29/12/23
170

29/12

Sr. No 004703

CE/ Dec 2023 003703

B.Tech(CSE) B.Tech VII SEMESTER

Cryptography and Network Security (PEC-CS-A-703)

Time: 3 Hours **Max. Marks:75**

Instructions:
1. *It is compulsory to answer all the questions (1.5 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

Q1 (a) What is Security? Explain various security goals. (1.5)

(b) How can you differentiate between the terms "Attack" and "Threat" in the context of information security? (1.5)

(c) Encrypt the following message using Playfair substitution cipher with key =HARSH. Plain Text ='Clouds are High' (1.5)

(d) Discuss the structure of x.509 Digital certificate. (1.5)

(e) What encryption algorithms does Kerberos support? (1.5)

(f) Differentiate between Internal and External Attacks in MANET. (1.5)

(g) What is the Web of Trust in the context of PGP? (1.5)

(h) How does the dynamic topology of MANETs impact the design of security mechanisms? (1.5)

(i) Discuss Selective forwarding Attack in Wireless Sensor Network. (1.5)

(j) Explain security challenges in Mobile Ad-hoc Network. (1.5)

PART -B

Q2 (a) Discuss AES Algorithm in detail with neat diagrams. Is AES considered secure against modern cryptographic attacks? (10)

(b) Suppose the Plain text message is: "Life is Beautiful" (5)

$$\text{Key} = \begin{matrix} 2 & 4 & 5 \\ 9 & 2 & 1 \\ 3 & 17 & 7 \end{matrix}$$

Generate cipher text using Hill Cipher Technique.

Q3 (a) Illustrate Diffie-Hellman Key Exchange Algorithm. (5)

(b) Explain the role of public key and private key in Digital Signature. Can a Digital signature be forged or duplicated? (10)

Q4 Explain IP Security. What is a Security Association (SA) in IPSec? What are the two main modes of operation in IPSec? (15)

Q5 (a) How does Kerberos work? What are the three main components of Kerberos? (5)

(b) What are three situations in which ensuring the security of email is crucial or highly desirable? How does PGP ensure the confidentiality of email messages and how PGP handles key management and distribution? (10)

003703/170/111/703

Q6 (a) Provide an overview of the security issues and potential attacks that can target the fundamental mechanisms of wireless sensor networks. (10)

(b) Differentiate between Spoofed, Altered and Replayed Routing Attack in WSN. (5)

Q7 Explain the following attacks in MANETs (15)

i)Byzantine Attack
ii)Data Flooding Attack
iii)Black Hole Attack
iv)Sleep Deprivation Attack

****