Sr. No.....

Dec 2018

B.Tech(IT), 5th SEMSTER

Network Security, (IT-311)

Time: 3 Hours **Max. Marks:60**

Instructions:
1. *It is compulsory to answer all the questions (2 marks each) of Part -A in short.*
2. *Answer any four questions from Part -B in detail.*
3. *Different sub-parts of a question are to be attempted adjacent to each other.*

PART -A 10*2= 20

Q1 (a) A small private club has only 100 members. How many secret keys are needed if the president decides that the two members who need to communicate should contact him first. The president then creates a temporary key to be used between the two. The temporary key is encrypted and sent to both members?

(b) Differentiate between Cryptography and cryptology?

(c) Define Kerckhoff's principle?

(d) Differentiate between inbound and outbound security associations?

(e) List various security issues regarding Databases?

(f) John is reading a mystery book involving cryptography. In one part of the book, the author gives a ciphertext "CIW" and two paragraphs later the author tells the reader that this is a shift cipher and the plaintext is "yes". In the next chapter, the hero found a tablet in a cave with "XVIWYWI" engraved on it. John immediately found the actual meaning of the ciphertext. What is the plaintext?

(g) What are honeypots?

(h) Brief the significance of covert channels?

(i) Distinguish between message integrity and message authentication?

(j) Explain the concept of password aging?

PART -B

Q2 (a) Given the key "student" apply play fair cipher to plain text "FACTIONALISM" to ensure confidentially at the destination? (5)

(b) Evaluate 5^{-1} mod 13 using Fermat's Theorem? (5)

Q3 (a) Differentiate between confuslon and diffusion? (5)

(b) Discuss Man in the Middle Attack with the help of an example? (5)

Q4 How key expansion process works in AES? Explain with the help of an example? (10)

Q5 (a) Explain a session key is generated and communicated by KDC in order to have communicate between two parties? (5)

(b) Explain in detail the process by which MD5 provides integrity to the system? (5)

Q6 (a) Describe various fields of Authentication Header (AH) of IP SEC protocol? (5)

(b) List out various security issues of Transport layer? (5)

Q7 Write short note on: (10)

i) X.509 certificate

ii) PGP protocol

****