19/11/13.

27

Roll No	

B.E/ B.TECH (FULLTIME) DEGREE END SEMESTER EXAMINATIONS, OCT/NOV 2013
DEPARTMENT OF INFORMATION TECHNOLOGY
IT9402 - CRYPTOGRAPHY AND SECURITY
(REGULATION 2008)

Time: 3 hours Max. Mark: 100
Answer ALL Questions

Part A (10X2=20)

1. Use playfair cipher to encrypt "Confidence is the key road to success" with the keyword "desire".
2. Use extended Euclid algorithm to find the GCD (482,1180).
3. What are the properties of GF(p)? Find the multiplicative inverse of GF(7).
4. Solve the exponentiation 6^{24} mod 35 using Euler's theorem.
5. In the elliptic curve group defined by $y^2 = x^3 + x + 7$ over F_{17}, what is P + Q if P = (2,0) and Q = (1,3)?
6. Let p=47 and g=5 be the values in Diffie Hellman key exchange. Generate the session key shared between the two parties A & B.
7. What are Kerberos realms?
8. What do you meant by Change cipher Spec protocol?
9. What are the four primitive operations in a take-grant system?
10. Differentiate mandatory and discretionary access control.

Part B (16X5=80)

11. i. Find an integer that has a remainder of 3 when divided by 7 and 13, but divisible by 12 using Chinese Remainder Theorem. (4)

    ii. Use affine cipher to encrypt " Cryptography" with the key (7,16). Perform decryption for the same. (4)

    iii. If $x^2 \equiv a \bmod p$ represents quadratic congruence, state the Euler's criterion. Show that 3 is a QR mod 13 and 5 is a QNR mod 13 and find all the QR and QNR for Z^*_{11}. And also solve $x^2 \equiv 36 \bmod 77$. (8)

12.a. i Explain the AES transformation functions in detail. (10)

    ii. Write the RSA algorithm. Bob and Alice need to communicate. Bob chooses 7 and 11 as p and q values and computes the necessary parameters for key setup. Bob encrypts the message 5 using RSA and sends it to Alice. Alice decrypts the message. Show all the computations involved. (6)

(OR)

b. i. Given 10 bit key k =1010000010, determine K1, K2 using SDES Key generation method where (4)

P10= 3 5 2 7 4 10 1 9 8 6
P8 = 6 3 7 4 8 5 10 9

ii Explain meet- in - middle attack in Triple DES. (4)
iii. Write and explain the RC4 algorithm. (8)

13 a i. Explain SHA-512 single round function with suitable diagram. (8)

ii. Consider a prime field GF(19). It has primitive root value of 10. Alan chooses a random integer value 5 and generates its key pair. John sends message with value 17 and chooses the key value k as 6 to generate the ciphertext. Use ElGamal Cryptosystem to show the computations involved in the communication . (6)

iii Find all the primitive roots of 27. (2)

(OR)

b. i. Explain DSA approach for generating digital signatures (8)

ii. Differentiate RSA and DSS approach for generating Digital Signatures (4)

iii. Consider the elliptic curve over GF(23) with a=1 and b=0.
a. Find the equation and all the points on the curve. Graph the points.
b. Check whether the point (9,5) lie on the elliptic curve over GF(23). (4)

14. a.i Explain how mutual authentication is achieved in Kerberos? (10)
ii. With a neat diagram, explain Public key Infrastructure. (6)

(OR)

b. i. Explain SSL architecture and its protocols in detail. (10)
ii What is a Security Association in IPSec. List its parameters. (6)

15. a. i Explain Bell-La Padula Confidentiality model. (8)
ii. Explain the security features of Trusted OS. (8)

(OR)

b. i. Illustrate the inference problem. Explain direct, indirect and tracker attacks with an example. (8)
ii. Explain trusted front end with suitable diagram. (8)