D

APJ ABDUL KALAM TECHNOLOGICAL UNIVERSITY

SECOND SEMESTER M.TECH DEGREE EXAMINATION, MAY 2016

Computer Science & Engineering

(Computer Science & Systems Engineering)

04CS6418—Foundations of Crypto Systems

Max. Marks : 60 Duration: 3 Hours

PART A

Answer All Questions

Each question carries 3 marks

1. Define the three security goals?
2. Find decryption key, if encryption key in a transposition cipher is [3 1 4 5 2].
3. What is the difference between a weak key, semi-weak key and possible weak key?
4. Distinguish between second preimage resistance and collision resistance.
5. List the categories of potential attacks on RSA.
6. Define trapdoor one-way function. Give an example.
7. What do you mean by man-in-the-middle attack?
8. How will you decrypt a message using elliptic curve cryptosystem?

PART B

Each question carries 6 marks

9. Explain various security services and mechanisms provided by ITU-T.

OR

10. Categorize the attacks into passive attacks and active attacks. Explain.
11. Encipher the message “life is full of surprises” using Vigenere cipher with keyword “HEALTH”. Decipher the message to get the plaintext.

OR

12. Explain differential and linear cryptanalysis in detail. Which one is a known-plaintext attack? What type of cryptanalytic attack is the other one?
13. Explain DES function in detail.

OR

14. Illustrate SubBytes transformation in AES.
15. Describe the digital signature process and services.

OR

16. Write brief notes on SHA-1.
17. Given the superincreasing tuple b = [7,11,19,39,79,157,313], r = 37, and modulus n = 900, encrypt and decrypt the letter “g” using the knapsack cryptosystem. Use [4 2 5 3 1 7 6] as the permutation table.

OR

18. Briefly explain the idea behind RSA cryptosystem.
19. Write notes on ElGamal digital signature scheme.

OR

20. Describe in detail the Diffie-Hellman key exchange protocol.