Roll Number: [ ]

ANNA UNIVERSITY – UNIVERSITY DEPARTMENT
B.E. (FULL-TIME) DEGREE EXAMINATION, NOV/DEC 2013

Seventh Semester – R2008
Branch: Computer Science & Engineering

23

CS9402 – CRYPTOGRAPHY & SECURITY
(End-Semester Examination)

Time: Three Hours Max. Marks: 100

Answer **ALL** Questions

Part A ($10 \times 2 = 20$ Marks)

1. In MD5, a message is padded even if its length is already a multiple of the block length. Why is this important?
2. What are the three major components of Feistel structure?
3. What is the Euler-Totient value of 91?
4. Find the GCD of $x^3 + x + 1$ and $x^2 + x + 1$ over $GF(2)$.
5. Suppose Alice wants Bob to sign a message M, under a public key cryptosystem. What does Bob do now?
6. How does PGP achieve e-mail compatibility?
7. What does IP-Security protect in transport mode?
8. What are the threats to a database?
9. What makes an Operating System "Secure"?
10. What is the strength of AES over DES?

Part B ($5 \times 16 = 80$ Marks)

11. (a) A girl was carrying a basket of eggs, and a man driving a horse hit the basket and broke all the eggs. Wishing to pay for the damage, he asked the girl how many eggs there were. The girl said she did not know, but she remembered that when she counted them by twos, there was one left over; when she counted them by threes, there were two left over; when she counted them by fours, there were three left over; when she counted them

119

by fives, there were four left; and when she counted them by sixes, there were five left over. Finally, when she counted them by sevens, there were none left over. 'Well,' said the man, 'I can tell you how many you had.' What was his answer? (8)

(b) Find the multiplicative inverse of $x^5 + x^4 + x$ modulo the irreducible polynomial $x^8 + x^4 + x^3 + x + 1$. (8)

12. (a) i. What are the different types of attacks possible on a block cipher? Explain with simple examples. (8)

ii. What do you mean by diffusion and confusion? Explain how is it achieved in a product cipher having two rounds. (5)

iii. What is the significance of having 56-bit key for the DES? (3)

(OR)

(b) i. Explain the design aspect of one round of AES. (10)

ii. Given that the key for round 9 of AES (in HEX) as

$$9A930B77\ \ 3FE57682\ \ C42A337B\ \ 5EAB1059$$

What are the first four bytes of the round key for round 10? Use the following SubByte value. (6)

Input	$5E$	AB	10	59
Output	58	62	CA	CB

13. (a) i. Explain Pohlig-Hellman algorithm for finding discrete logarithm. (8)

ii. Use the Pohlig-Hellman algorithm to find the discrete logarithm of 153 to the base 2 in $Z181$, i.e., solve for $x : 2^x = 153 \ mod\ (181)$. (8)

(OR)

(b) i. Explain MD5 algoritms for generating message digest. (8)

ii. Explain Digital Signature Algorithm, and prove its correctness. (8)

14. (a) How do we achieve email security with S/MIME. (16)

(OR)

(b) How do we achieve IP security with tunnel mode operation. (16)

15. (a) What is Trusted Operating System. Explain the design principle for Trusted Operating System. (16)

(OR)

(b) How do we protect a database from various possible attacks. Explain.(16)

*****