Course Code: 16IT611 **R16**

SIDDHARTH INSTITUTE OF ENGINEERING & TECHNOLOGY: PUTTUR
Siddharth Nagar, NarayanavanamRoad –517583

QUESTION BANK (DESCRIPTIVE)

Subject with Code: INFORMATION SECURITY (16IT611) **Course & Branch**: B. Tech - CSIT

Year & Sem: IV B.Tech & I-Sem **Regulation:** R16

UNIT –I

1 a)	Discuss in detail about various types of Security attacks with neat diagrams.	[L6,CO1]	[6M]
1 b)	What is symmetric key cryptography? Discuss its advantages and limitations?	[L6,CO1]	[6M]
2.	Consider the following: Plaintext: "MONARCHY" Secret key: "INSTRUMENTS" What is the corresponding cipher text using play fair cipher method?	[L5,CO1]	[12M]
3.a)	Describe in detail about Conventional Encryption Model.	[L4,CO1]	[6M]
3.b)	Consider the following: Plaintext: "ACT" Secret key: "GYBNQKURP" Compute the cipher text from given plain text and key using hill cipher method	[L5,CO1]	[6M]
4.	Explain the following substitution techniques with suitable examples. (i) Caesar Cipher (ii) One -Time pad	[L2,CO1]	[12M]
5.	Draw the general structure of DES and explain the encryption-decryption process. Evaluate its strength with DES.	[L6,CO1]	[12M]
6.a)	Describe in detail about Conventional Encryption Model.	[L4,CO1]	[6M]
6.b)	Determine the security mechanisms required to provide various types of security services.	[L5,CO1]	[12M]
7.	Explain the characteristics and operations of RC4 Encryption algorithm	[L2,CO1]	[12M]
8.	Explain the encryption and decryption of AES With neat Diagram.	[L2,CO1]	[12M]
9.a)	Explain about the Encryption and decryption functions Triple DES.	[L2,CO1]	[6M]
9.b)	Explain how diffusion and confusion are used in Block Ciphers	[L2,CO1]	[6M]
10.a)	Differentiate linear and differential crypto-analysis	[L2,CO1]	[6M]
10.b)	Write the difference between a block cipher and a stream cipher	[L2,CO1]	[6M]

Course Code: 16IT611 **R16**

UNIT –II

1	Explain RSA algorithm with suitable examples.	[L2,CO2]	[12M]
2.a)	Determine the GCD(24140,16762) using Euclid's algorithm.	[L5,CO2]	[6M]
2.b)	Compare conventional encryption with public key encryption	[L2,CO2]	[6M]
3.	Perform RSA for Data Confidentiality. Perform RSA Encryption/Decryptic for the following set of data: P=3, Q=11, e=7, M=5.	[L5,CO2]	[12M]
4.	What is public key cryptography? How achieve confidentiality and Authentication using public key cryptography.	[L1,CO2]	[12M]
5.a)	What are the requirements and applications of public key cryptography?	[L1,CO1]	[6M]
5.b)	Discuss about Euler's theorem.	[L6,CO2]	[6M]
6.a)	Explain the Chinese Remainder theorem.	[L2,CO2]	[6M]
6.b)	State Fermat's theorem.	[L2,CO2]	[6M]
7.	What are elliptic curves? Describe how the elliptic curves are useful for Cryptography	[L1,CO2]	[12M]
8.	Analyze how men-in-middle attack is performed on Diffie - Hellman Key exchange algorithm.	[L4,CO2]	[12M]
9.	Design Diffie - Hellman Key exchange algorithm. Evaluate using Diffie - Hellman key exchange technique. Let p=353 be the prime number and α=3 be it's primitive root. Let A and B secret keys Xa =97 and Xb =233. Compute the following : (i)Public key of A and B (ii)Common secret key.	[L5,CO2]	[12M]
10.a)	State modular arithmetic operations with example.	[L2,CO2]	[6M]
10.b)	State Fermat's theorem with example.	[L3,CO1]	[6M]

Course Code: 16IT611 **R16**

UNIT –III

1 a)	List out applications of cryptographic hash functions.	[L1,CO3]	[6M]
1.b)	Explain the characteristics are needed in secure hash function?	[L2,CO3]	[6M]
2.	Describe hash function based on cipher block chaining.	[L6,CO4]	[12M]
3.	What is hash function? Explain the requirements of Hash functions.	[L2,CO2]	[12M]
4.	Explain the process of deriving eighty 64-bit words from 1024 bits for processing of a single blocks and also discuss single round function in SHA-512 algorithm.	[L2,CO1]	[12M]
5.	Describe HMAC algorithm in detail.	[L6,CO1]	[12M]
6.a)	Compare different types of SHA algorithms with parameters.	[L2,C03]	[6M]
6.b)	Discuss about the objectives of HMAC and its security features.	[L2,CO3]	[6M]
7.	Explain the classification of authentication function in detail.	[L2,CO1]	[12M]
8.	Describe simple hash function and birthday attack.	[L6,CO3]	[12M]
9.	Deign RSA-PSS Digital Signature Algorithm	[L6,CO3]	[12M]
10.	Illustrate the following (i)Mask generation function (ii)Signature Verification	[L2,CO3]	[12M]

Course Code: 16IT611 **R16**

UNIT –IV

1	What is secret key distribution? Explain secret key distribution with confidentiality and authentication.	[L1,CO1]	[12M]
2.	Give an overview of X.509 certificates and its formats.	[L3,CO4]	[12M]
3.a)	Enumerate the differences between Kerberos Version 4 and 5.	[L3,CO2]	[6M]
3.b)	Explain the authentication procedures defined by X.509 certificate.	[L3,CO1]	[6M]
4.	Write and explain Client/ Server Authentication Exchange service in Kerberos version.	[L4,CO2]	[12M]
5.	Explain key management and distribution in detail.	[L1,CO1]	[12M]
6.	Draw and explain the architecture model and management functions of Public Key- Infrastructure.	[L1,CO1]	[12M]
7.	Discuss various PGP cryptographic functions and services in detail.	[L3,CO4]	[12M]
8.	Explain how email messages are protected using S/MIME signing and encryption?	[L1,CO2]	[12M]
9.	Write short notes on the following. (i)PGP (ii)S/MIME	[L3,CO1]	[12M]
10.a)	What is Public Key certificate? Explain its usage with X.509 certificates.	[L1,CO1]	[6M]
10.b)	What is Radix 64 format? What is its use in PGP?	[L3,CO1]	[6M]

Course Code: 16IT611 **R16**

UNIT –V

1	What is the use of SSL protocol? Explain SSL record protocol operation with SSL record format.	[L1,CO1]	[12M]
2.	With a neat sketch explain the IPSec scenario and IPSec Services.	[L2,CO1]	[12M]
3.	Why Internet Key Exchange is used? Write and explain header and payload formats of it.	[L1,CO1]	[12M]
4.	Write and explain TLS functions and alert codes of Transport Layer Security.	[L3,CO4]	[12M]
5.	Draw and discuss the Architecture of IPSec.	[L5,CO2]	[12M]
6.	Give the taxonomy of malicious programs. Define each one.	[L1,CO1]	[12M]
7.a)	What are the different types of viruses? How do they get into the systems?	[L1,CO1]	[12M]
7.b)	Explain Intrusion detection in detail.	[L2,CO1]	
8.	What is a firewall? What is the need for firewalls? What is the role of firewalls in protecting networks.	[L1,CO4]	[12M]
9.a)	Explain ESP Header of IPSec.	[L2,CO1]	[12M]
9.b)	What is meant by stateful packet inspection? What are the advantages and disadvantages		
10.	Compare the features of host based IDS and network based IDS. Why, when and where to use host based IDS?	[L2,CO2]	[12M]

Prepared by:
BHUKYA RAJA KUMAR, Assistant Professor.