2017

(Old Syllabus)

COMPUTER SCIENCE AND ENGINEERING

Paper – CSEB – 506

(Cryptography)

Full Marks – 70

The figures in the margin indicate full marks

Candidates are required to give their answers in their own words as far as practicable

Answer ***Question No. 1 , 2*** and ***any four*** from the rest

1. Answer ***any five*** questions : 2×5

(a) Find all multiplicative pairs in Z_{11}.

(b) Distinguish between Z_n and Z_n^*.

(c) For the following equation, find an integer that satisfies the equation. $7x \equiv 4(\text{mod}5)$

(d) Define Galois Field.

(e) Find the value of $\phi(32)$, Where ϕ denotes Euler's totient function.

(f) Verify that the number 17 is a prime through square root test.

(g) Find the order of all elements in $G = \langle Z_{10}^*, X \rangle$.

(h) What do you mean by "Avalanche effect" ?

2. Answer ***any five*** questions : 4×5

(a) Write an algorithm for testing primality of a number using Miller-Rabin test.

(b) State extended Euclidean algorithm and use it to find the GCD of (84,320).

(c) What is Key wrapping ? How is it useful ?

(d) State the second criterion for a cryptographic hash function and associate the concerned birthday problem.

(e) Find the results of 21^{24} mod 8 using Fast exponentiation method.

(f) Discuss the advantage(s) of using counter algorithmic mode compared to CBC.

(g) Discuss the Lamport's Hash algorithm for authentication and state the uniqueness of the said algorithm.

(h) Why do you think the mixing transformation (Mix Columns) is not needed in DES; but is needed in AES?

3. (a) Use the extended Euclidean algorithm to find the inverse of $(x^4 + x^3 + 1)$ in GF (2^5) using the modulus $(x^5 + x^2 + 1)$.

(b) Prove that the difficulty of an alternative collision attack is proportional to $2^{n/2}$. 5+5

4. State the properties of a standard public-key cryptography algorithm. Describe RSA and show that these properties hold in context of RSA. 3+7

5. Comment on the Key management issue for secret key cryptography. Describe the role of Key Distribution Centre for Key management. Is it helps for authentication ? Justify your answer. 2+4+4

6. Discuss the principle behind proposing a product cipher by Shannon. Show how these principles are implemented in DES. 3+7

7. (a) Discuss "Chosen cipher text attack" with an example.

(b) Write an algorithm for decryption in Knapsack cryptosystem.

(c) What do you mean by "Digital signature"? 4+4+2

8. (a) Write a short note on "Analysis of Diffie-Hellman" key exchange algorithm.

(b) Describe the sub-key generation algorithm in AES. 5+5