CBCS SCHEME

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

21IS71

Seventh Semester B.E./B.Tech. Degree Examination, Dec.2024/Jan.2025
Cryptography and Network Security

Time: 3 hrs. Max. Marks: 100

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

Module-1

1 a. Draw the simplified model of symmetric encryption and explain it. **(06 Marks)**

b. Explain caeser cipher with example. **(04 Marks)**

c. Explain playfair cipher algorithm. Find the cipher text for plain text = "instruments" with key = "MONARCHY". **(10 Marks)**

OR

2 a. Encrypt the plaintext "Cryptography" using Hill Cipher algorithm with key $K = \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$ and decrypt the same. **(10 Marks)**

b. With a neat schematic diagram, explain the DES encryption algorithm. **(10 Marks)**

Module-2

3 a. With a neat diagram, explain the six ingredients of a public-key cryptography. **(06 Marks)**

b. Explain the requirements and applications for public key cryptography. **(04 Marks)**

c. Explain the Elganal crypto system. **(10 Marks)**

OR

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

b. Explain the Diffe-Hellman key exchange algorithm. **(10 Marks)**

Module-3

5 a. With a neat diagram, explain public key Authority and Public key certificates techniques for distribution of public keys. **(10 Marks)**

b. Explain the key distribution scenario with relevant diagram. **(10 Marks)**

OR

6 a. Explain secret key distribution with confidentiality and authentication, with a neat diagram. **(10 Marks)**

b. With a neat diagram, explain control vector Encryption and Decryption. **(10 Marks)**

Module-4

7 a. Describe Public key infrastructure, with neat diagram. **(10 Marks)**

b. Explain Remote user – Authentication principles. **(10 Marks)**

OR

8 a. With a neat diagram, explain the general format of X.509 certificate. **(10 Marks)**

b. Explain the differences between Kerberos version 4 and version 5 and also mention the technical deficiencies in Kerberos version 4 protocols. **(10 Marks)**

Module-5

9	a.	Describe in detail PGP (Pretty Good Privacy) cryptographic functions.	(10 Marks)
	b.	Describe the various header fields defined in MIME.	(05 Marks)
	c.	List the important features of IKE key determination algorithm.	(05 Marks)

OR

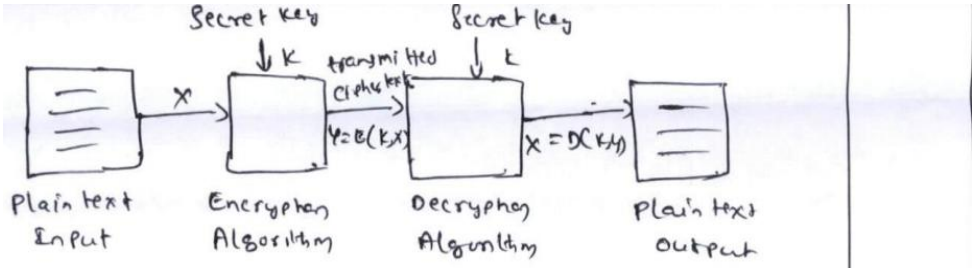
10	a.	Explain the Applications and Benefits of IPsec.	(10 Marks)
	b.	With a neat diagram, describe IKE header and payload format.	(10 Marks)

* * * * *

VTU QUESTION PAPER - Jan. 2025

Cryptography and Network Security (21IS71)

SCHEME & SOLUTION

Question No	Solution & Marks Allocation
1	1.a  Block Diagram ⟶ 2M Explanation of plaintext, Encryption algorithm, secret key, ciphertext, Decryption algorithm. ⟶ 4M 1.b Brief explanation of caesar cipher ⟶ 2M Any example ⟶ 2M 1.c Explanation of four rules of playfair cipher to perform Encryption ⟶ 4M Plaintext: IN ST RU ME NT SX key: MONARCHY 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 ⟶ 6M CIPHER TEXT: GD A TL M Z CL RG XA

2

2. a

Plaintext : CRYPTOGRAPHY Key = $\begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix}$

Encryption => $C = P \cdot K \bmod 26$

Decryption => $P = C \cdot K^{-1} \bmod 26$

Encryption :

"CR" => $[2 \quad 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 \Rightarrow [25 \quad 25] = [2\ X]$

"YP" => $[24 \quad 15] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 \Rightarrow [5 \quad 19] = [F\ T]$

"TO" => $[19 \quad 14] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 \Rightarrow [7 \quad 18] = [H\ S]$

"GRA" => $[6 \quad 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 \Rightarrow [9 \quad 13] = [J\ N]$

"AP" => $[0 \quad 15] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 \Rightarrow [23 \quad 17] = [X\ R]$

"HY" => $[7 \quad 24] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \bmod 26 = [1 \quad 14] \Rightarrow [B\ O]$

Ciphertext C => 2X FT HS JN XB RO → 4M

Finding K^{-1}

$K^{-1} = \frac{1}{\det K} \times \text{adj } K \bmod 26$

$K^{-1} = \frac{1}{43} \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix} \bmod 26$

$\det K = 43$

$\text{adj } K = \begin{bmatrix} 7 & -4 \\ -5 & 9 \end{bmatrix}$

Multiplicative Inverse of $43^{-1} = 23$

$K^{-1} = \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix}$ → 2M

Decryption :

"2X" => $[25 \quad 23] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 = [2 \quad 17] = [C\ R]$

"FT" = $[5 \quad 19] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 \Rightarrow [24 \quad 15] = [Y\ P]$

"HS" = $[7 \quad 18] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 \Rightarrow [19 \quad 14] \Rightarrow [T\ O]$

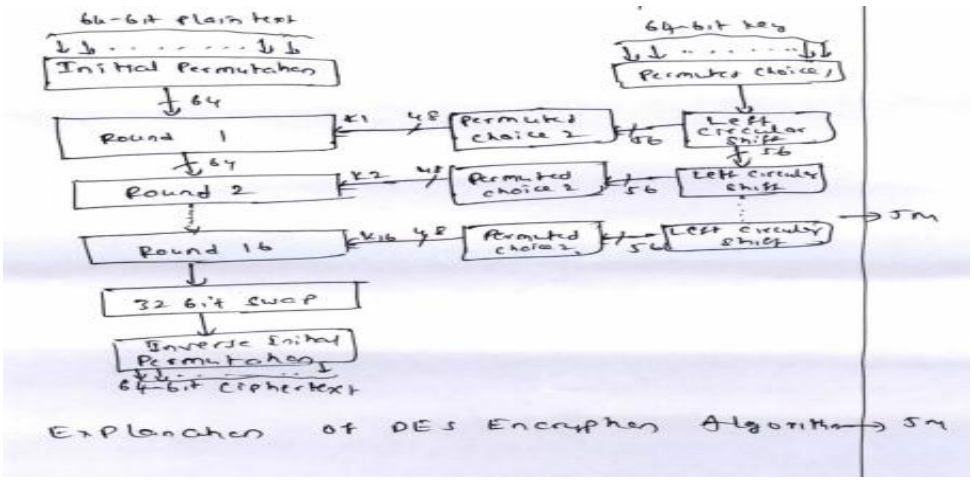
"JN" = $[9 \quad 13] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 \Rightarrow [6 \quad 17] = [G\ R]$

"XB" => $[23 \quad 1] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 \Rightarrow [0 \quad 15] \Rightarrow [A\ P]$

"RO" => $[17 \quad 14] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \bmod 26 \Rightarrow [7 \quad 24] = [H\ Y]$

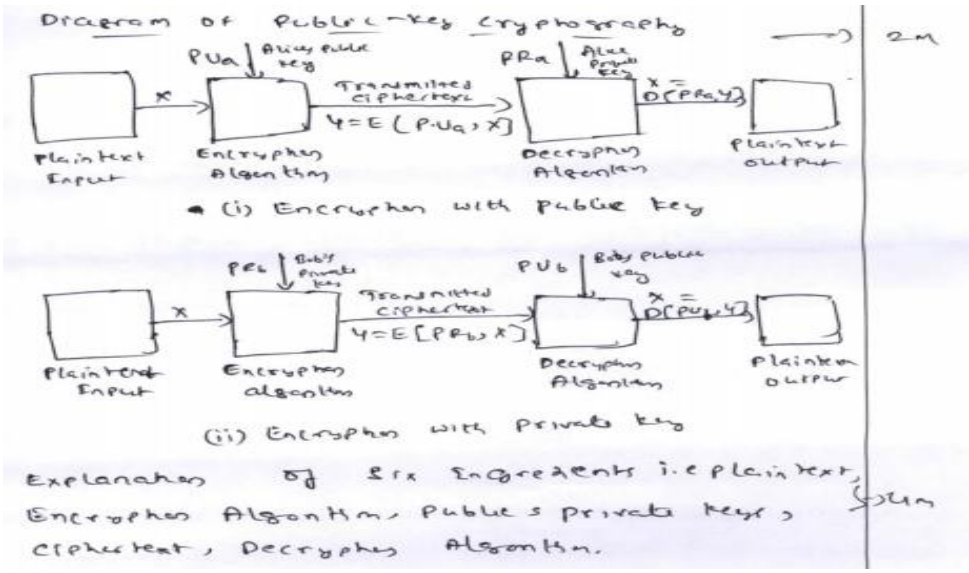
Plaintext => CRYPTOGRAPHY → 4M

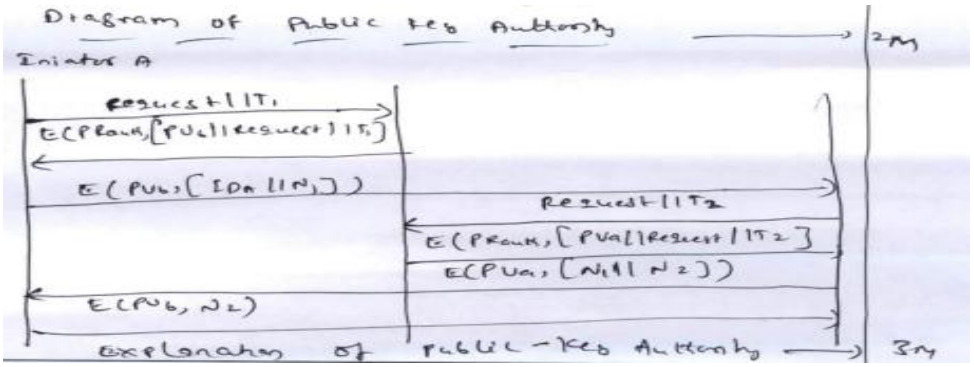
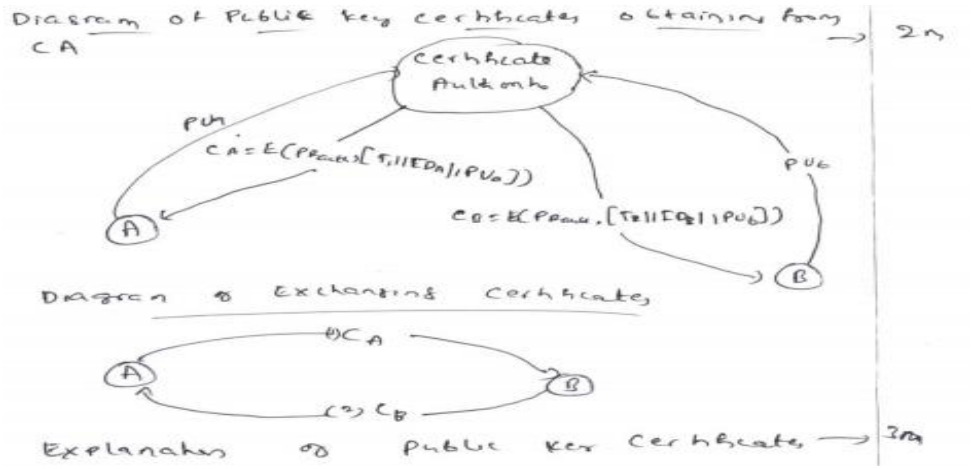
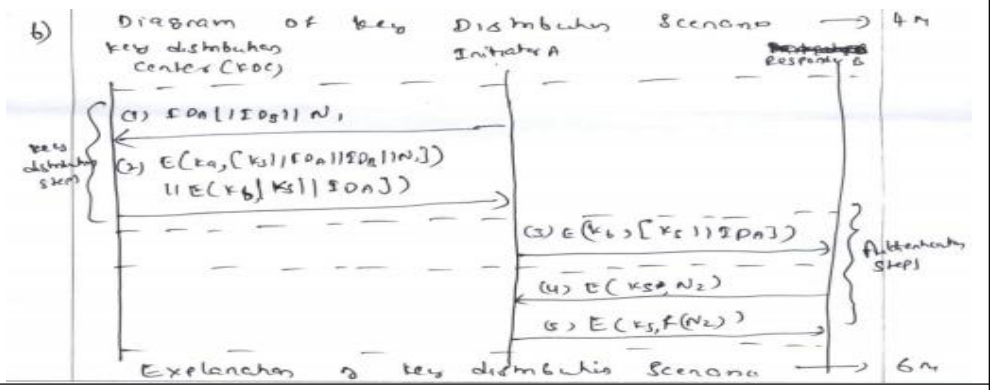
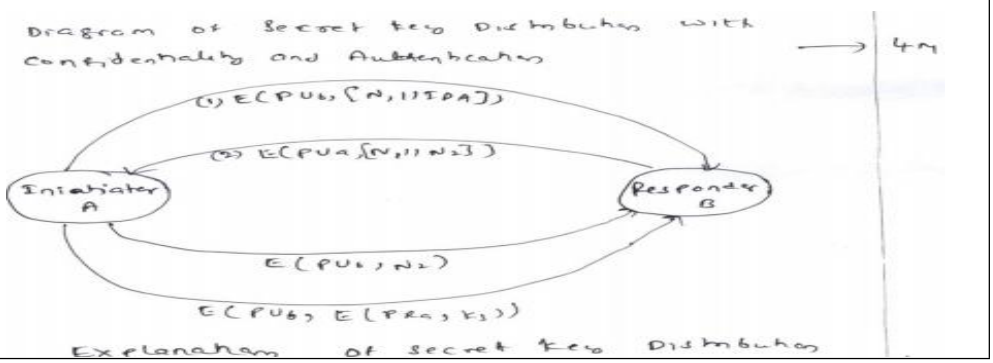
2.b



→ 3M

Explanation of DES Encryption Algorithm → 5M

3	a.  Explanation of six ingredients i.e plaintext, Encryption Algorithm, Public & private keys, ciphertext, Decryption Algorithm. → 4M b. Requirement for Public key cryptography → 2M Application for public key cryptography → 4M c. Elgamal Cryptosystem Explanation * Global public Elements * key Generation by Alice * Encryption by Bob with Alice public key → 4M * Decryption by Alice with Alice's private key Brief explanation of above 4
4	a. Explanation of RSA Algorithm → 5M P = 17, q = 11, e = 7 n = p × q = 17 × 11 = 187 Φ(n) = (p−1)(q−1) = 16 × 10 = 160 de ≡ 1 (mod 160) and d < 160 d = 23 Because 23 × 7 = 161 mod 160 = 1 Public key = {7, 187}, private key = {23, 187} Encryption: C = m^e mod n → 5M = 88^7 mod 187 = 11 Decryption: m = c^d mod n = 11^23 mod 187 = 88 b. The Diffie-Hellman key exchange algorithm → 5M Explanation Global Public elements → 1M User A Key Generation → 1M User B Key Generation → 1M calculating of Secret key by user A → 1M calculating of secret key by user B → 1M

5	a.   b. 
6	a. 

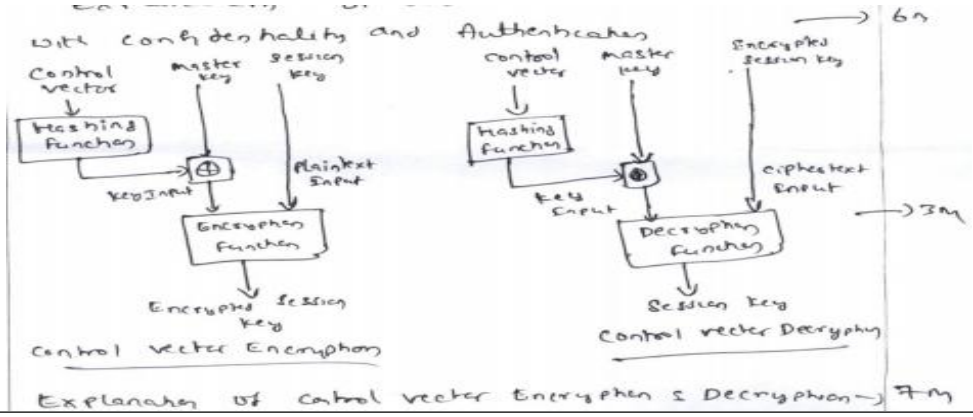
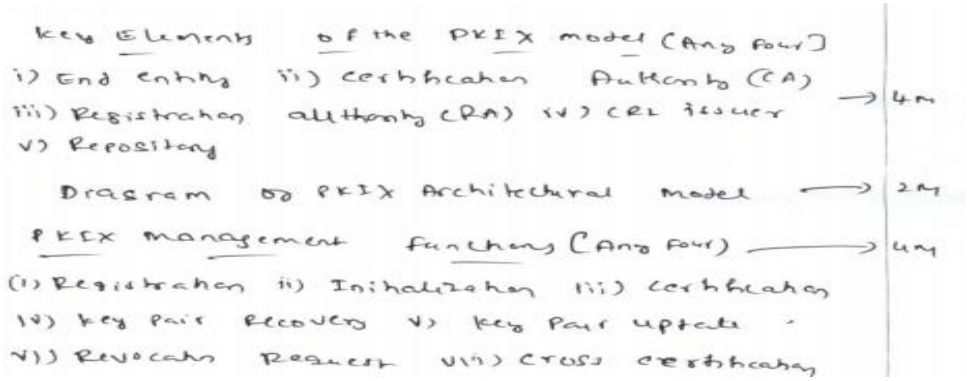
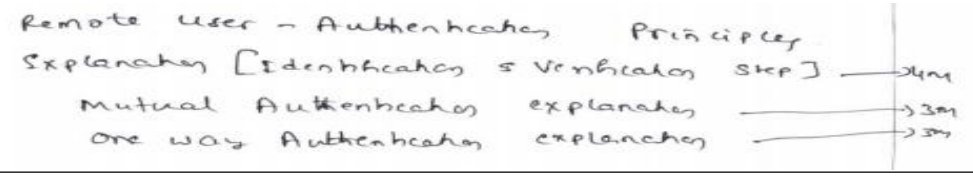
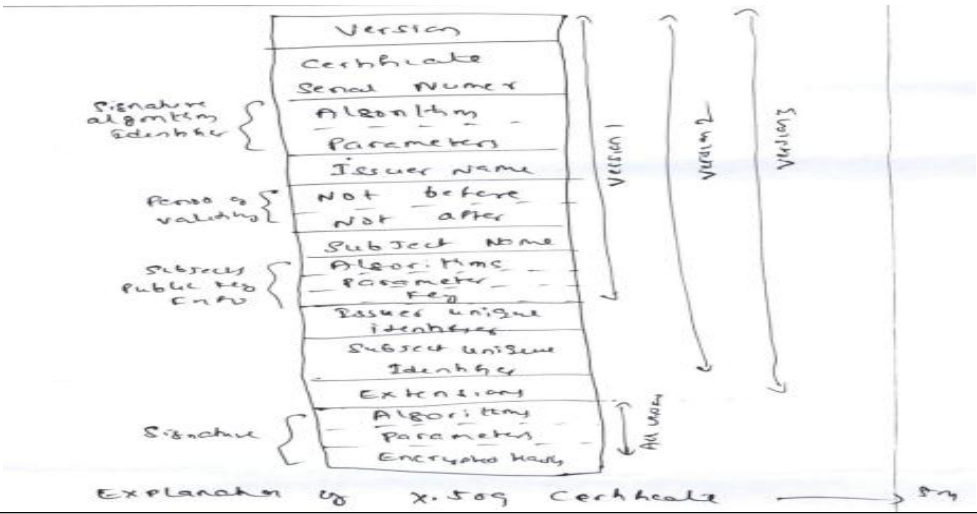
	b. 
7	a.  b. 
8	a. 

	Diagram shows the general format of X.509 certificate b. Differences between Version 4 & 5 of Kerberos → 6M Technical Deficiencies of Version 4 → 4M	5 M
9	a. Any 2 cryptographic functions Explanation i) Authentication only ii) Confidentiality only iii) Confidentiality + Authentication For Diagrams b. Five Header fields defined in MIME are i) MIME Version ii) Content type iii) Content-transfer-Encoding iv) Content-ID v) Content-Description Explanation of each carries one mark c. Listing the five important features of IKE key determination algorithm each carries one mark	6M 4M 5M 5M
10	a. Benefit of IPSec Applications of IPSec b. Diagram of IKE Header Bit: 0 8 16 24 31 Initiator's security Parameter index (SPI) Responder's security Parameter index (SPI) Next Payload 8 | Major Ver 4 | Minor Ver 4 | Exchange type 8 | Flags 8 Message ID Length Explanation of fields Diagram of Payload Header 0 8 16 31 Next Payload | C | Reserved | Payload Length Explanation	6M 6M 3M 2M 3M 2M 3M