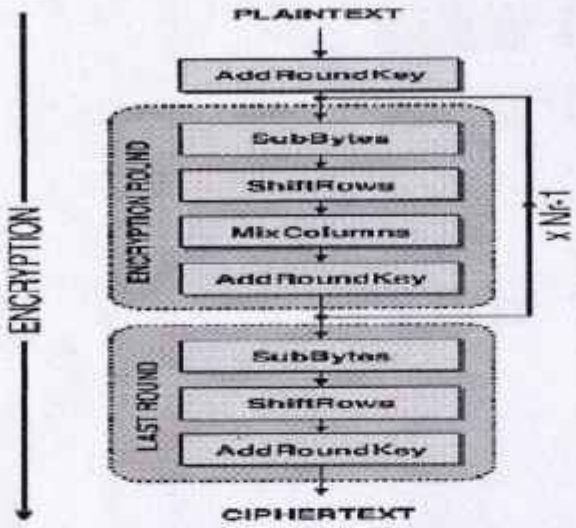
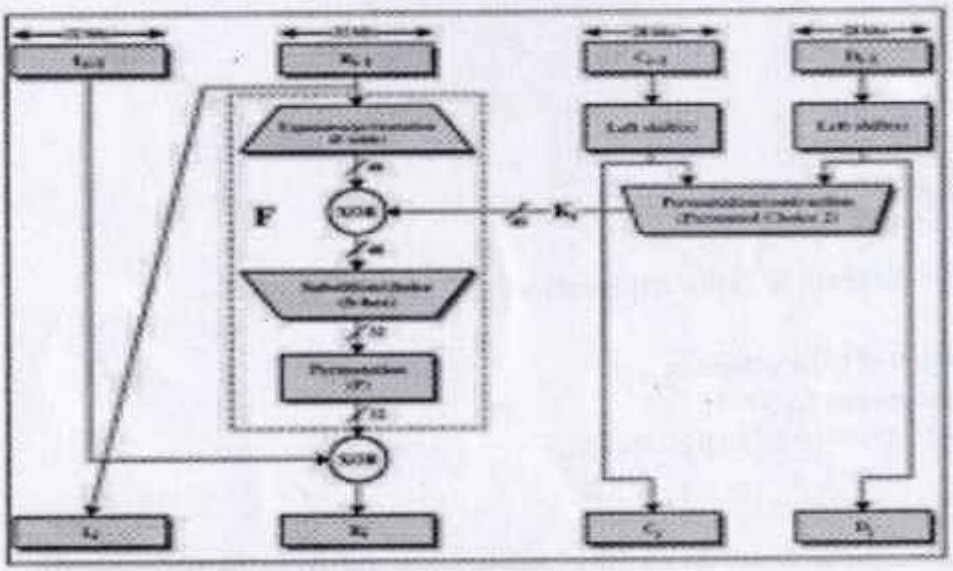
Principal

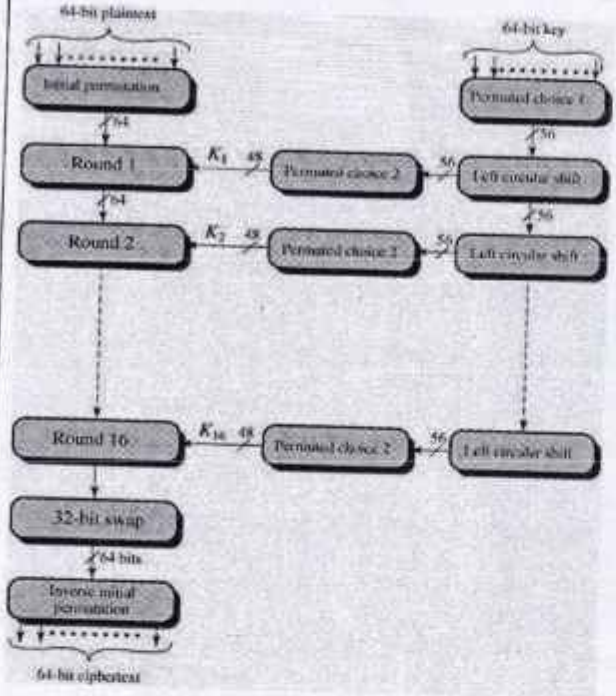
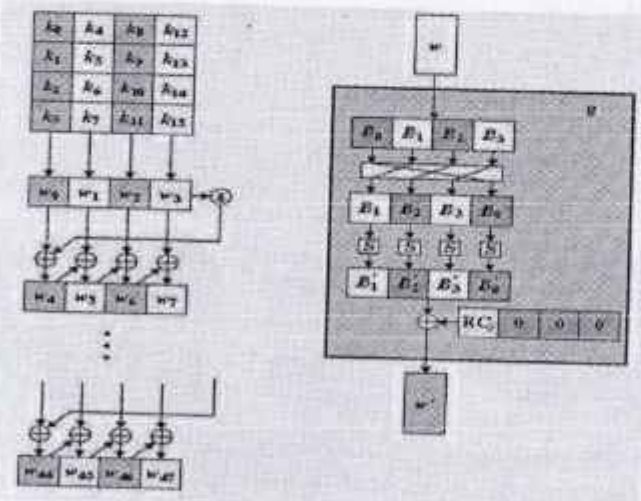
Selected

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
SECOND INTERNAL TEST 2023-24 EVEN SEMESTER
SCHEME AND SOLUTION for SET A

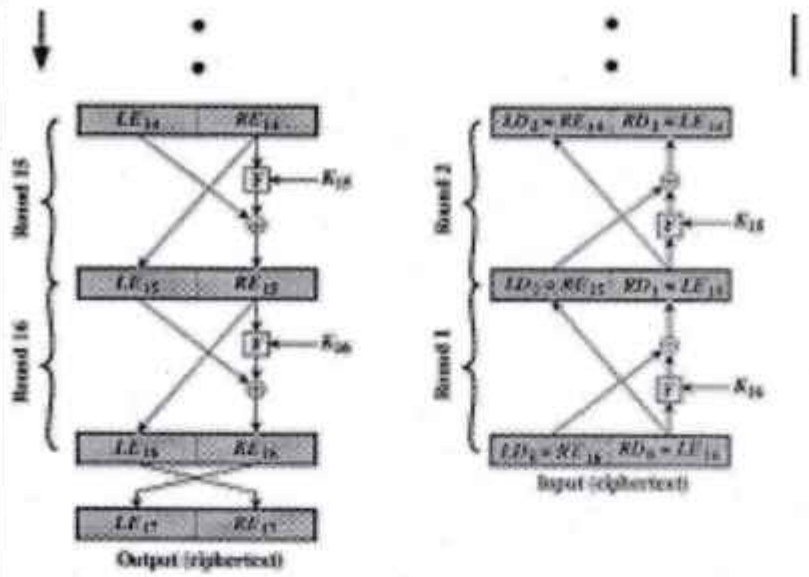
Degree : B. E
Branch : E&CE
Course Title : Cryptography

Semester: VI A & B
Course Code: 21EC642
Max Marks: 30

Q No.	Points	Marks
1 a	 Fig 1 M and explanation 3M	4M
1b	State Fermat's theorem:1 M Proof: 2M $3^{990} \bmod 91 = 1$ ½ marks each & $3^{999} \bmod 10 = 1$	4M
1c		4M

	2M for diagram & 2M for explanation.	4M
2a.	DES encryption & decryption process  1M for diagram & 3Mfor explanation.	
2b.	 1M for diagram & 2Mfor explanation.	4M
	Definition of Euler's theorem Totient function for 37=36 $600= 2^3*3*5^2= [8-4][3-1][25-5]=160$ 1M	

2c.



1M for diagram & 3Mfor explanation.

4M

3a.

PAYMOREMONEY encrypt using Hill cipher

Key K=

17	17	15
21	18	21
2	2	19

Plain text

$$\begin{pmatrix} 15 & 0 & 24 \\ 12 & 14 & 17 \\ 4 & 12 & 14 \\ 13 & 4 & 24 \end{pmatrix}$$

Cipher = $\begin{pmatrix} 303 & 303 & 681 \\ 532 & 490 & 797 \\ 348 & 312 & 578 \\ 353 & 341 & 735 \end{pmatrix}$

4M

Cipher = $\begin{pmatrix} 17 & 17 & 5 \\ 12 & 22 & 17 \\ 10 & 0 & 6 \\ 15 & 3 & 7 \end{pmatrix}$

3b

The Principles of Public-Key Cryptosystems with authentication

1M for diagram & 3Mfor explanation

4M

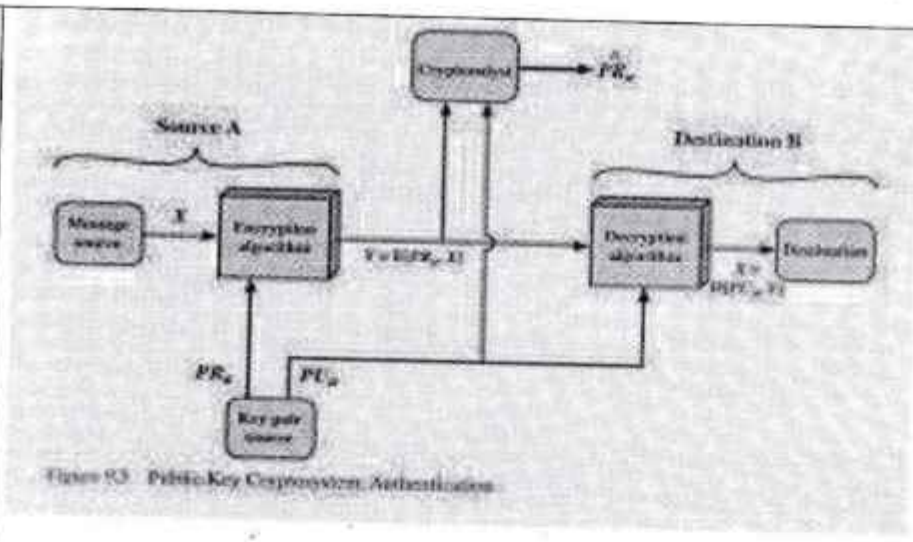


Figure 9.3 Public-Key Cryptosystem: Authentication

RSA algorithm given P=5, Q=11, e=3 and encrypt the message M=EC and decrypt the same.

P=5 Q=11 e=3 and M=EC: 42

n=55, Φ=40

Given e=3

de mod40=1 d=27

Encryption C1= M^e mod n= 4^3mod 55=9

C2= M^e mod n= 2^3mod 55=8

Decryption D= $C1^d$ mod n = 9^{27} mod 55=4

$C1^d$ mod n = 4^{27} mod 55=2

4a.

Def for Substitution and Transposition technique 1M

Diffusion and Confusion technique

AUTHENTICATION using Rail fence method & Key technique given KEY as 4132 4M

RAILFENCE: A T E T C T O

U H N I A I N

A T E T C T O U H N I A I N

4 1 3 2 **O/P UNANHIIXTTTXAECO**

A U T H

E N T I

C A T I

O N X X

4b.	The Principles of Public-Key Cryptosystems with authentication and secrecy.	4M

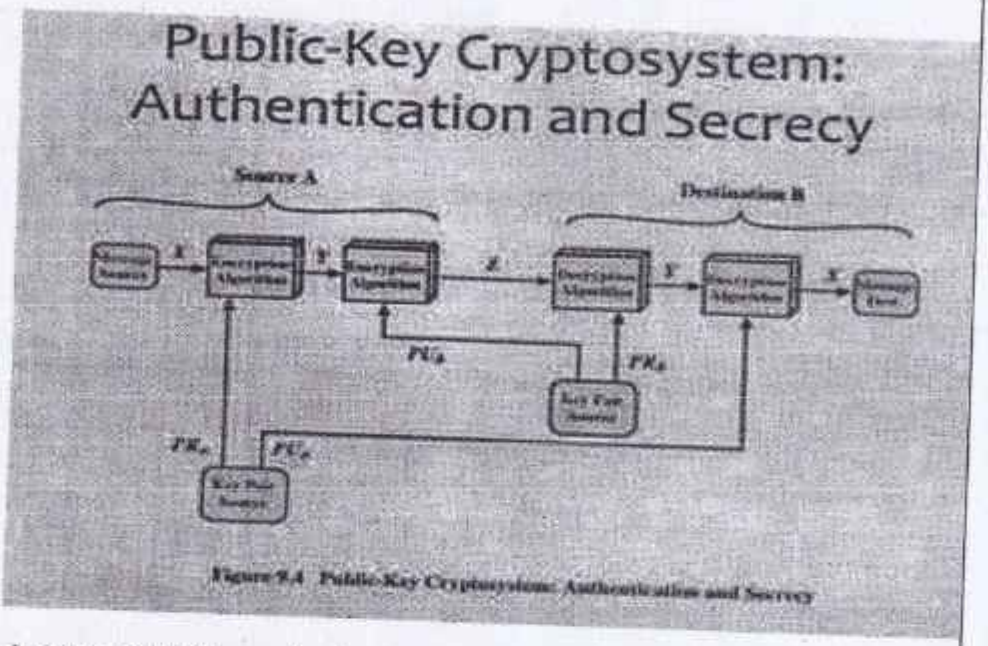


Figure 9.4 Public-Key Cryptosystem: Authentication and Secrecy

1M for diagram & 1Mfor explanation

RSA ALGORITHM

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1;\ 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

Signature of Course In-charge Signature of Module Coordinator Signature of HOD

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109

SECOND INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER

SET B

USN										

egree : B.E
ranch : Electronics & Communication Engg.
ourse Title : Cryptography
uration : 60 Minutes

Semester : VI A& B
Course Code : 21EC642
Date : 29th June 2024
Max Marks : 20

Note: Answer ONE full question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Question	Marks	CO mapping	K-Level
	PART-A			
1(a)	State & prove Euler's theorem. **Solve** $\Phi(q)$ and $P^{\Phi(q)}$ mod q given values 1) P=3, q=7 2) q= 12, P= 5	4	CO3	K3
(b)	Explain the concept of Substitution byte, Mix column & Shift row operation with neat diagram in AES algorithm	4	CO3	K2
(C)	**Illustrate** the round operation in DES algorithm & compare DES and AES algorithm	4	CO3	K3
	OR			
2(a)	Define a **WORD** in AES algorithm & **illustrate** the working of **'g' function** in AES Key expansion algorithm with a neat diagram.	4	CO3	K3
(b)	Explain the Feistel encryption and decryption process with a neat diagram	4	CO3	K2
(C)	Define Fermat's little theorem and **Solve** the value of X given $\mathbf{X^{103} \equiv 4}$ **mod 11** and find the remainder for $\mathbf{2^{35} mod 7}$ and $\mathbf{7^{20} mod 21}$	4	CO3	K3
	PART-B			
3(a)	**List** and explain the process used in RSA algorithm for encrypting and decrypting the data & Define Authentication, Digital Signature, Confidentiality	4	CO2	K3
(b)	Encrypt the plain text 'CIPHER' using Hill cipher algorithm and **Solve** the cipher text. Given Key K= $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$	4	CO4	K3
	OR			
4(a)	**Solve** the encrypted data given the plain text **ELECTRONICS** using Rail fence method & Key technique given KEY as 4132. & Define **Monoalphabetic cipher & Polyalphabetic cipher**	4	CO2	K3
(b)	With a neat block diagram explain the Principles of Public-Key Cryptosystems with confidentiality & **Solve** cipher text given plain text as **KS** using the RSA algorithm given P=3, Q=11, e=7	4	CO4	K3

Name & Signature of Course In charge:

Name & Signature of Module Coordinator

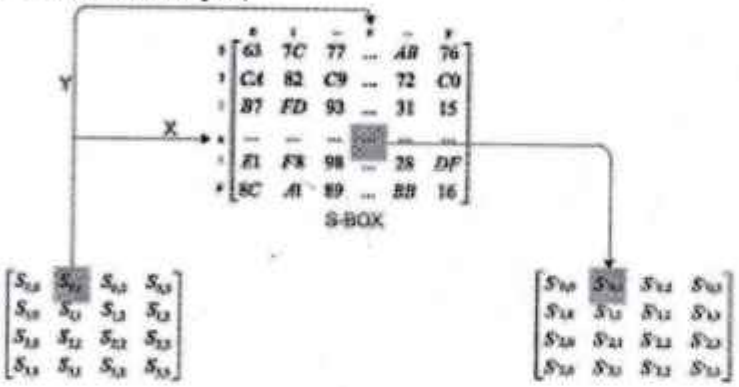
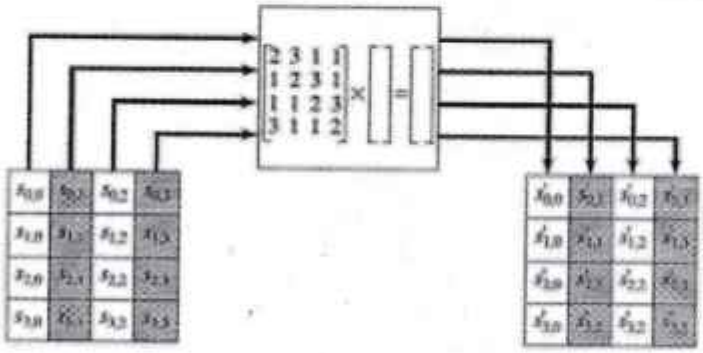
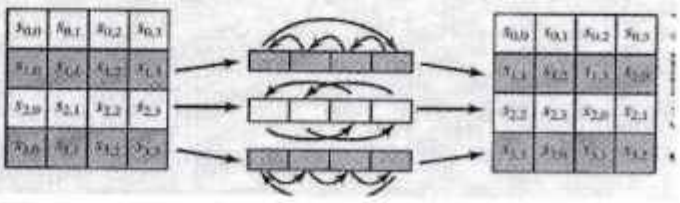
HOD ECE

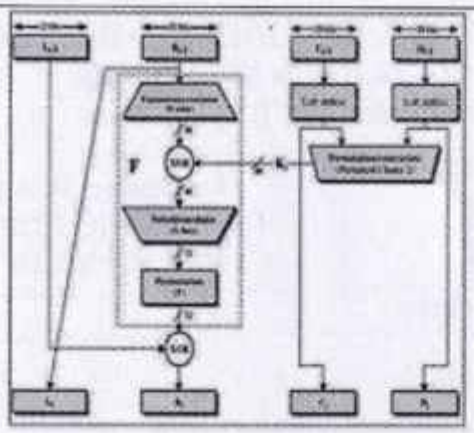
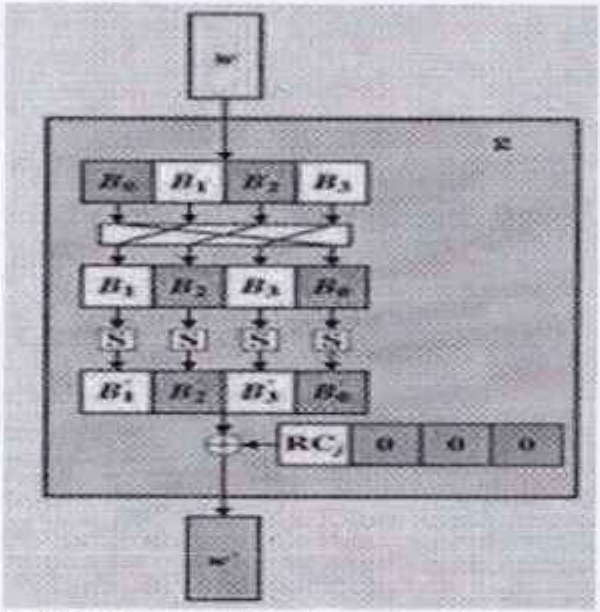
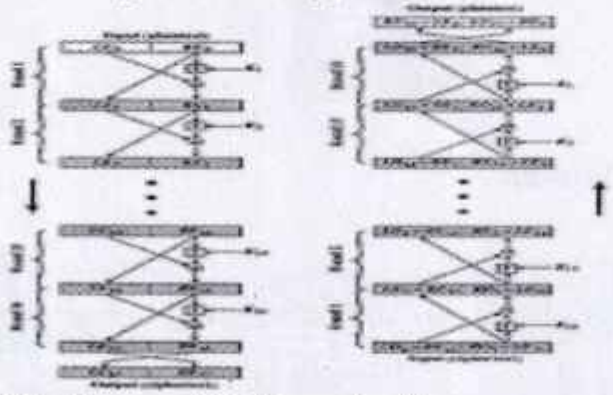
Principal

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
SECOND INTERNAL TEST 2023-24 EVEN SEMESTER
SCHEME AND SOLUTION for SET B

Degree : B. E
Branch : E&CE
Course Title : Cryptography

Semester: VI A & B
Course Code: 21EC642
Max Marks: 30

Q No.	Points	Marks
1 a	Def of Euler's theorem & proof . **Find** $\Phi(q)$ for $\Phi(7)=6$, $\Phi(12)= 2^2*3 = 2*2= 4$ And $P^{\Phi(q)}$ mod q given values 3^6 mod 7=1 5^4mod 12 = 1	4M
1b	**Substitution byte,**  **Mix column**  **Shift row operation in AES algorithm** • Rules of shifting rows, • Row 1 → No Shifting • Row 2 → 1 byte left shift • Row 3 → 2 byte left shift • Row 4 → 3 byte left shift 	4M

1c	 **figure 1M & 2M for explantion** **Comparison AES does not follow Feistel 1M**	4M
2a.	**Def of WORD** in AES algorithm 1M The working of **'g' function** in AES Key expansion  1 M for figure and 2M for explanation	4M
2b.	Feistel encryption and decryption process with a neat diagram  1 M for figure and 3M for explanation	4M

2c.

Definition Fermat's little theorem 1M

X given $\mathbf{X^{103} \equiv 4 \bmod 11 = 5}$ **2M**

The remainder for $\mathbf{2^{35} \bmod 7 = 4}$ **2M**
and $\mathbf{7^{20} \bmod 21 = 1}$

4M

3a

Key Generation	
Select p, q	p and q both prime, $p \neq q$
Calculate $n = p \times q$	
Calculate $\phi(n) = (p-1)(q-1)$	
Select integer e	$\gcd(\phi(n), e) = 1; 1 < e < \phi(n)$
Calculate d	$d \equiv e^{-1} \pmod{\phi(n)}$
Public key	$PU = \{e, n\}$
Private key	$PR = \{d, n\}$

Encryption	
Plaintext:	$M < n$
Ciphertext:	$C = M^e \bmod n$

Decryption	
Ciphertext:	C
Plaintext:	$M = C^d \bmod n$

4M

3b

CIPHER' using Hill cipher algorithm
and **find** the cipher text.

Given Key K= $\begin{bmatrix} 6 & 24 & 1 \\ 13 & 16 & 10 \\ 20 & 17 & 15 \end{bmatrix}$

Plain text $\begin{pmatrix} 2 & 8 & 15 \\ 7 & 4 & 17 \end{pmatrix}$ cipher= $\begin{pmatrix} 416 & 431 & 307 \\ 434 & 521 & 302 \end{pmatrix}$ = $\begin{pmatrix} 0 & 15 & 21 \\ 18 & 1 & 16 \end{pmatrix}$

4M

4a.

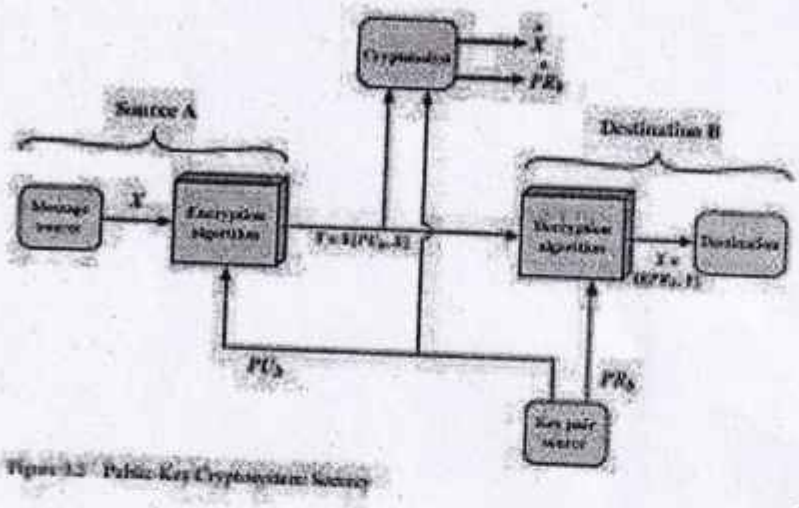
plain text **ELECTRONICS** using Rail fence method & Key technique given KEY as 4132

RAILFENCE: E E T O I S 1M

L C R N C

O/P= ETOISLCRNC

4M

	4 1 3 2 O/P LRCCNXEOSETI 1M E L E C T R O N I C S X Definition for **Monoalphabetic cipher & Polyalphabetic cipher 1M EACH**	
4b.	The Principles of Public-Key Cryptosystems with CONFIDENTALITY.  2M **KS** using the RSA algorithm given P=3, Q=11, e=7 P=3 Q=11 e=7 and M=KS: 10 18 n=33, Φ=20 Given e=7 de mod20=1 d=3 Encryption C1= M^e mod n= 10^7mod 33=10 C2= M^e mod n= 18^7mod 33=6 Decryption D= $C1^d$ mod n = 10^3 mod 33=10 $C1^d$ mod n = 6^3 mod 33=18 2M	4M

Signature of Course In charge **Signature of Module Coordinator** **Signature of HOD**

K.S. INSTITUTE OF TECHNOLOGY, BENGALURU - 560109
THIRD INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER

SET: A

USN										

Degree	:	**B. E.,**	**Semester**	:	**VI**
Branch	:	**E&CE**	**Course Code**	:	**21EC642**
Course Title	:	**Cryptography**	**Date**	:	**31st July 2024**
Duration	:	**60 Minutes**	**Max Marks**	:	**20**

Note: Answer **ONE full** question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

Q No.	Questions	Marks	CO	K-Level
	PART-A			
1(a)	**Explain** Generalized Geffe generator & Alternating Stop& Gogenerator with a neat diagram.	4	CO5	K2
(b)	**Explain** the application & working of A5 generator and Thresholdgenerator.	4	CO5	K2
(c)	**Explain** Linear feedback shift register with a neatdiagram.	4	CO5	K2
	OR			
2(a)	**Explain** Linear Congruential Generator with an example.	4	CO5	K2
(b)	**Explain** Gifford generator & Geffe generator.	4	CO5	K2
(c)	**Explain** Bilateral Stop and Go generator and Jennings Generator	4	CO5	K2
	PART –B			
3(a)	**Solve** P+Q and 2P for the given $E_{11}(8,10)$, P= (3,7) and Q= (5,9) and explain Elliptic Curve Arithmetic on the curve.	4	CO4	K3
(b)	Make use of Diffie Hellman's Key exchange algorithm and **solve** Public Key of user A & B for $E_{11}(1,6)$, G(1,3) and private Key of User A is 2 and B is 1 and explain ECC.	4	CO4	K3
	OR			
4(a)	Make use of ECC algorithm encrypt the data given $E_{11}(1,1)$, G(1,3),n=20.Assume secret key between the user as 1.**Solve** all the private key and Public key.	4	CO4	K3
(b)	**Solve** Shared key if Public Key for $E_{11}(1,1)$, G (2,2) and private Key of User A is 1 and B is 2 and Explain ECC encryption algorithm.	4	CO4	K3

Name & Signature of Course In charge | **Name & Signature of Module Coordinator** | **HOD ECE** | **Principal**

Selected

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
THIRD INTERNAL TEST 2023-24 EVEN SEMESTER
SCHEME AND SOLUTION for SET A

Degree : B. E
Branch : E&CE
Course Title : Cryptography

Semester: VI A & B
Course Code: 21EC642
Max Marks: 20

Q No.	Points	Marks
1 a	**Generalized Geffe Generator:** • Instead of choosing between two LFSRs,this scheme chooses between k LFSRs,as long as k is a power of 2. • More complex than Geffe generator and correlation attack is possible. • Correlation attack is outputs of individual LFSRs can be combined keystream and attacked using linear algebra. **Alternate Stop and Go Generator** • It uses three LFSRs of different length.LFSR-2 is clocked when the output of LFSR-1 is 1; • LFSR-3 is clocked when the output of LFSR-1 is 0.The output of the generator is the XOR of LFSR-2 and LFSR-3.This generator has a long period and large linear complexity. • The correlation attack found against LFSR-1,but it does not substantially weaken the generator.There have been other attempts at keystream generators along these lines	4M
1b	**A5:** • A5consist of 3 LFSRs; register lengths are 19, 22 and 23 ; • All the feedback polynomials are sparse. • The output is the XOR of the three LFSRs. • A5 uses variable control clock. Each register is clocked based on its own middle bit, XORed with the inverse threshold function of the middle bits of all three registers. usually two of the LFS of clock in each round. • The basic ideas behind A5 are good. • It is very efficient.It passes all non statistical tests; it's only known weakness is that it's registers are short enough to make exhaustive search feasible.Variants of A5 with the longer shift registers and denser feedback polynomials should be secure.	4M

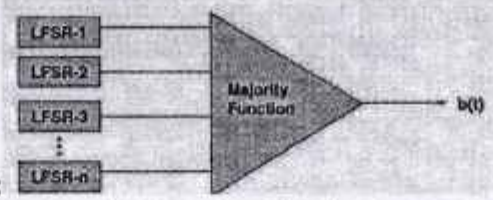
1c

Lets assume that we use three LFSRs, then the output generator can be written as:

$b = (a_1 \wedge a_2) \oplus (a_1 \wedge a_3) \oplus (a_2 \wedge a_3)$ (similar to Geffe)

Linear complexity:

$n_1n_2+n_1n_3+n_2n_3$ (larger than Geffe)



Thresholdgenerator:

4M

1c

Linear feedback shift registers (LFSRs)

- Characteristics:
  - LFSRs are well-suited to hardware implementation
  - Produce sequences of large period
  - Produce sequences with good statistical properties
  - Due to their structure, they can be readily analysed using algebraic techniques

4M

2a.

- Definition:

A *linear feedback shift register* (LFSR) of length L consists of L stages (or delay elements) numbered 0, 1, ..., L-1, each capable of storing one bit and having one input and one output; and a clock which controls the movement of data. During each unit of time the following operations are performed:

(i) the content of stage 0 is output and forms part of the output sequence

(ii) the content of stage I is moved to stage I-1 for each I, $1 \le i \le L-1$

(iii) the new content of stage L-1 is the feedback bit s, which is calculated by adding together modulo 2 the previous contents of a fixed subset of stages 0, 1, ..., L-1

4M

2b.

A widely used technique for pseudorandom number generation is an algorithm first proposed by Lehmer [LEHM51], which is known as the linear congruential method.Linear congruential generators are pseudo random sequence generators of the form $X_n=(aX_{n-1}+b) \bmod m$ in which X_n is the nth number of the sequence, and X_{n-1} is the previous number of the sequence .The variables a,b and m are constants : a is the multiplier,b is the increment ,and m is the modulus. The key or seed is the value of X_0.

The strength of the linear congruential algorithm is that if the multiplier and modulus are properly chosen, the resulting sequence of numbers will be statistically indistinguishable from a sequence drawn at random (but without replacement) from the set 1, 2, c, m - 1. But there is nothing random at all about the algorithm, apart from the choice of the initial value X_0. Once that value is chosen, the remaining numbers in the sequence follow deterministically. This has implications for cryptanalysis.

If an opponent knows that the linear congruential algorithm is being used and if the parameters are known (e.g., $a = 7^5$, $c = 0$, $m = 2^{31} - 1$), then once a single number is discovered, all subsequent numbers are known. Even if the opponent knows only that a linear congruential algorithm is being used, knowledge of a small part of the sequence is sufficient to determine the parameters of the algorithm. Suppose that the opponent is able to determine values for X_0, X_1, X_2, and X_3. Then

$X_1 = (aX_0 + c) \bmod m$

$X_2 = (aX_1 + c) \bmod m$

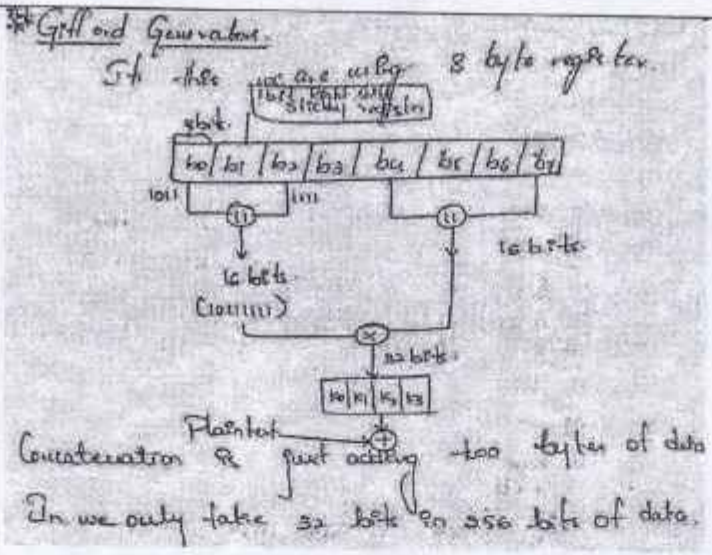
$X_3 = (aX_2 + c) \bmod m$

These equations can be solved for a, c, and m.

4M

2b

*Gifford Generator



4M

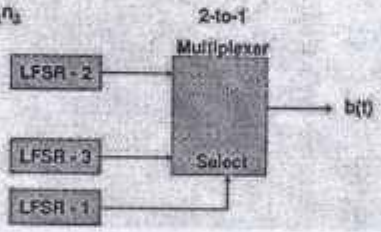
3a.

Geffe Generator

- A combination of three LFSRs
- If a_1, a_2 and a_3 are the outputs of the three LFSRs, the output of the generator can be calculated by the following equation

  $b = (a_1 \wedge a_2) \oplus ((\neg a_2) \wedge a_3)$
- If the LFSRs have lengths n_1, n_2, and n_3, respectively, then the linear complexity of the generator is

  $(n_1+1)n_2+n_1n_3$



4M

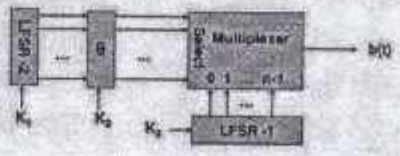
3c.

Bilateral Stop and Go Generator

- This generator uses two LFSRs,both of length 'n'.
- The output of the generator is the XOR of the putputs of each LFSR.
- If the output of LFSR-2 at time t-1 is 0 and at time t-2 is 1,then LFSR-2 does not clock at time 't'.
- Conversely, if the output of LFSR-1 is time t-1 is 0 and the output at t-2 is 1,and if LFSR-1 clocked at time't',then LFSR-2 does not clock at time't'.
- The linear complexity of this system is equal to the period.

Jennings Generator

- Uses a multiplexer to combine two LFSRs
- Multiplexer selects one bit of LFSR-2 for each output bit
- LFSR-1 controls the multiplexer
- A function maps the output of LFSR-2 to the input of the multiplexer
- Key is the initial states of the LFSRs and the mapping function



4M

3a)

$x_{p+q} = \Delta^2 - x_p - x_q = 1^2 - 3 - 5$

$\Rightarrow 1 - 8 = -7 \bmod 11 \Rightarrow 4$

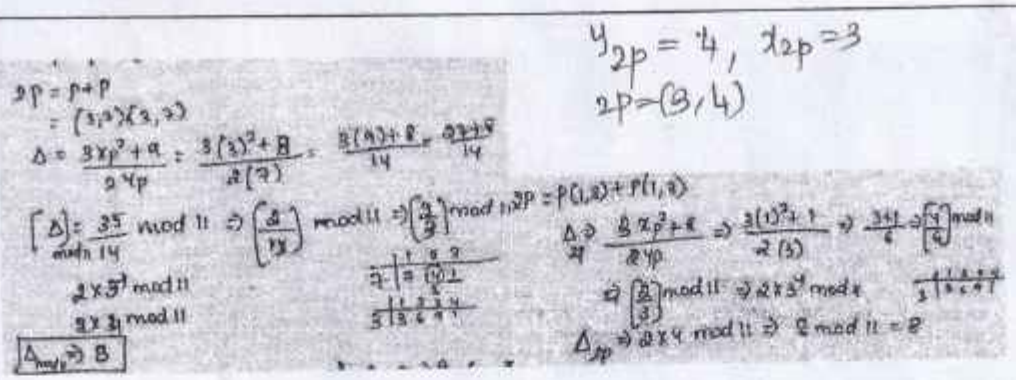
$y_{p+q} = \Delta(x_p - x_{p+q}) - y_p$

$= +1\,(3 - (-7)) - 7$

$y_{p+q} = 1(3+7) - 7 \Rightarrow 10 - 7 = 3$

$p+q = (+4, 3)$

$\Delta = \left[\frac{q-7}{5-3}\right] : \frac{2}{2} = 1$

4a.		4M
4b.	$X_A=1$, $X_B=1$, $Y_A=GX_A=(2,2)$, $X_B=2$, $Y_B=2(2,2)=(10,2)$, =5, $K_A=Y_BX_A=GX_AY_B=(10,2)(1)=(10,2)$, $K_B=Y_AX_B=(10,2)$	4M

Signature of Course In charge

Signature of Module Coordinator

Signature of HOD

K.S. INSTITUTE OF TECHNOLOGY, BENGALURU - 560109
THIRD INTERNAL TEST QUESTION PAPER 2023-24 EVEN SEMESTER

SET: B

USN										

Degree	:	**B. E.,**	**Semester**	:	**VI**
Branch	:	**E&CE**	**Course Code**	:	**21EC642**
Course Title	:	**Cryptography**	**Date**	:	**31st July 2024**
Duration	:	**60 Minutes**	**Max Marks**	:	**20**

Note: Answer **ONE full** question from each part.

K-Levels: K1-Remebering, K2-Understanding, K3-Applying, K4-Analyzing, K5-Evaluating, K6-Creating

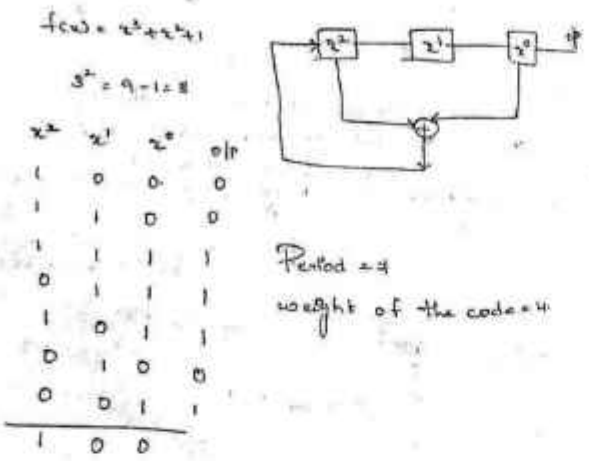
Q No.	Questions	Marks	CO	K-Level
	PART-A			
1(a)	**Make use of** Linear Feedback shift register and explain the working of given $g(x)=1+x^2+x^3$ and find the period & Key generated. Consider initial key value as 1,0,0	4	CO5	K3
(b)	**Explain** the concept of Generalized Geffe generator with an example and definelinearity complex and correlation attack.	4	CO5	K2
(c)	**Explain** Beth Piper Stop & Go generator & Self-Decimated Generators with a neat diagram.	4	CO5	K2
	OR			
2(a)	**Make use of** Linear Feedback shift register and explain the working of given $g(x)=1+x+x^3$ and **solve** the period & Key generated. Consider initial key value as 1,0 0 …	4	CO5	K3
(b)	**Explain** Additive Generators and FISH additive generator.	4	CO5	K2
(c)	**Explain** NANOTEQ and RAMBUTAN	4	CO5	K2
	PART –B			
3(a)	For the given Elliptical equation $Y^2=X^3+2X+8$ in z_{11} field if the given G(2,8).**Solve** public key of user A and B .given $n_A=1, n_B=2$,plain text (2,6),K=1.	4	CO4	K3
(b)	Make use of an Elliptic Curve Arithmetic on the curve of $E_{23}(1,1)$,p=(3,10)q=(9,7) , **Solve** 2P+Q and explain ECC.	4	CO4	K3
	OR			
4(a)	**Solve** P+Q and 2P ,2Q .given P=(2,7) & Q=(4,10) for GF(7).	4	CO4	K3
(b)	**Solve** cipher text for message(1,6) given $E_{23}(1,0)$ .consider n=50,K=1,G(2,8).solve Private and Public key for user A and B G(4,2) and private Key of User A is 1 and B is 2 and Explain ECC encryption algorithm.	4	CO4	K3

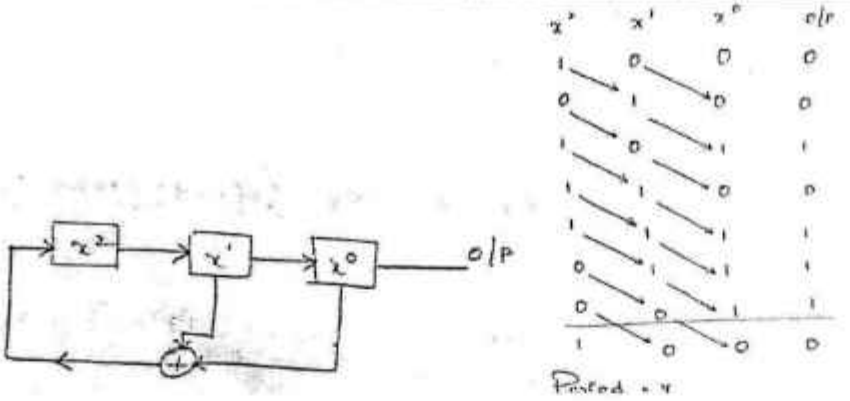
Name & Signature of Course In charge	Name & Signature of Module Coordinator	HOD ECE	Principal

K.S. INSTITUTE OF TECHNOLOGY, BANGALORE - 560109
THIRD INTERNAL TEST 2023-24 EVEN SEMESTER
SCHEME AND SOLUTION for SET B

Degree : B. E
Branch : E&CE
Course Title : Cryptography

Semester: VI A & B
Course Code: 21EC642
Max Marks: 20

Q No.	Points	Marks
1 a		4M
1b	**Linear Complexity** • Definition: An LFSR is said to generate a sequence s if there is some initial state for which the output sequence of the LFSR is s. An LFSR is said to generate a finite sequence s^n if there is some initial state for which the output sequence of the LFSR has s^n as its first n terms. • Definition: The linear complexity of an *infinite* binary sequence s, denoted L(s), is defined as follows: - if s is the zero sequence s = 0, 0, 0, ..., then L(s) = 0 - if no LFSR generates s, then L(s) = ∞ - otherwise, L(s) is the length of the shortest LFSR that generates s. **Generalized Geffe Generator** • Instead of choosing between two LFSRs,this scheme chooses between k LFSRs,as long as k is a power of 2. • More complex than Geffe generator and correlation attack is possible. • Correlation attack is outputs of individual LFSRs can be combined keystream and attacked using linear algebra. Correlation Attack: Cryptographers try to get a high linear complexity by combining the output of several output sequences in some nonlinear manner.The danger is that one or more of the internal output sequences often just outputs of individual LFSRs can be correlated with the combined keystream and attacked using linear algebra.This is called a correlation attack.	4M
1c	**Beth Piper Stop and Go Generator** • It uses the output of one LFSR to control the clock of another LFSR. • The clock input of LFSR-2 is controlled by the output of LFSR-1,So that LFSR -2 can change its state at time 't' only if the output of LFSR-1 was 1 at time t-1. • The linear complexity of the generator is not yet proved in general case. • But,it falls to a correlation attack. **Self-Decimated Generators** • It Control their own clock. • In Rueppel's generator,when the output of the LFSR is 0,the LFSR is clocked 'd' times. • When the output of the LFSR is 1,the LFSR is clocked 'k' times.  (2x2M)	4M

2a.		4M
2b.	Additive Fibonacci generators (AFG) are widely used in cybersecurity devices to generate pseudorandom sequences of bits or numbers. By itself, such a generator is not cryptographically strong. Nevertheless, using it is fundamental to create a completely secure and resistant cryptanalysis algorithm.(2M) Fish is an additive generator based on techniques used in the shrinking generator .It produces a stream of 32 bit words which ccan be XORed with a plaintext stream to produce ciphertext,or XORed with a ciphertext stream to produce plain text.The algorithm is named as it is because it is a Fibonacci shrinking generator. (2M)	4M
2c.	NANOTEQ: • Nanoteq is a South African electronics company . • This is their algorithm that has been fielded by the South African police to encrypt their fax transmissions and for other uses as well. • It uses 127 bit LFSR with a fixed feedback polynomial; the key is the initial state of the feedback register. • The 127 bits of the register are reduced to single key stream bit using 25 primitive cells. • Each input of the function is XORed with some bit of the key. • There is also a secret permutation that depends on the particular implementation .This algorithm is only available in hardware (2M) • RAMBUTAN: It has 112 bit key and can operate in three modes ECB, CBC and 8 bit CFB.This strongly indicates that it is a block algorithm, but rumours point elsewhere. • It is LFSR streamcipher. • it has 5 shift registers each one of a different length around 80 bits. • The feedback polynomials or family sparse with only about 10 taps each. • Each shift register provides for inputs very large and complex non linear function which eventually spits out a single bit.(2M)	4M

3a. 4M

$\Delta = 5$

$x \Rightarrow \Delta^2 - x_P - x_P$

$\Rightarrow 5^2 - 2 - 2 \Rightarrow 25 - 4 = 21 \bmod 11$

$x_B \Rightarrow 10$

$y = \Delta(x_P - x) - y_P \Rightarrow 5(2 - 10) - 8$

$\Rightarrow -48 \bmod 11$

$y_B = 7$

$P_B = (10, 7)$

$n_A = 1$

$P_A = n_A G \Rightarrow 1(2,8) = (2,8)$

$n_B = 2$

$P_B = n_B G \Rightarrow 2(2,8) \Rightarrow (2,8) + (2,8)$

$\Delta = \frac{3(2)^2 + 2}{2(8)} \Rightarrow \frac{3(4)+2}{16} \Rightarrow \frac{12+2}{16} \Rightarrow$

$\Delta \Rightarrow \frac{7}{8} \bmod 11 \Rightarrow 7 \times 8^{-1} \bmod 11$

$C_1[c_x \; c_y]$

$C_y = P_m + kP_B$

$\Rightarrow (2,8) + 1(10,7) \Rightarrow (2,8) + (10,7)$

$\Delta = \frac{7-8}{10-2} \Rightarrow \frac{-1}{8} \Rightarrow 8^{-1} \bmod 11 \Rightarrow 7 \times 8 \bmod 11 \Rightarrow x_3$

$\Delta = 7$

$x_c \Rightarrow \Delta^2 - x_P - x_Q \Rightarrow 7^2 - 2 - 10 \Rightarrow 49 - 12 \Rightarrow 37 \bmod 11$

$x_c = 4$

$y_c \Rightarrow \Delta(x_P - x_c) - y_P \Rightarrow 7(2 - 4) - 8 \Rightarrow 7(-2) - 8 \Rightarrow -14 - 8$

$\Rightarrow -22 \bmod 11$

$y_c = 2$

$C = [C_x \quad (4,2)]$

$C_x \Rightarrow kG \Rightarrow 1(2,8)$

$C = [(2,8) \quad (4,2)]$

3b. 4M

$\Delta_{2P} \Rightarrow \frac{3(3)^2 + 1}{2(10)} \Rightarrow \frac{3(9)+1}{20} \Rightarrow \frac{28}{20}$

$\Rightarrow 5 \times 20^{-1} \bmod 23$

$4^{-1} \bmod 23$

$\Delta_{2P} \Rightarrow 6$

$x_{2P} \Rightarrow 6^2 - 3 - 3 \Rightarrow 36 - 6 \Rightarrow 30 \bmod 23$

$\Rightarrow 7$

$y_{2P} \Rightarrow 6(3 - 7) - 10 \Rightarrow -24 - 10 \Rightarrow 8 \bmod$

$y_{2P} = 12$

$\Delta_{2P+Q} \Rightarrow (7,12) + (9,7)$

$\Delta \Rightarrow \frac{7-12}{9-7} \Rightarrow \frac{-5}{2} \Rightarrow \frac{-5}{2} \bmod 23$

$\Rightarrow -5 \times 12 \bmod 23$

$\Rightarrow -60 \bmod 23$

$\Delta_{2P+Q} \Rightarrow 9$

4a. 4M

$\Delta_{2P} \Rightarrow (2,7) + (2,7)$

$\Delta = \frac{10-7}{6-2} \Rightarrow \frac{3}{2} \bmod 9$

$\Delta = \frac{3(2)^2 + 1}{2(7)} \Rightarrow \frac{3(4)+1}{14} \Rightarrow \frac{13}{14} \bmod 9$

$\Rightarrow 12 \bmod 9 = 5$

$\Delta = 5$

$\Rightarrow \frac{6}{14} \bmod 9 \Rightarrow \frac{3}{7} \bmod 9$

$\Delta = 08$

$\Delta_{2q} \Rightarrow \frac{3(4)^2+1}{2(10)} \Rightarrow \frac{3(16)+1}{20} \Rightarrow \frac{49}{20} \bmod 23 \Rightarrow \frac{2}{20} \bmod 23$

$\Delta_{2q} = 0$

$x_{2q} \Rightarrow 0^2 - 4 - 4 \Rightarrow -8 \bmod 23 \Rightarrow 6$

$y_{2q} \Rightarrow 0(4-6) - 10 \Rightarrow -10 \bmod 23 \Rightarrow 4$

4b.

"User A

$n_A = 2$

$2 < 50$

$P_B = n_B Q \Rightarrow 2(3,8) \Rightarrow (3,8)+(3,8$

$\Delta = \frac{3(3)^2+1}{2(8)} \Rightarrow \frac{3(4)+1}{16} \Rightarrow \frac{13}{16} \bmod 23$

$\Rightarrow \frac{13}{16} \bmod 23 \Rightarrow 13 \times 16^{-1} \bmod 23$

$\Rightarrow 13 \times 9 \bmod 23$

$\Rightarrow 117 \bmod 23$

$\Delta = 09$

$x = \Delta^2 - x_p - x_p \Rightarrow 9^2 - 3 - 3$

$\Rightarrow 75 \bmod 23$

$x = 14$

$y = \Delta(x_p - x) - y_p \Rightarrow 9(3 - 14) - 8$

$\Rightarrow -107 \bmod 23$

$y = 11$

$P_A = (14, 11)$

4M

Signature of Course In charge

Signature of Module Coordinator

Signature of HOD