Roll. No									

B.E / B.Tech (Full Time) DEGREE END SEMESTER EXAMINATIONS, NOV / DEC 2012

COMPUTER SCIENCE AND ENGINEERING

SEVENTH SEMESTER

35

CS 9402 – CRYPTOGRAPHY AND SECURITY

(REGULATIONS 2008)

Time: 3 hr Max.Mark:100

Answer All Questions

Part – A (10 X 2 = 20 Marks)

1. What are the square roots of 1 mod n if n is 22 (a composite)?
2. Does the number 561 pass the Fermat test? Specify.
3. Why does the DES function need an expansion permutation?
4. Find the results of the 27^{-1} mod 41 and 70^{-1} mod 101, using Fermat's little theorem?
5. What is the padding for SHA-512 if the length of the message is 5120 bits?
6. Show that 2 is a primitive root of 11 in Diffie-Hellman scheme with a common prime q=11 &primitive root α=2.
7. What services are provided by IPSec?
8. What is the difference between SSL connection and an SSL session?
9. List out the drawbacks of partitioning as a means of implementing multilevel security for databases.
10. Define the term tracker attacks?

Part – B (5 X16=80)

11. i) Perform the encryption and decryption using RSA algorithm by generating the public and private keys for the given values P=17 & Q=11. (Choose 'e' by condition of RSA). (8)

    ii) Given the plain text {000102030405060708090A0B0C0D0E0F} and the key {01010101010101010101010101010101} in AES, perform the following. (8)

    a. Show the original contents of the **State**, displayed as a 4 X 4 matrix

    b. Show the value of **State** after initial AddRoundKey, after SubBytes, after ShiftRows, after MisColumns.

12. A) i. Encrypt the message " meet me at the usual place" using the Hill cipher with the key (8)

$$\begin{pmatrix} 9 & 4 \\ 5 & 7 \end{pmatrix}$$ show your calculations and the result.

    ii. State and prove the Chinese remainder theorem and also solve $x^2 = 1 \pmod{35}$. (8)

(OR)

12. B) i. Use PlayFair cipher to encipher the message "the key is hidden under the door pad". The secret key is "GUIDANCE". (8)

ii. State and prove Fermat's and Euler's theorem (8)

13. A) i. Write the Diffie Hellman algorithm key exchange algorithm and find the A's and B's Shared Key, if user A has private key X_A =5 and user B has private key X_B =12 for the given prime number P=71 and Primitive root α = 7. (Also find A's and B's Public key). (12)

ii. In what ways can a hash value be secured so as to provide message authentication? (4)

(OR)

B) i. Explain the SHA-1 compression function with its logic of single step. (8)

ii. Discuss in detail about the DSS algorithm (8)

14. A) i. Describe the process of how key rings are used in message transmission and reception in PGP with its diagram of message generation (8)

ii. Discuss any two approaches to secure user authentication in a distributed environment. (8)

(OR)

B) i. Explain the Anti-Replay Service mechanism in IP security with neat diagram (8)

ii. Describe the SET participants and sequence of events that are required for a transaction in Secure Electronic Transaction (8)

15. A) i. Write the set of rules combining the secrecy controls of the Bell-La-padula Model with the integrity controls of the biba model in trusted operating system. (8)

ii. Discuss the trade-off between granularity and efficiency (8)

(OR)

B) i. Explain the advantages and disadvantages of partitioning as a means of implementing multilevel security for databases. (8)

ii. Discuss the purpose of encryption in a multilevel secure database management system? (8)