| Reg. No. | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|

| Question Paper Code | 12234 |
|---|---|

**B.E. / B.Tech - DEGREE EXAMINATIONS, NOV / DEC 2023**

Seventh Semester

**Information Technology**

(Common to Computer Science and Engineering)

**20ITPC701 - CRYPTOGRAPHY AND NETWORK SECURITY**

(Regulations 2020)

Duration: 3 Hours Max. Marks: 100

**PART - A (10 × 2 = 20 Marks)**

Answer ALL Questions

| | | *Marks, K-Level, CO* |
|---|---|---|
| 1. | What is meant by passive and active attack? | *2,K1,CO1* |
| 2. | Convert the given text "Anna University" into cipher text using rail fence technique. | *2,K1,CO1* |
| 3. | Solve $11^7$ mod 13. | *2,K2,CO2* |
| 4. | What is an abelian group? Give an example. | *2,K2,CO2* |
| 5. | Define Euler's theorem. | *2,K1,CO3* |
| 6. | Define Chinese remainder Theorem. | *2,K1,CO3* |
| 7. | Perform encryption and decryption using RSA Alg. for the following. P=7; q=11; e=17; M=8. | *2,K1,CO4* |
| 8. | Explain about asymmetric key cipher. | *2,K2,CO4* |
| 9. | State any three requirements for authentication. | *2,K2,CO5* |
| 10. | Define the term message digest. | *2,K1,CO5* |

**PART - B (5 × 13 = 65 Marks)**

Answer ALL Questions

| | | | |
|---|---|---|---|
| 11. | a) | Using playfair cipher algorithm encrypts the message "ENGINEERING" using the key "MONARCHY "and explain. | *13,K2,CO1* |
| | | **OR** | |
| | b) | Explain the substitution encryption techniques in detail. | *13,K2,CO1* |
| 12. | a) | Briefly explain Euclid's Algorithm along with example. | *13,K2,CO2* |
| | | **OR** | |
| | b) | Explain in detail about Groups, Rings and Fields. | *13,K2,CO2* |
| 13. | a) | (i) Explain in detail about Euler's Totient Theorem. | *7,K2,CO3* |
| | | (ii) State and Prove Fermat's theorem. | *6,K2,CO3* |

**OR**

b) Explain Chinese Remainder theorem and find X for the given set of congruent equation CRT. *13,K3,CO3*

$X \equiv 2 \pmod 3$
$X \equiv 3 \pmod 5$
$X \equiv 2 \pmod 7$

14. a) With a neat sketch explain the Elliptic curve cryptography with an example. *13,K2,CO4*

**OR**

b) Explain Diffie-Hellman algorithm and find the secret key shared between user A and user B Diffie-Hellman algorithm for the following q=353; α (primitive root)=3, XA=45 and XB=50. *13,K2,CO4*

15. a) Explain in detail about X.509 authentication services. *13,K2,CO5*

**OR**

b) Describe digital signature algorithm and show how signing and Verification is done DSS. *13,K2,CO5*

**PART - C (1 × 15 = 15 Marks)**

16. a) Describe in detail about SSL/TLS. *15,K2,CO6*

**OR**

b) Explain the operational description of PGP. *15,K2,CO6*