Dr. P.K. Gupta

JAYPEE UNIVERSITY OF INFORMATION TECHNOLOGY, WAKNAGHAT

TEST -3 EXAMINATION- 2021

B.Tech 8th Semester

COURSE CODE: 18B1WCI734 MAX. MARKS: 35

COURSE NAME: CRYPTOGRAPHY AND NETWORK SECURITY

COURSE CREDITS: 02 MAX. TIME: 2 Hours

Note: *All questions are compulsory. Carrying of mobile phone during examinations will be treated as case of unfair means.*

Section A (Do any FIVE) **[1x5 = 5]**

1) What is the OSI security architecture?
2) Differentiate between active and passive security threats.
3) Explain modes of operation for block ciphers.
4) Explain 2DES and 3DES encryption and decryption.
5) Explain general schemes for distribution of public keys.
6) What is the need for digital signatures? Explain important properties of digital signatures.

Section B (Do any FIVE) **[3x5 = 15]**

1) Explain a monoalphabatic cipher system and carryout cryptanalysis of the same.
2) With the help of a diagram explain the Feistel encryption & decryption technique.
3) What do you understand from polynomial arithmetic's? How will you adopt Euclidean algorithm to find the GCD of two polynomials?
4) Explain the following.
   i. Rings.
   ii. Groups.
   iii. Finite fields.
5) With the help of a diagram explain key expansion algorithm for AES.
6) Explain RSA algorithm for public key cryptography?

Section C

1. Solve the following simultaneous congruence's using the Chinese Remainder Theorem **[5]**
   $x \equiv 6 \pmod{11}$, $x \equiv 13 \pmod{16}$, $x \equiv 9 \pmod{21}$, $x \equiv 19 \pmod{25}$
2. Show that set of all positive integers constitute an abelian group. **[5]**
3. What is Fermat's little theorem? Solve $x^{86} \equiv 6 \pmod{29}$ using Fermat's little Theorem. **[5]**