

CBCS SCHEME



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)

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.

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

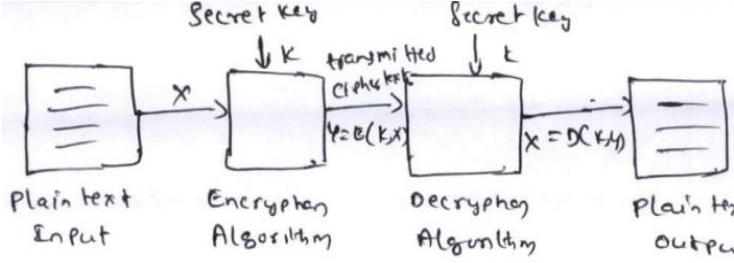
OR

**CMRIT LIBRARY
BANGALORE - 560 037**

VTU QUESTION PAPER - Jan. 2025

Cryptography and Network Security (21IS71)

SCHEME & SOLUTION

Question No	Solution & Marks Allocation																									
1	<p>1.a</p>  <p>Block Diagram → 2m</p> <p>Explanation of plaintext, Encryption algorithm, secret key, ciphertext, Decryption algorithm. → 4m</p>																									
1.b	<p>Brief explanation of Caesar Cipher → 2m</p> <p>Any example → 2m</p>																									
1.c	<p>Explanation of four rules of Playfair cipher to perform Encryption → 4m</p> <p>Plaintext: IN ST RU ME NT SX Key: M MONARCHY</p> <table border="1" style="margin-left: auto; margin-right: auto;"> <tr> <td>M</td><td>O</td><td>N</td><td>A</td><td>R</td></tr> <tr> <td>C</td><td>H</td><td>Y</td><td>B</td><td>D</td></tr> <tr> <td>E</td><td>F</td><td>Q</td><td>S</td><td>K</td></tr> <tr> <td>L</td><td>P</td><td>G</td><td>T</td><td></td></tr> <tr> <td>U</td><td>V</td><td>W</td><td>X</td><td>Z</td></tr> </table> <p>→ 6m</p> <p><u>CIPHER TEXT: EDA TLM2 CL PQ XA</u></p>	M	O	N	A	R	C	H	Y	B	D	E	F	Q	S	K	L	P	G	T		U	V	W	X	Z
M	O	N	A	R																						
C	H	Y	B	D																						
E	F	Q	S	K																						
L	P	G	T																							
U	V	W	X	Z																						

2

2. a

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

Encryption: $C = P \cdot K \pmod{26}$

Decryption: $P = C \cdot K^{-1} \pmod{26}$

Encryption:

$$\text{"CR"} \Rightarrow [2 \ 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \pmod{26} \Rightarrow [25 \ 23] = [2 \ X]$$

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

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

$$\text{"EN"} \Rightarrow [6 \ 17] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \pmod{26} \Rightarrow [9 \ 13] = [\text{J N}]$$

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

$$\text{"HU"} \Rightarrow [7 \ 24] \begin{bmatrix} 9 & 4 \\ 5 & 7 \end{bmatrix} \pmod{26} \Rightarrow [1 \ 14] = [\text{L O}]$$

Ciphertext ($C \Rightarrow 2 \ X \ \text{FT} \ \text{HS} \ \text{JN} \ \text{XB} \ \text{BO}$) $\rightarrow 4m$

Finding K^{-1}

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

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

$$\det K = 43$$

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

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

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

Decryption:

$$\text{"2X"} \Rightarrow [25 \ 23] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [2 \ 17] = [\text{CR}]$$

$$\text{"FT"} \Rightarrow [5 \ 19] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [24 \ 15] = [\text{YP}]$$

$$\text{"HS"} \Rightarrow [7 \ 18] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [19 \ 14] = [\text{TO}]$$

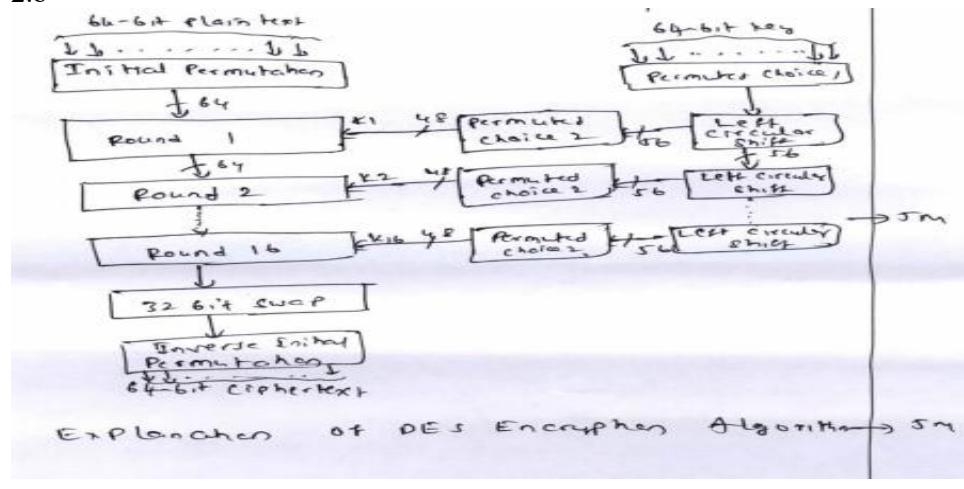
$$\text{"JN"} \Rightarrow [9 \ 13] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [6 \ 17] = [\text{EN}]$$

$$\text{"XB"} \Rightarrow [23 \ 17] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [0 \ 15] = [\text{AP}]$$

$$\text{"BO"} \Rightarrow [1 \ 14] \begin{bmatrix} 5 & 12 \\ 15 & 25 \end{bmatrix} \pmod{26} = [7 \ 24] = [\text{HU}]$$

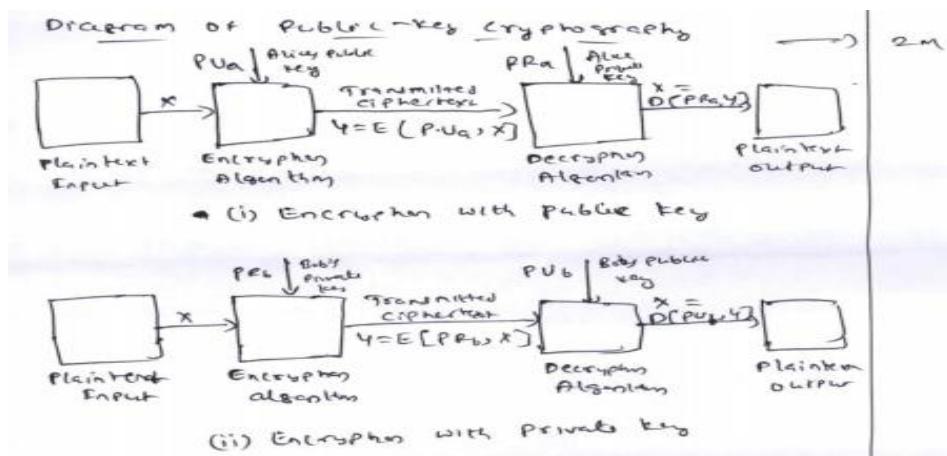
Plaintext \Rightarrow CRYPTOGRAPHY $\rightarrow 4m$

2.b



3

a.



Explanation of six ingredients i.e. plaintext, Encryption Algorithm, Public & private keys, Ciphertext, Decryption Algorithm.

b.

Requirements for Public Key Cryptography → 6M
Applications for Public Key Cryptography → 6M

c.

ElGamal Cryptosystem Explanations

- Global public Elements
- key generation by Alice
- Encryption by Bob with Alice's public key
- Decryption by Alice with Alice's private key

6M

Brief explanation of above 4

4

a.

Explanation of RSA algorithm → 5M

$$\begin{aligned}
 p &= 17, q = 11, n = 7 \\
 n &= p \times q = 17 \times 11 = 187 \\
 \phi(n) &= (p-1)(q-1) = (16 \times 10) = 160 \\
 de &\equiv 1 \pmod{160} \Rightarrow d < 160 \\
 d &= 23 \text{ Because } 23 \times 7 = 161 \pmod{160} = 1 \\
 \text{Public Key} &= \{7, 187\} \text{ & private key} = \{23, 187\} \\
 \text{Encryption: } c &= m \text{ mod } n \\
 &= 887 \text{ mod } 187 = 17 \\
 \text{Decryption: } m &= c^d \text{ mod } n \\
 &= 11^{23} \text{ mod } 187 = 88
 \end{aligned}$$

b.

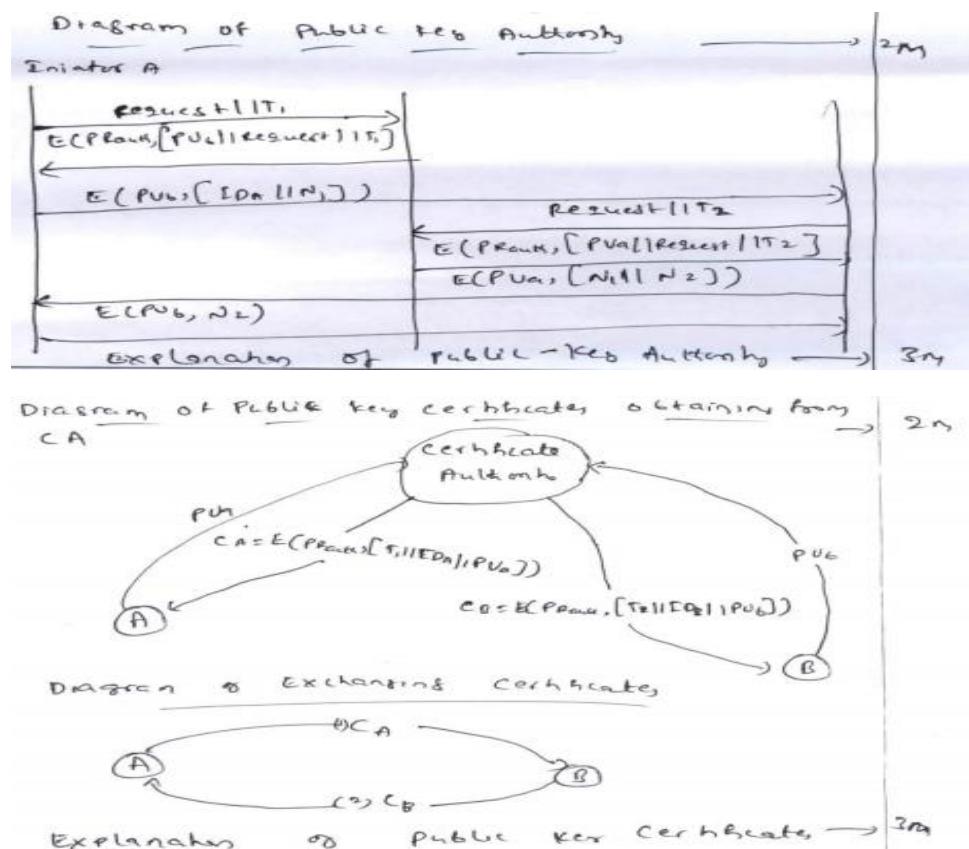
The Diffie-Hellman key exchange algorithm

Explanations

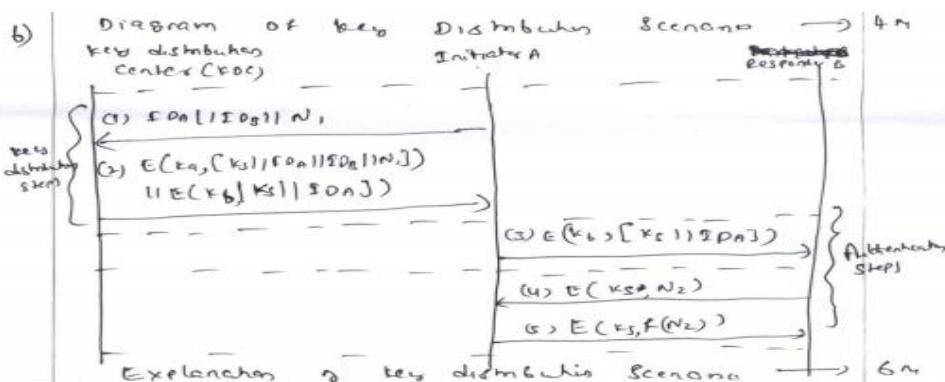
- Global Public elements → 1M
- User A key generation → 1M
- User B key generation → 1M
- calculating of secret key by user A → 1M
- calculating of secret key by user B → 1M

5

a.

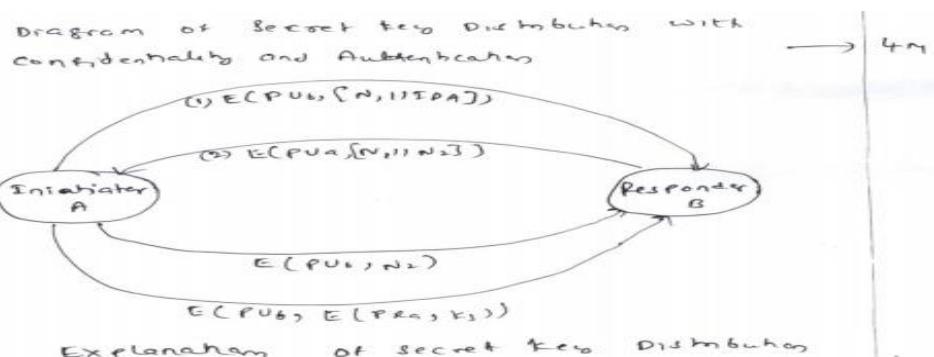


b.



6

a.



	b.
	<p>With confidentiality and Authentica Control vector master session key Hashing Function Key Input Encipher Function Encrypted session key Control vector Encryption</p> <p>Authenticators Control vector master key Hashing Function Key Input Decipher Function Session Key Control vector Decryption</p> <p>Encrypted session key Ciphertext Input Session Key Control vector Decryption</p> <p>Explanation of Control vector Encryption & Decryption → 7M</p>
7	<p>a.</p> <p><u>Key Elements of the PKIX model (Any Four)</u></p> <ol style="list-style-type: none"> End entity Certificate Authority (CA) Registration authority (RA) CRL issuer Repository <p>Diagram of PKIX Architectural Model → 2M</p> <p><u>PKIX management functions (Any Four)</u> → 4M</p> <ol style="list-style-type: none"> Registration Initialization Certification Key Pair Recovery Key Pair update Revocation Request Cross certification
8	<p>b.</p> <p>Remote user - Authentication Principle</p> <p>Explanation [Identification & Verification step] → 2M</p> <p>Mutual Authentication explanation → 3M</p> <p>One way Authentication explanation → 3M</p> <p>a.</p> <p>Version Certificate Serial Number Algorithm Parameters Issuer Name Not before Not after Subject Name Algorithm Parameters Issuer Unique Identifier Subject Unique Identifier Extensions Algorithm Parameters Encrypted Keys</p> <p>Signature algorithm identifier Period of validity Subject public key Signature</p> <p>Explanation of X.509 Certificate → 8M</p>

	<p>Diagram shows the general format of X.509 certificate</p> <p>b.</p> <p>Differences between Version 4.5 & Kerberos Technical deficiencies of Version 4</p>	5m
9	<p>a.</p> <p>Per P cryptographic Function Explanation i) Authentication only ii) Confidentiality only iii) Confidentiality & Authentication Per Diagrams</p> <p>b.</p> <p>Five Header fields defined in MIME are i) MIME version ii) Content-type iii) Content-transfer-Encoding iv) Content-SP v) Content-Description Explanation of each comes one mark</p> <p>c.</p> <p>Listing the five important features i) IKE key determination algorithm each comes one mark</p>	6m
10	<p>a.</p> <p>Benefits of IPsec Applications of IPsec</p> <p>b.</p> <p>Diagram of IKE Header Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Initiator's security Parameter index (20s) Responder's security Parameter Index (20s) Next Payload [4] [4] Exchange ID [8] Flags [8] Message ID Length Explanation of fields</p> <p>Diagram of Payload Headers Bit: 0 1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31 Next Payload [8] Reserved [16] Payload Length [31]</p>	6m