Exam Seat No:_____ Enrollment No:_____

# C.U.SHAH UNIVERSITY

**Wadhwan City**

**Subject Code : 5TE02ANS1** **Summer Examination-2014** **Date: 30/06/2014**

**Subject Name: Advance Cryptography & Network Security**

**Branch/Semester:- M.Tech(CE) /II** **Time:2:00 To 5:00**

**Examination: Regular**

**Instructions:-**

**(1)** Attempt all Questions of both sections in same answer book / Supplementary

**(2)** Use of Programmable calculator & any other electronic instrument is prohibited.

**(3)** Instructions written on main answer Book are strictly to be obeyed.

**(4)**Draw neat diagrams & figures (If necessary) at right places

**(5)** Assume suitable & Perfect data if needed

---

## SECTION-I

**Q-1 Attempt following Questions.**

| | | | |
|---|---|---|---|
| | a) | Differentiate Substitution and Transposition Techniques. | 2 |
| | b) | Define Authentication. Explain different types of Authentication. | 2 |
| | c) | If sender Sends plaintext as "information", Find Ciphertext Using Rail fence. | 2 |
| | d) | Define one-way property. | 1 |
| Q-2 | a) | Describe Data Encryption standard. | 5 |
| | b) | Explain Key Distribution Scenario with suitable diagram. | 5 |
| | c) | Write Short Note on Blum Blum Shub Generator. | 4 |
| | | **OR** | |
| Q-2 | a) | Using RSA Algorithm, two prime numbers p=7, q=29 and M=6 find e, d and Ciphertext. | 5 |
| | b) | Explain Security Attack with examples. | 5 |
| | c) | Write Short note on Digital Signature Algorithm. | 4 |
| Q-3 | a) | Explain Block Cipher Modes of operation. | 7 |
| | b) | Using Hill Cipher Plaintext as "Paymoremoney" and key as First row as17 17 5 Second row as 21 18 21 third row as 2 2 19 Find out Ciphertext. | 7 |
| | | **OR** | |
| Q-3 | a) | Explain Advanced Encryption Standard. | 7 |
| | b) | Using Hill Cipher Ciphertext as "pqcfku" Find Plaintext. | 7 |

## SECTION-II

**Q-4 Attempt following Questions.**

| | | | |
|---|---|---|---|
| | a) | Differentiate SET and SSL. | 2 |
| | b) | Write Full form of virus. Explain use of Virus. | 2 |
| | c) | What is the function of TGS? | 2 |
| | d) | Which techniques are Unbreakable and Why? | 1 |
| Q-5 | a) | Explain Diffie – Hellman Key Exchange with Example. | 5 |
| | b) | List and briefly explain authentication functions. | 5 |
| | c) | Write Short Note on Web Security Consideration. | 4 |
| | | **OR** | |

| | | | |
|---|---|---|---|
| Q-5 | a) | Explain Function of PGP. | 5 |
| | b) | Explain the requirements of authentication function. | 5 |
| | c) | Explain Worms and Trojan Horse. | 4 |
| Q-6 | a) | Explain Secure Hash Algorithm. | 7 |
| | b) | Explain SSL Architecture. | 7 |

**OR**

| | | | |
|---|---|---|---|
| Q-6 | a) | Explain HMAC. | 7 |
| | b) | Explain Firewall Design Principle. | 7 |

*******30***14****S**