*Total number of printed pages:* **Programme(UG)/7th Semester/UCSE714**

**2023**

***Cryptography and Network Security***

*Full Marks: 100*

Time: Three hours

***Answer any Five questions.***

| | | | |
|---|---|---|---|
| 1. | a) | i) Differentiate between Public key and Private key Cryptography in details with the help of diagram.<br>ii) Write two advantages and disadvantages of these. | 6+4=10 |
| | b) | Discuss the principles of Security Services. When we can ensure that our system is Secure? | 8+2=10 |
| 2. | | a) What is RSA. Write the algorithm of RSA.<br>b) In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then find the private key of A.<br>c) Consider the RSA algorithm with p =11 and q = 3.<br>i) Consider e=6 and e = 7. Which would be an appropriate choice for public key of A and why?<br>ii) Having made your choice, compute the public key and corresponding private key.<br>d) What are the major vulnerability points of the RSA algorithm? | 4*5=20 |
| 3 | a) | Describe a scheme to produce Digital Signature with the help of diagram. | 5 |
| | b) | What is the Diffie-Hellman Key Exchange Algorithm? Suppose Alice and Bob agreed on p as 7 and g as 5. Find the value of secret keys? | 5+3=8 |
| | c) | Explain the security threat of the Diffie-Hellman Key Exchange Algorithm with the help of an example. | 7 |
| 4 | a) | Using Playfair cipher encrypt and decrypt the message "Attack tonight" using the key "Monarchy". | 3+3=6 |
| | b) | Show the encryption and decryption process of Rail Fence encryption scheme for the Plaintext= "ATTACK ON TITAN TONIGHT" with number | 3+3=6 |

of rails = 4.

c) What do you mean by Confusion and Diffusion? Discuss its differences. 8

4. a) **Solve the modular arithmetic:** 1*8=8

i. **257 mod 5**

ii. **-158 mod 14**

iii. **-71 mod 10**

iv. **1/9 mod 26**

v. **-114 mod 3**

vi. **212 mod 4**

vii. **-8 mod 11**

viii. **2152 mod 4**



b) Do each of the following inverses exist ? If yes, what are they ? If no, explain why not ? 3+3=6

i. $132^{-1}$ **(mod 341)**

ii. $78^{-1}$ **(mod 415)**

c) Find the **gcd (161, 28)** also find the value of s and t using Extended Euclidean Algorithm. 2+2+2= 6

5. a) Using Chinese remainder theorem solve the value of X: 10

**$X \equiv 2 \pmod 4$, $X \equiv 1 \pmod 5$, $X \equiv 3 \pmod 9$, $X \equiv 7 \pmod{13}$**



b) Find the primitive roots of 11. 10

6. **Write short note on** 4*5=20

a) Substitution and Transposition cipher

b) Active attacks and Passive attacks

c) Stream & block ciphers

d) Authentication and Authorization

**********