Ex/PG/SWE/T/129B/2018

M.E. SOFTWARE ENGINEERING
FIRST YEAR
SECOND SEMESTER EXAM 2018

INFORMATION & NETWORK SECURITY

Time: Three hours

Full Marks-100

Attempt any five (5) questions.

1.

[6+4+4+6]

a. Describe the Vigenere cipher.

b. Consider the plaintext “jadavpur university”, find the corresponding ciphertext using Vigenere cipher with key as “jusl” (ignore blank).

c. Consider the ciphertext “**VHV**SSP**QUC**EMRVBVBBB**VHV**SURQGIBDUGRNICJ**QUC**ERVUAXSSR”., which is output of Vigenere cipher. Give an estimation on the length of the key with the help of the bold (matched) substring.

d. Describe the different cryptanalysis attacks with suitable diagrams.

2.

[6+6+(5+3)]

a. Use Extended Euclidean algorithm to find 7^{-1} mod 160.

b. Use square and multiplication method to find 115^{23} mod 187.

c. Describe the RSA cryptosystem and illustrate RSA system for p=17, q=11, e=7 and message is m=4.

3.

[14+6]

a. Describe the working principle of the IPSec with suitable diagrams.

b. How IPSec protects the system from replay attack.

4.

[(2+8)+(2+8)]

a. What are the services provided by PGP services? How does PGP provide confidentiality for e-mail and file storage applications? Draw the block diagram and explain its components.

b. List the services of SSL. Describe the SSL Specific protocol – Handshake action in detail.

5.

[8+(3+3+2+4)]

a. What is cipher stealing? Describe this in Electronic Codebook (ECB) Mode with proper diagram.

b. Address of the following issues of DES (with diagram if possible)
   i. weak keys
   ii. semi-weak keys
   iii. key complement
   iv. ‘double DES with two keys k_1 and k_2 is useless as a single DES with k_3 does same thing’

[P.T.O.]

6. [3+(2+1+4)+5+5]

a. Prove that number of primes is infinite.

b. Define the terms quadratic residue. Given two numbers 'a' and a prime number 'p', how we know that 'a' is quadratic residue respect to 'p'? Find the all quadratic residue from the set Z_{13}*.

c. Prove that if there are just 23 students in a classroom, it is likely (with probability ≥ ½) that two students have same birthday (ignoring year of birth).

d. What is the minimum and maximum number of padding bits that can be added to a message in SHA-512?

7. [10+10]

a. Explain with diagram, how Diffie Hellman key exchange works?

b. Describe the 'RSA Signature on the Message Digest' with proper diagram.