B.E.(FULL-TIME) DEGREE END SEMESTER EXAMINATIONS, MAY 2014

ELECTRONICS AND COMMUNICATION ENGINEERING BRANCH

VIII SEMESTER

EC9028 - CRYPTOGRAPHY AND NETWORK SECURITY

(REGULATION 2008)

Time: 3 Hours Max.marks: 100

Answer ALL Questions

PART-A (10x2=20 Marks)

1. What is the difference between a monoalphabetic cipher and a polyalphabetic cipher?
2. Construct a Playfair matrix with the key "LARGEST" and encrypt the message "MUST".
3. What is meant by diffusion and confusion?
4. What is a trapdoor one-way function?
5. State Fermat's and Euler's theorem.
6. Compute 2^{43210} mod 101.
7. What is the difference between a message authentication code and a one-way hash function?
8. What is digital signature?
9. List out the protocols comprise in SSL.
10. Distinguish between transport mode and tunnel mode of IP security

PART-B (5x16=80 Marks)

11. (i) Explain the various categories of security services and security mechanisms. **(8)**

    (ii) Using Hill cipher, encrypt the plaintext "MAY" and show the calculations for the corresponding decryption of the ciphertext to recover the original plaintext. Assume the encryption key K is given by

$$\mathbf{K} = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$$ **(8)**

12.a.(i) With neat diagram, explain the Block Cipher Modes of Operation. **(10)**

(ii) Illustrate and Explain the RC4 algorithm. **(6)**

(OR)

12. b. (i) How are the S-box and Inverse S-box constructed in AES? Using this procedure, Compute the substitute byte value for byte "80". **(10)**

(ii) With neat diagram, explain the AES key expansion algorithm. **(6)**

13. a. (i) Define and explain Chinese Remainder Theorem(CRT). Solve $x \equiv 7 (\mathrm{mod} 12345)$ and $x \equiv 3 (\mathrm{mod} 11111)$ using CRT. **(8)**

(ii) Perform encryption and decryption using the RSA algorithm for the following: p = 5; q = 11, e = 3; M = 9. **(8)**

(OR)

13. b. (i) Calculate the multiplicative inverse of $(x^7 + x + 1)$ mod $(x^8 + x^4 + x^3 + x + 1)$ **(8)**

(ii) The Miller-Rabin test can determine if a number is not prime but cannot determine if a number is prime. How can such an algorithm be used to test for primality? Explain. **(8)**

14. a. With neat block diagram, explain the basic arithmetical and logical functions of SHA 512.

(OR)

14. b. (i) With neat diagram, explain the RSA approach and DSS approach for generating digital signatures. Also explain the functions of Digital Signature Standard signing and verifying. **(10)**

(ii) Users A and B use the Diffie-Hellman key exchange technique with a common prime q = 71 and a primitive root α = 7.

I. If user A has private key $X_A = 5$, what is A's public key Y_A?

II. If user B has private key $X_B = 12$, what is B's public key Y_B?

III. What is the shared secret key? **(6)**

15. a. What is a dual signature and what is its purpose? With neat block diagram, explain the Secure Electronic Transaction (SET).

(OR)

15.b. Explain the process of the Authentication Header and Encapsulating Security Payload Protocols of IP Security. List out its benefits.