GEETHANJALI INSTITUTE OF SCIENCE & TECHNOLOGY
(AN AUTONOMOUS INSTITUTION)
(Approved by AICTE, New Delhi & Affiliated to JNTUA, Ananthapuramu)
(Accredited by NAAC with "A" Grade, NBA (EEE,ECE &ME) & ISO9001:2008CertifiedInstitution)

QUESTIONBANK(DESCRIPTIVE)

Subject Name with Code: Cryptography &Network Security(23A0526T)
Course & Branch: B.TECHCSE, AIML,CSE(CS) Year& Semester: III-IIRegulation: RG23

UNIT - I

S.No.	Question	[BT Level] [CO][Marks]
2 Marks Questions (Short)		
1.	State the **block size and key sizes of AES**.	L1/CO1/2M
2.	What is a **Transposition Cipher**?	L1/CO1/2M
3.	Define the **Symmetric Cipher Model**.	L1/CO1/2M
4.	What is meant by a **Security Attack**?	L1/CO1/2M
5.	What are **Security Mechanisms**? Give two examples.	L1/CO1/2M
6.	List out the Various types of **Security Services**.	L1/CO1/2M
7.	Distinguish between **Passive and Active attacks**	L2/CO1/2M
8.	What is **Steganography**?	L2/CO1/2M
9.	What is **OSI Security Architecture**?	L1/CO1/2M
10.	Define **Computer Security** and state its objectives.	L2/CO1/2M
11.	**Explain OSI Security Architecture**. Describe the components of the architecture and their significance.	L2/CO1/10M
12.	Write short notes on i) cryptography and ii) Steganography	L2/CO1/10M
13.	**Explain Security Attacks**. Classify them into **passive and active attacks** with suitable examples.	L2/CO1/10M
14.	**Explain Security Services** provided by network security. Describe authentication, confidentiality, integrity, and non-repudiation	L2/CO1/10M
15.	**Explain Security Mechanisms**. Discuss how these mechanisms support security services.	L2/CO1/10M
16.	**Explain the Model for Network Security** with a neat diagram and describe the role of encryption and keys.	L4/CO1/10M
17.	**Explain Classical Encryption Techniques**. Describe **substitution techniques and transposition techniques** with examples.	L2/CO1/10M
18.	Explain the encrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to get original plain text. $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	L2/CO1/10M
19.	**Explain the Traditional Block Cipher Structure** and describe the **Data Encryption Standard (DES)** in detail.	L2/CO1/10M
20.	**Explain the Advanced Encryption Standard (AES)**. Describe the **AES structure and transformation functions**.	L2/CO1/10M

UNIT - II

S.No.	Question	[BT Level] [CO][Marks]
2 Marks Questions (Short)		
1.	Define the **Euclidean Algorithm**.	L1/CO2/2M
2.	What is meant by **Modular Arithmetic**?	L1/CO2/2M
3.	State **Fermat's Little Theorem**?	L3/CO2/2M
4.	State **Euler's Theorem**.	L1/CO2/2M
5.	What is the **Chinese Remainder Theorem**?	L1/CO2/2M
6.	Define **Discrete Logarithm**.	L1/CO2/2M
7.	What is a **finite field**?	L1/C02/2M
8.	Define a finite field of the form **GF(p)**.	L2/CO3/2M
9.	What is **Public Key Cryptography**?	L1/CO3/2M
10.	What is **Elliptic Curve Cryptography (ECC)**?	L1/CO3/2M
Descriptive Questions (Long)		
11.	**Explain Fermat's Little Theorem** and **Euler's Theorem**, and describe their significance in modular computations	L1/CO2/10M
12.	State Chinese remainder theorem and find X for the given set of congruent equations using CRT (a) X = 1(mod 5) X = 2(mod 7) X = 3(mod 9) (b) X = 2(mod 3) X = 3(mod 5) X = 2(mod 7) X = 4(mod 11)	L2/CO2/10M
13.	Explain ECC - Diffie Hellman key Exchange with both keys in detail with an example.	L4/CO2/10M
14.	**Analyze** the **Discrete Logarithm Problem** and explain why it is computationally hard.	L2/CO2/10M
15.	Explain the RSA algorithm to perform key generation, encryption, and decryption for secure communication and apply RSA algorithm to the following example: p=7,q=11,e=17,M=8. .	L3/CO3/10M
16.	**Explain** the concept of **Finite Fields** and describe finite fields of the form **GF(p)** and **GF(2^n)**.	L3/CO2/10M
17.	**Analyze** the security of **RSA** based on the integer factorization problem. Explain It?	L4/CO3/10M
18.	**Analyze** the role of **modular arithmetic and finite fields** in public key cryptographic algorithms. Briefly Explain it?	L3/CO2/10M
19.	User Alice & Bob User Alice & Bob exchange the key using Diffie Hellman alg. Assume α=5 q=83 X_A=6 X_B=10. Find Y_A, Y_B, K.	L2/CO2/10M
20.	**Explain** the **Euclidean Algorithm** and **Modular Arithmetic**, and discuss their importance in cryptography.	L2/CO2/10M

Signature of the Staff:

Signature of Department Academic Committee Member 1:

Signature of Department Academic Committee Member 2:

Signature of Department Academic Committee Member 3: