CS8792 – CRYPTOGRAPHY AND NETWORK SECURITY

UNIT I INTRODUCTION

Security trends - Legal, Ethical and Professional Aspects of Security, Need for Security at Multiple levels, Security Policies - Model of network security – Security attacks, services and mechanisms – OSI security architecture – Classical encryption techniques: substitution techniques, transposition techniques, steganography- Foundations of modern cryptography: perfect security – information theory – product cryptosystem – cryptanalysis.

C402.1 Understand the fundamentals of networks security, security architecture, threats and vulnerabilities

PART A

Q. No	QUESTIONS	BT LEVEL	COMPETENCE	CO	PO
1.	What is Cryptography and Cryptanalysis?	BTL-1	Remember	**C402.1**	PO1
2.	Define cryptology	BTL-1	Remember	**C402.1**	PO1
3.	Define security mechanism.	BTL-1	Remember	**C402.1**	PO1
4.	What is the difference between threat and attack?	BTL-4	Analyse	**C402.1**	PO2
5.	Differentiate passive attack and active attack.	BTL-4	Analyse	**C402.1**	PO2
6.	Point out the types of cryptanalytic attacks.	BTL-1	Remember	**C402.1**	PO2
7.	Differentiate an unconditionally secure cipher and a computationally secure cipher?	BTL-4	Analyse	**C402.1**	PO2
8.	What is a product cipher?	BTL-1	Remember	**C402.1**	PO1
9.	What are the essential components of a cipher model?	BTL-1	Remember	**C402.1**	PO1
10.	What are the two basic functions used in encryption algorithms?	BTL-1	Remember	**C402.1**	PO1
11.	Encrypt the plaintext “DOCUMENT” using Caesar cipher with key=3.	BTL-3	Apply	**C402.1**	PO3
12.	Using the Rail Fence technique, find out the ciphertext for the following plaintext. “College of Engineering, Anna University”	BTL-3	Apply	**C402.1**	PO3
13.	Use the Vigenere cipher with keyword “TEN” to encipher the message “LIFE”.	BTL-3	Apply	**C402.1**	PO3
14.	Decipher the following ciphertext using brute force attack: CMTMROOEOORW (Hint: Algorithm – Rail fence)	BTL-5	Evaluate	**C402.1**	PO3
15.	What are the basic techniques used in classical cipher?	BTL-1	Remember	**C402.1**	PO1
16.	Mention some of the monoalphabetic and poly alphabetic ciphers	BTL-1	Remember	**C402.1**	PO1
17.	What is steganography?	BTL-1	Remember	**C402.1**	PO1
18.	What is one time pad?	BTL-1	Remember	**C402.1**	PO1
19.	What are rotor machines? State its use.	BTL-1	Remember	**C402.1**	PO1

20.	What is the need for multiple levels of security policies?	BTL-2	Understand	**C402.1**	PO1

PART B & C

Q. No	QUESTIONS	BT LEVEL	COMPETENCE	CO	PO
1.	Discuss in detail the OSI Security Architecture highlighting the attacks, mechanisms and services.	BTL-2	Understand	**C402.1**	PO1
2.	Discuss the security trends and the terminologies involved in Security.	BTL-2	Understand	**C402.1**	PO1
3.	Discuss the model for network security along with secure access model with suitable diagrams	BTL-2	Understand	**C402.1**	PO1
4.	Explain in detail about the Symmetric cipher model with necessary diagrams.	BTL-2	Understand	**C402.1**	PO1
5.	Explain the transposition techniques and substitution techniques in detail with suitable examples	BTL-2	Understand	**C402.1**	PO1
6.	Encrypt and decrypt the following messages using Play fair cipher. Use MONARCHY as keyword. Use X as the filler character for spaces if necessary. • BALLOON • CRYPTOGRAPHY • SECURITY • SWARAJ IS MY BIRTH RIGHT • MEET ME TOMORROW	BTL-3	Apply	**C402.1**	PO3
7.	Using Hill Cipher, encipher and decipher the following message. Ignore the spaces. "CRYPTOGRAPHY AND NETWORK SECURITY" using the following key: K= $\begin{matrix}03 & 02\\05 & 07\end{matrix}$. K= 3 10 20 20 9 17 9 4 17	BTL-5	Evaluate	**C402.1**	PO3
8.	Elaborate on the Legal, Ethical and Professional aspects of Security	BTL-2	Understand	**C402.1**	PO1
9.	Discuss on the foundations of modern cryptography and Information Theory highlighting the aspects of Perfect secrecy.	BTL-2	Understand	**C402.1**	PO1
10.	Using Hill Cipher, encipher and decipher the following message. Ignore the spaces. "PAY MONEY" using the key: K= 17 17 5 21 18 21 2 2 19	BTL-5	Evaluate	**C402.1**	PO3