CBCS SCHEME

USN ☐☐☐☐☐☐☐☐☐☐

21EC642

Sixth Semester B.E. Degree Examination, June/July 2024

Cryptography

Time: 3 hrs. Max. Marks: 100

Note: Answer any FIVE full questions, choosing ONE full question from each module.

Module-1

1 a. Explain the division algorithm with an example. **(07 Marks)**

b. Define Ring. State six properties of Rings. **(07 Marks)**

c. Explain the Euclidean algorithm. Calculate the GCD(60, -24) **(06 Marks)**

OR

2 a. Lists the properties of modular arithmetic for integer in 2n with expression. **(07 Marks)**

b. Explain the polynomial arithmetic. Find polynomial arithmetic over GF(2) for $f(x) = x^7 + x^5 + x^4 + x^3 + x + 1$ and $g(x) = x^3 + x + 1$. **(07 Marks)**

c. Develop set of tables for polynomial arithmetic modulo of $x^3 + x + 1$ over GF(2^3). **(06 Marks)**

Module-2

3 a. Draw and explain model of symmetric encryption. **(07 Marks)**

b. Explain the playfair cipher and its rules for the following keyword : "MONARCHY" plaintext : "Cryptography". **(07 Marks)**

c. Explain the vernam Cipher with a neat diagram. **(06 Marks)**

OR

4 a. Draw and explain model of symmetric cryptosystem. **(07 Marks)**

b. Explain the Caesar Cipher technique Encrypt plaintext "Cryptography" with key = 3. **(06 Marks)**

c. Using Hill Cipher algorithm Encrypt the plaintext "paymoremoney" using the key,

$$K = \begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}$$ **(07 Marks)**

Module-3

5 a. State and prove Euler's theorem. **(05 Marks)**

b. Explain the DES encryption algorithm with neat diagram. **(10 Marks)**

c. Explain Block Cipher with neat diagram. **(05 Marks)**

OR

6 a. Explain Feistel encryption and decryption with neat diagram. **(10 Marks)**

b. State and prove Fermat's theorem. **(05 Marks)**

c. Explain Euler's Totient function. Determine (i) $\phi(37)$ and $\phi(35)$. **(05 Marks)**

Module-4

7 a. Bring out differentiate between conventional encryption and public-key encryption. Explain the requirement of public-key cryptography. **(10 Marks)**

b. Explain RSA algorithm. Using RSA algorithm perform encryption and decryption using p = 17, q = 11, e = 7 and M = 88. **(10 Marks)**

Important Note : 1. On completing your answers, compulsorily draw diagonal cross lines on the remaining blank pages.
2. Any revealing of identification, appeal to evaluator and /or equations written eg, 42+8 = 50, will be treated as malpractice.

OR

8 a. Explain the Diffie-Hellman key exchange algorithm. Evaluate a Diffie-Hellman key exchange for $q = 23$ and $\alpha = 9$.
   (i) If User A has private key $X_A = 4$
   What is A's public key $Y_A = ?$
   (ii) If User B has private key $X_B = 3$
   What is B's public key $Y_B = ?$
   (iii) What is shared key ? **(10 Marks)**

b. Describe Elgamal cryptographic system. **(10 Marks)**

Module-5

9 a. Write short notes on, (i) NANOTEQ (ii) A5 (iii) Linear Congruential generator. **(10 Marks)**

b. Explain Additive generator. **(06 Marks)**

c. With a neat diagram, explain Threshold generator. **(04 Marks)**

OR

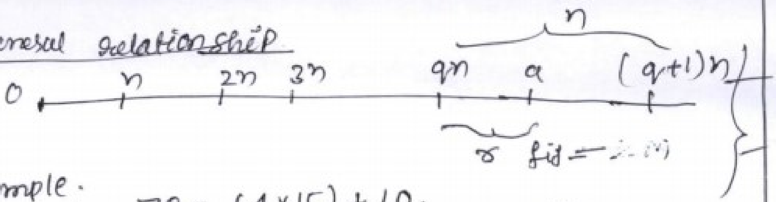
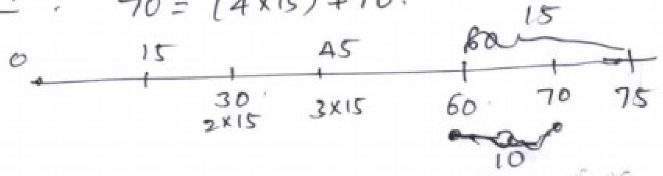
10 a. Explain linear feedback shift register with a neat diagram. **(06 Marks)**

b. With a neat diagram, explain Geffe generator and Jennings generator. **(10 Marks)**

c. Explain Gifford with a neat diagram. **(04 Marks)**

* * * * *

Cryptography (21EC642)
June/July 2024- VTU Question Paper
Scheme and Solutions

Question Number	Solution	Marks Allocated
1.a	**The Division algorithm** Def^n – 1M $a = qn + r \quad 0 \le r < n; \quad q = [a/n)$ General relationship  fig – 2M Example: $70 = (4 \times 15) + 10.$  fig – 2M	1M 2M 2M 2M
1 b.	**Ring** → Def^n. $\{R, +, \times)$ is set of elements with 2 binary operation. Properties: 1) closure under multiplication 2) Associative of multiplication $a(bc) = (ab)c$ 3) Distributive laws: $a(b+c) = ab + ac$ for all $a, b,$ in R $(a+b)c = ac + bc$ in R 4) Commutativity of multiplication $ab = ba$ for a, b in R 5) multiplicative identitity $a1 = 1a$ 6) No zero divisors $ab = 0$. then either $a = 0$ or $b = 0$	1M 6M

Subject Title : . Cryptography **Subject Code :** 21EC642

Question Number	Solution	Marks Allocated
1. c.	Euclidean algorithm 1. c is a divisor of a & of b. 2. Any divisor of a & b is a divisor of c. Euclid(a,b) $gcd(a, b) = max[k, \text{ such that } k \mid a \ \& \ k \mid b]$ if B=0. return A = gcd(a,b) R = A mod B A ← B B ← R $gcd(60, -24) = 12$	4M 2M
2 a.	modular arithmetic properties Expressions 1) commutative laws – $(w+x) \bmod n = (x+w) \bmod n$ $(w \times x) \bmod n = (x \times w) \bmod n$ 2) Associative law. – $[(w+x)+y] \bmod n = [w+(x+y)] \bmod n$ $(w \times x) \times y \bmod n = w \times (x \times y) \bmod n$ 3) Distributive law – $w \times (x+y) \bmod n = (w \times x)+(w \times y) \bmod n$ 4) Identities – $(0+w) \bmod n = w \bmod n$ $(1 \times w) \bmod n = w \bmod n$. 5) Additive Inverse (−w) – for each $w \in Z_n$, there exists a z such that $w+z = 0 \bmod n$	2M 2M 3M
2 b)	polynomial arithmetic ; A polynomial of degree $n \geq 0$. is an expression $f(x) = a_n x^n + a_{n-1} x^{n-1} + \dots + a_1 x + a_0 = \sum_{i=0}^{n} a_i x^i$ Explanation $f(x)$ $x^7 + x^5 + x^4 + x^3 + x + 1$ $g(x)$ $+ (x^3 + x + 1)$ $+$ $x^7 + x^5 + x^4$ = addition a) $= x^7 + x^5 + x^4$ Substraction $= x^7 + x^5 + x^4$ multiplication $= x^{10} + x^4 + x^2 + 1$ Division Quotient – $x^4 + 1$ Remainder – 0	3M 1M 1M 1M 5M

Subject Title : Cryptography **Subject Code :** 21EC642

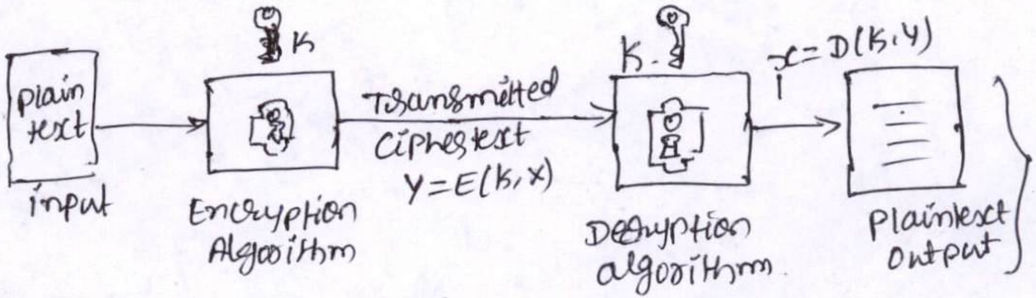
Question Number | **Solution** | **Marks Allocated**

2. c. polynomial modulo (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
0	0	1	x	$x+1$	x^2	x^2+1	x^2+1	x^2+x+1
1	1	0	$x+1$	x	x^2+1	x^2	x^2+x+1	x^2+x
x	x	$x+1$	0	1	x^2+x	x^2+x+1	x^2	x^2+1
$x+1$	$x+1$	x	1	0	x^2+x+1	x^2+x	x^2+1	x^2
x^2	x^2	x^2+1	x^2+x	x^2+x+1	0	1	x	$x+1$
x^2+1	x^2+1	x^2	x^2+x+1	x^2+x	1	0	$x+1$	x
x^2+x	x^2+x	x^2+x+1	x^2	x^2+1	x	$x+1$	0	1
x^2+x+1	x^2+x+1	x^2+x	x^2+1	x	$x+1$	x	1	0

6 M

3. a)



3M

fig. model of ~~con~~symmetric encryption

Each bit Explanation with necessary equations — 4M

3. b) The best-known multiple-letter encryption is the playfair. It is based on use of 5x5 matrix of letter constructed using a keyword.

Keyword: MONARCHY

Rules → 3M

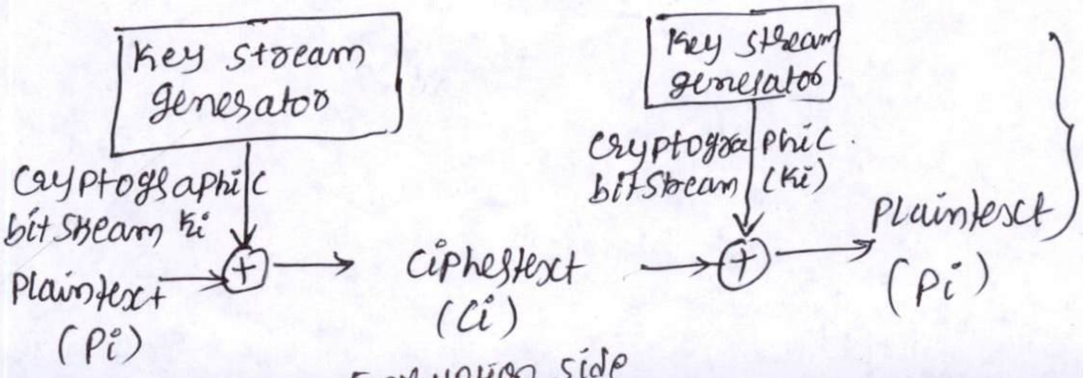
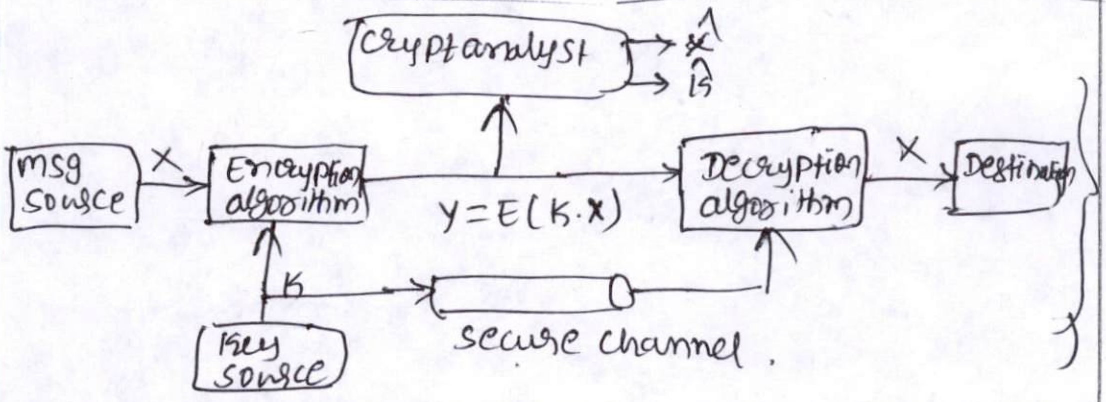
M	O	N	A	R
C	H	Y	B	D
E	F	G	I/J	K
L	P	Q	S	T
U	V	W	X	Z

2M

Plain text: CR YP to graphy

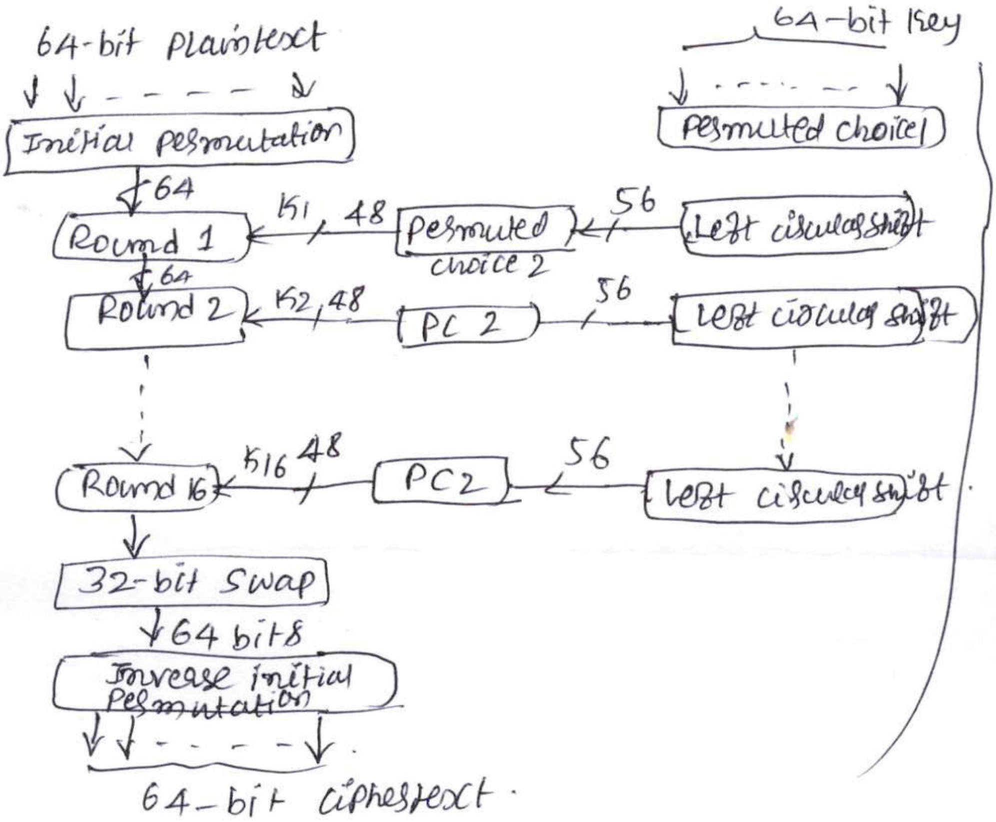
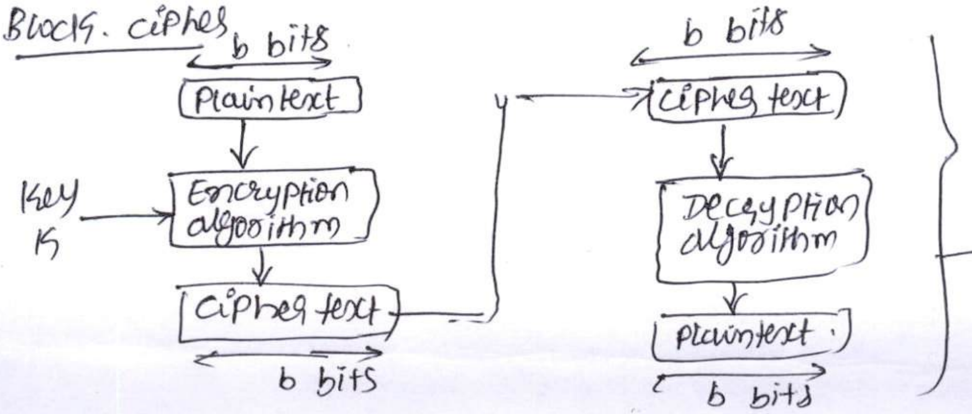
Cipher text : DM HQ PR KNO SYB

2M

Question Number	Solution	Marks Allocated
3.C	Vernam cipher  	3M
	Encryption side Explanation: $\underset{\substack{\downarrow \\ \text{ciphertext}}}{C_i} = P_i \underset{\substack{\downarrow \\ \text{EXOR}}}{\oplus} K_i$ – ith binary digit of key decryption $P_i = C_i \oplus K_i$	3M
4a.	 fig. model of symmetric cryptosystem	3M
	Explanation	4M
4 b)	Caesar cipher: involves replacing each letter of the alphabet with the letter standing three places further down alphabet.	1M
	plaintext: a b c --z ciphertext D E F --C $C = E(K.P) = (P+K) \bmod 26$ $C = E(3,P) = P+3 \bmod 26$ $P = D(K.C) = (C-K) \bmod 26$. $P = D(3.C) = (C-3) \bmod 26$.	3M

Question Number	Solution	Marks Allocated
	Example : " plain text : cryptography cipher text : "FUBSWRJUDSKB"	2M
4.c	Hill cipher : $C = E(K,P) = PK \bmod 26 \longrightarrow$	1M
	Step 1 ; pay mor emo ney [15 0 24] [12, 14, 17] [4 12 14] [13, 4, 24]	2M
	$C = \overset{K}{\begin{bmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{bmatrix}} \overset{P}{\begin{bmatrix} 15 & 12 & 4 & 13 \\ 0 & 14 & 12 & 4 \\ 24 & 17 & 14 & 24 \end{bmatrix}} \bmod 26$ $= \begin{bmatrix} 375 & 527 & 342 & 409 \\ 819 & 861 & 594 & 849 \\ 486 & 375 & 298 & 490 \end{bmatrix} \bmod 26$	2M
	$= \begin{bmatrix} 11 & 7 & 4 & 19 \\ 13 & 3 & 22 & 17 \\ 18 & 11 & 12 & 22 \end{bmatrix} = \begin{bmatrix} L & H & E & T \\ N & D & W & R \\ S & L & M & W \end{bmatrix}$ plain text : pay more money cipher text : LNS HDL EWMTRW	2M
5.a	Euler's theorem : states that for every a and n that are relatively prime : $a^{\phi(n)} \equiv 1 (\bmod n)$	1M
	proof : $R = \{x_1, x_2 -- x_{\phi(n)}\}$ $S = (ax_1 \bmod n), ax_2 \bmod n --ax_{\phi(n)} \bmod n\}$ $a^{\phi(n)} \times \left[\prod_{i=1}^{\phi(n)} x_i\right] = \prod_{i=1}^{\phi(n)} (x_i \bmod n)$ $(a^{\phi(n)} = 1 \bmod n)$	4M

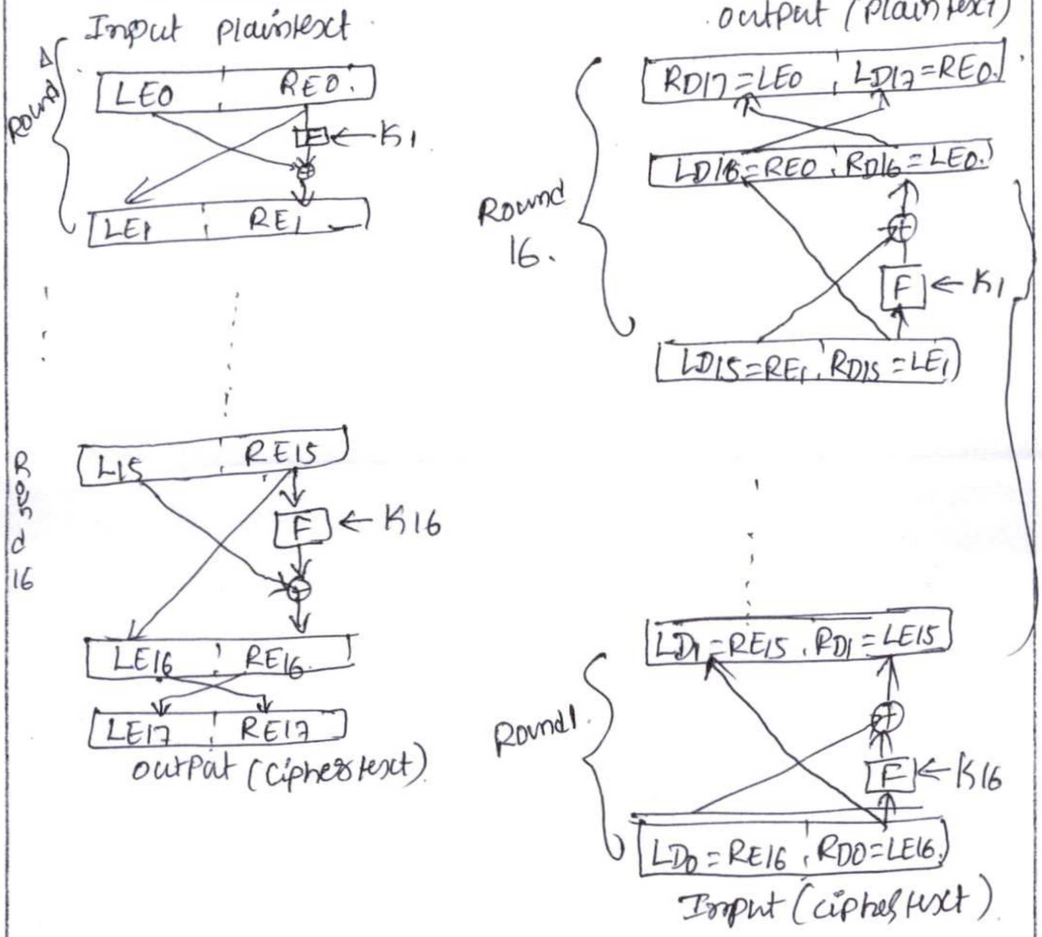
Subject Title : Cryptography Subject Code : 21EC642

Question Number	Solution	Marks Allocated
5.b.	 fig. DES Encryption Explanation → 5M	5M
5.c.	Block cipher  Explaination—2M	3M
6.a.		

Subject Title : Cryptography Subject Code : 21EC642

Question Number | Solution | Marks Allocated

6.a) Feistel Encryption & Decryption



5M

Explanation — 5M

6.b) Fermat's theorem : If p is prime & a is positive integer not divisible by p. then

$$a^{p-1} \equiv 1 (\bmod p)$$

2M

$$a \times 2a \times \cdots \times (p-1)a = [1 \times 2 \times \cdots \times p-1] \bmod p$$

$$a^{p-1}(p-1)! = (p-1)! \bmod p$$

$$a^{p-1} = 1 \bmod p$$

proof

3M

6.c Euler's Totient function. — Explanation → 2

$\phi(n)$

~~$\phi(37)$ = 1 2 3 4 5 6~~

$\phi(37) = 36$

$\phi(35) = 24$

3M

Subject Title : Cryptography   Subject Code : 21EC642

Question Number	Solution	Marks Allocated
7 a.	See comparison below	5M

conventional Encryption	public-key Encryption
1. same key is used for encryption & Decryption	1. seperate key for Encryption & decryption. (pair of key)
2. sender & rcr must share the algorithm & key.	2. one of the matched pair of key
3. key must be kept secret	3. one of the 2 keys must be kept secret.
4. algorithm plus ciphertext insufficient to determine the key.	4. to determine the other key
5. It must be impossible to decipher a msg if the key is secret	5. If one of key is secret.

7b. Requirement of public-key cryptography

1. public key PUb, private key PRb.
2. $C = E(PU_b, M)$
3. $M = D(PR_b, C) = D[PR_b, E(PU_b, M)]$
4. It is computationaly infeasible for knowing the public key PUb to determine the private key, PRb
5. knowing the public key PUb, & ciphertext C to recover the original msg. M
6. $M = D[PU_b, E(PR_b, M)] = D[PR_b, E(PU_b, M)]$

5M

7.b RSA algorithm.

1. p, q. two prime number.
2. $n = pq$. $\phi(n) = (p-1)(q-1)$
3. e with $\gcd(\phi(n), e) = 1$; $1 < e < \phi(n)$
4. $d = e^{-1} \pmod{\phi(n)}$
5. $C = M^e \bmod n$ — ciphertext
6. $M = C^d \bmod n$ — Decrypt.

5M

→ $p = 17$, $q = 11$

$n = pq = 11 \times 17 = 187$

$\phi(n) = (p-1)(q-1) = 16 \times 10 = 160$.

$e = 7$.

$C = 88^7 \bmod 187 = 11$

$M = 11^{23} \bmod 187 = 88$.

$d = 23$.

5M.

8.a. Diffie-Hellman key exchange Algorithm

Alice		Bob.
Alice & Bob share a prime numbers q and an integer α, such that α < q & α is primitive root of q		Prime no. q & α such that α < q & α is a primitive root of q
Alice generate a private key X_A such that $X_A < q$.		Bob. generate a private key X_B = ~~α~~$^{X_B} < q$ ~~mod~~
Alice calculates a public key $Y_A = \alpha^{X_A} \bmod q$	Y_A Y_B	Bob calculate a public key $Y_B = \alpha^{X_B} \bmod q$
Alice receives Bob's public key Y_B in plaintext		Bob receives Alice's public key Y_A in plaintext
Alice calculates shared secret key $K = (Y_B)^{X_A} \bmod q$		Bob calculates shared $K = (Y_A)^{X_B} \bmod q$.

5M

$q = 23 \quad \alpha = 9. \quad X_A = 4, \quad X_B = 3$

$Y_B = \alpha^{X_B} \bmod q \qquad Y_A = \alpha^{X_A} \bmod q$

$Y_B = 9^3 \bmod 6 = 16, \qquad Y_A = 9^4 \bmod 23 = 6.$

$\boxed{Y_A = 6, \ Y_B = 16.}$ — 3M

$K_A = (Y_B)^{X_A} \bmod q \qquad K_B = (Y_A)^{X_B} \bmod q$

$= (16)^4 \bmod 23 = 9 \qquad = (6)^3 \bmod 23 = 9$

$\boxed{K_A = K_B = 9.}$ — 2M.

8.b. Elgamal cryptographic system

- It is used in Digital signature standard.

Global public elements

q → prime no. α α < q & α a primitive root of q.

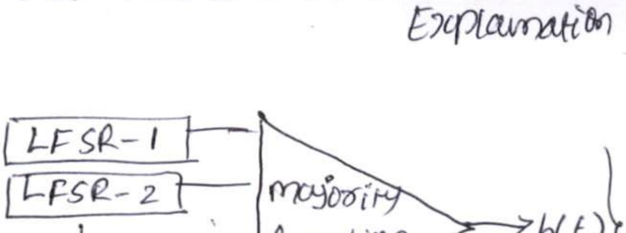
Key generation ~~for~~ by. Sender side

Select Private X_A $X_A < q - 1.$

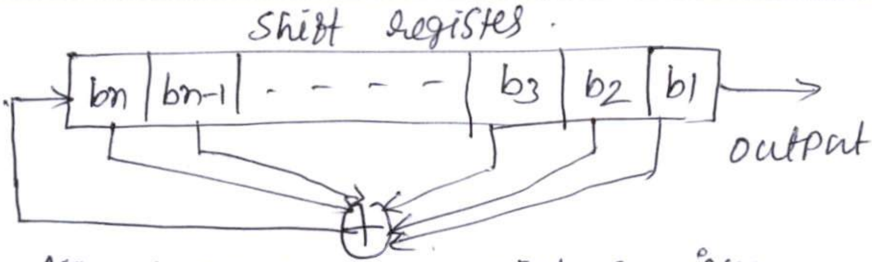
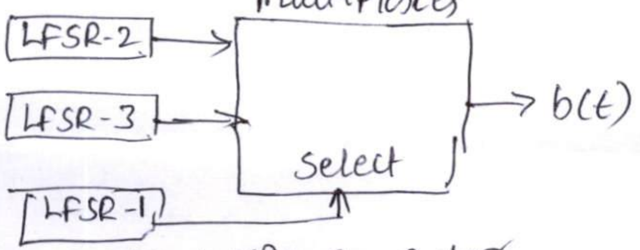
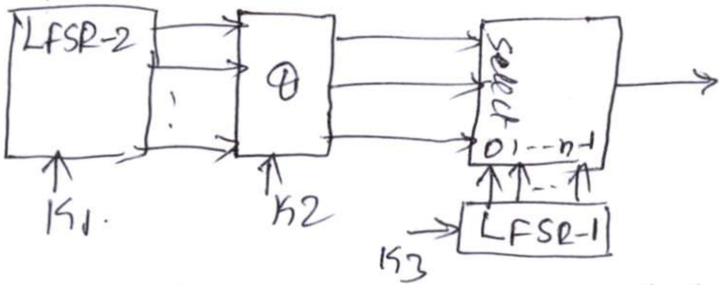
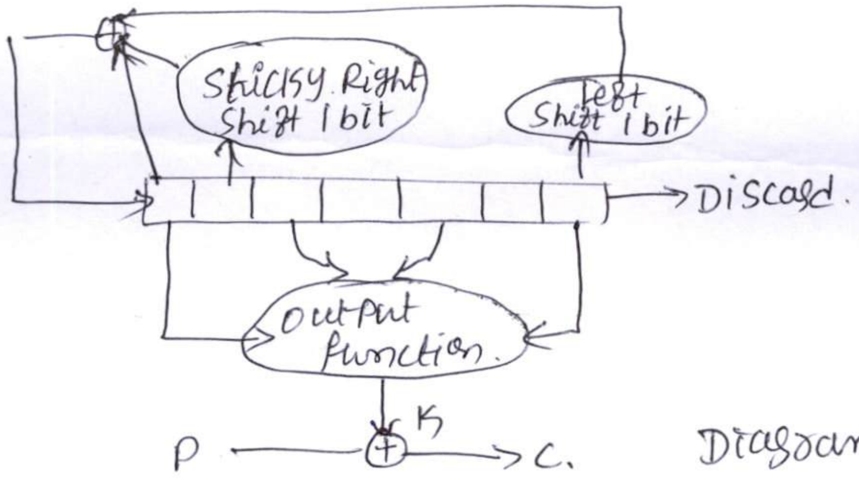
Calculate Y_A $Y_A = \alpha^{X_A} \bmod q.$

Public key {q, α, Y_A}

3M

Question Number	Solution	Marks Allocated
	Encrypt by Receiver with Send public key. plaintext $M<q$, select random integer $K<q$ $K=(Y_A)^K \bmod q$, $C_1=\alpha^K \bmod q$, $C_2=KM \bmod q$ ciphertext C_1, C_2.	→ 2M
	Decryption $C1, C_2$ calculate $K=(C_1)^{X_A} \bmod q$ plaintext $M=C_2 K^{-1} \bmod q$	2M
	Explanation	3M
9.a.	i) Nanoteq – It use 127-bit LFSR with a fixed f/b polynomial., the K is initial state of the f/b register. explanation.	3M 2M
	ii) A5 → - Stream cipher used to encrypt GSM. Explanation	4M
	iii) Linear congruential generator → Pseudo random sequence generator. $X_n = \{a.X_{n-1}+b) \bmod M$ Explanation	4M.
9.b.	Additive generator The ith ~~gen~~ word of the generator is $X_i = \{X_{i-a}+X_{i-b}+X_{i-c}+\cdots+X_{i-m}) \bmod 2^n$ Explanation	5M 6M
9.c.	Threshold generator  	2M
	Explanation	2M.

Subject Title : Cryptography Subject Code : 21EC642

Question Number	Solution	Marks Allocated
10.a	 fig - linear feedback shift register Explanation	3M 3M
10.b	2 to 1 multiplexer  fig. Geffe generator diagram - Explanation -	3M 2M
	 fig. Jennings generator Explanation	3M 2M
10.c	 fig. Gifford Diagram Explanation	2M 2M