SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF
ELECTRONICS AND COMMUNCATION ENGINEERING

QUESTION BANK

VI SEMESTER

1906603 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulation – 2019

Academic Year 2024 – 2025 (EVEN SEMESTER)

Prepared by

Dr. C. Saravanakumar, Assistant Professor

SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)
SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF ELECTRONICS AND COMMUNICATION ENGINEERING

QUESTION BANK

SUBJECT: Cryptography and Network Security
SEM / YEAR : VI Sem / III Year

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				
PART – A				
Q.No	**Questions**	**CO**	**BT Level**	**Competence**
1.	Differentiate symmetric and asymmetric encryption?	1	BTL1	Remember
2.	State Legal, Ethical and Professional Aspects of Security.	1	BTL2	Understand
3.	What are the two basic functions used in the encryption algorithm?	1	BTL1	Remember
4.	Why the asymmetric cryptography is bad for huge data? Specify the reason.	1	BTL2	Understand
5.	List the types of attack.	1	BTL1	Remember
6.	Define Model of network security.	1	BTL2	Understand
7.	Identify an example for substitution and transposition ciphers.	1	BTL1	Remember
8.	Explain network security.	1	BTL2	Understand
9.	Distinguish Encryption and Decryption.	1	BTL1	Remember
10.	Define cryptography.	1	BTL2	Understand
11.	What are the 3 aspects of security?	1	BTL1	Remember
12.	Define security mechanisms.	1	BTL2	Understand
13.	Write the difference between Substitution and Transposition techniques.	1	BTL1	Remember
14.	Why it is not practical to use an arbitrary reversible substitution cipher?	1	BTL2	Understand
15.	Compare Block and Stream cipher.	1	BTL1	Remember
16.	Define Cryptanalysis	1	BTL2	Understand
17.	Define Steganography.	1	BTL1	Remember
18.	Decipher the following cipher Text using brute force attack: CMTMROOEOORW (Hint: Algorithm-Rail fence)	1	BTL2	Understand
19.	Convert the Given Text “VALLIAMMAI” into cipher text using Rail fence Technique.	1	BTL1	Remember
20.	Differentiate active attack and passive attack.	1	BTL2	Understand
21.	List out the problems in one time pad	1	BTL1	Remember
22.	Why modular arithmetic has been used in cryptography?	1	BTL2	Understand
23.	Specify the components of encryption algorithm	1	BTL1	Remember
24.	List the entities that are to be kept secret in conventional encryption techniques.	1	BTL2	Understand

PART – B				
1.	Describe the differences between steganography and cryptography with example in details.	1	BTL3	Apply
2.	(i)Define Security trends - Legal, Ethical and Professional aspects of Security (ii) State about the Security at Multiple levels and explain Security Policies	1	BTL4	Analyze
3.	Demonstrate Playfair cipher and Railfence cipher with suitable examples.	1	BTL3	Apply
4.	Discuss about the security goals with respect to cryptography.	1	BTL4	Analyze
5.	i) Define Steganography? Describe various techniques used in Steganography. ii) State mono-alphabetic cipher? How it is different from Caesar cipher	1	BTL3	Apply
6.	Discuss about any 2 substitution Techniques with an example under each technique.	1	BTL4	Analyze
7.	(i) Discuss the various security mechanisms (ii) Summarize OSI security architecture model with neat diagram	1	BTL3	Apply
8.	Given Cipher text "YMJTYMJWXNIJTKXNQJSHJ", the message is encrypted by Caesar cipher and k=5. Decrypt the original message.	1	BTL4	Analyze
9.	Encrypt the following using play fair cipher with the keyword MONARCHY. Use X for the blank spaces. The plain text is "SWARAJ IS MY BIRTH RIGHT".	1	BTL3	Apply
10	Perform encryption and decryption using Hill Cipher for the following. Message: PEN Key: ACTIVATED	1	BTL4	Analyze
11.	(i) Classify and briefly define types of cryptanalytic attacks based on what is known to the attacker. (ii) Explain briefly the two general approaches to attacking a cipher.	1	BTL3	Apply
12.	Examine and Illustrate the network security model and its important parameters with a block diagram.	1	BTL4	Analyze
13.	Evaluate the Characteristics of Modern Cryptography and working Principle.	1	BTL3	Apply
14.	Encrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to get original plain text. $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	1	BTL4	Analyze
15.	Illustrate the Transposition Techniques (any 2) in detail with suitable examples.	1	BTL3	Apply
16.	Apply additive cipher with key = 2- to encrypt the message "this is an exercise". Ignore the spaces between words. Decrypt the message to get the original plain text.	1	BTL3	Apply
17.	Using Vigenere cipher, encrypt the word "explanation" using the Key leg.	1	BTL4	Analyze
PART C				

1.	Illustrate the Classical Encryption Technique with an example.	1	BTL3	Apply
2.	(i) Illustrate the rules to perform encryption using play fair cipher and encrypt 'snowshooos' using 'monarchy' I and J count as one letter and x is the filler letter. (ii) Encrypt the word "Semester Result" with the keyword "Examination" using playfair cipher.	1	BTL4	Analyze
3.	Encrypt the message "FINALYEAR" at the sender end and decrypt the message at receiver end With using Hill-cipher with the key. $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	1	BTL3	Apply
4.	Compare transposition cipher and substitution cipher. Apply two stage transpositions Cipher on the "treat diagrams as single units" using the keyword "sequence".	1	BTL4	Analyze
5.	Discuss examples from real life, where the following security objectives are needed: (i) Confidentiality (ii) Integrity (iii) Non- repudiation Suggest suitable security mechanisms to achieve them.	1	BTL3	Apply

UNIT II - SYMMETRIC CRYPTOGRAPHY				
MATHEMATICS OF SYMMETRIC KEY CRYPTOGRAPHY: Algebraic structures - Modular arithmetic- Euclid's algorithm- Congruence and matrices - Groups, Rings, Fields- Finite fields- SYMMETRIC KEY CIPHERS**:** SDES – Block cipher Principles of DES – Strength of DES – Differential and linear cryptanalysis - Block cipher design principles – Block cipher mode of operation – Evaluation criteria for AES – Advanced Encryption Standard - RC4 – Key distribution				
PART – A				
Q.No	**Questions**	**CO**	**BT Level**	**Competence**
1.	Write the Euclidean Algorithm.	2	BTL1	Remember
2.	List the fundamental elements of abstract algebra or modern algebra	2	BTL2	Understand
3.	Why set of all Integers is not a field?	2	BTL1	Remember
4.	Assume that a = 255 and n = 11. We can find q = 23 and r = 2 using the division algorithm we have learned in arithmetic. Calculate q and r for a= -255 and n=11	2	BTL2	Understand
5.	Define Finite Group	2	BTL1	Remember
6.	Find gcd (1970, 1066) using Euclid's algorithm.	2	BTL2	Understand
7.	What is the difference between a block cipher and a stream cipher?	2	BTL1	Remember
8.	State the five modes of operation of block cipher?	2	BTL2	Understand
9.	Explain the strength of triple DES.	2	BTL1	Remember
10.	Explain S-DES Structure.	2	BTL2	Understand
11.	What is triple encryption? How many keys are used in triple encryption?	2	BTL1	Remember
12.	Show general design of S-AES encryption cipher	2	BTL2	Understand

13.	Identify Data units used in AES.	2	BTL1	Remember
14.	Find 11^7 mod 13.	2	BTL2	Understand
15.	Compare DES and AES.	2	BTL1	Remember
16.	List the parameters (block size, key size and no. of rounds) for the three AES versions.	2	BTL2	Understand
17.	Explain idea of RC4 stream cipher.	2	BTL1	Remember
18.	Explain Flat Multiple KDCs.	2	BTL2	Understand
19.	Discuss Key-Distribution Center.	2	BTL1	Remember
20.	Explain Hierarchical Multiple KDCs.	2	BTL2	Understand
21.	What is the difference between diffusion and confusion?	2	BTL1	Remember
22.	Brief the strengths of triple DES.	2	BTL2	Understand
23.	Is it possible to use the DES algorithm to generate message authentication code? Justify.	2	BTL1	Remember
24.	Write down the difference between the public key and private key cryptosystems.	2	BTL2	Understand
	PART – B			
1.	Describe Modulo Arithmetic operations and properties in detail.	2	BTL3	Apply
2.	(i) Describe in detail the key generation in AES algorithm and its expansion format (ii) Describe Triple DES and its applications.	2	BTL4	Analyze
3.	Describe AES algorithm with all its round functions in detail.	2	BTL3	Apply
4.	Describe DES algorithm with neat diagram and explain the steps.	2	BTL4	Analyze
5.	Solve gcd(98, 56) using Extended Euclidean algorithm. Write the algorithm also	2	BTL3	Apply
6.	Discuss the following in detail (i) Modular Exponentiation (ii) Finite fields	2	BTL4	Analyze
7.	Explain the DES and General structure of DES with diagrams.	2	BTL3	Apply
8.	Identify the purpose of Differential and linear cryptanalysis and explain with neat diagram.	2	BTL4	Analyze
9.	For each of the following elements of DES, indicate the comparable element in AES if available. i) XOR of sub key material with the input to the function ii) f function iii) Permutation p iv) Swapping of halves of the block.	2	BTL3	Apply
10	Explain the following modes of operation in block cipher. (i) Electronic code book. (ii) Cipher block chaining.	2	BTL4	Analyze
11.	(i) How Meet in the middle attack is performed on double Data encryption Standard? (ii) Explain the substitution bytes transformation and add round	2	BTL3	Apply

	key transformation of AES cipher.			
12.	Discuss the properties that are to be satisfied by Groups, Rings and Fields.	2	BTL4	Analyze
13.	Explain about Block cipher design principles – Block cipher mode of operation.	2	BTL3	Apply
14.	Discuss about Public Key distribution and Symmetric-Key Distribution.	2	BTL4	Analyze
15.	Explain the Cipher feedback mode and output feedback mode of operation in block cipher.	2	BTL3	Apply
16.	Find 11^{13} mod 53 using modular exponentiation.	2	BTL3	Apply
17.	Demonstrate that the set of polynomials whose coefficients forms a field is a ring.	2	BTL4	Analyze
PART C				
1.	What do you mean by AES? Diagrammatically illustrate the structure of AES and describe the steps in AES encryption process with example.	2	BTL3	Apply
2.	Discuss Structure of Simplified DES (S-DES) and Cipher and Reverse Cipher.	2	BTL4	Analyze
3.	Explain Key-distribution center with all aspects with neat diagram.	2	BTL3	Apply
4.	Measure the Public key-distribution and Symmetric Key-Distribution.	2	BTL4	Analyze
5.	(i) Explain the bitwise XOR operation which involved in RC4? (ii) In finite arithmetic $(x^6 + x^4 + x^2 + x + 1) + (7 + x + 1) = ?$	2	BTL3	Apply

UNIT III - PUBLIC KEY CRYPTOGRAPHY				
MATHEMATICS OF ASYMMETRIC KEY CRYPTOGRAPHY: Primes – Primality Testing – Factorization – Euler‘s totient function, Fermat‘s and Euler‘s Theorem - Chinese Remainder Theorem – Exponentiation and logarithm - ASYMMETRIC KEY CIPHERS: RSA cryptosystem – Key distribution –Key management – Diffie Hellman key exchange - ElGamal cryptosystem – Elliptic curve arithmetic-Elliptic curve cryptography.				
PART – A				
Q.No	**Questions**	**CO**	**BT Level**	**Competence**
1.	Define Co primes.	3	BTL1	Remember
2.	Define Euler’s theorem.	3	BTL2	Understand
3.	What is a primitive root of a number?	3	BTL1	Remember
4.	State Fundamental Theorem of Arithmetic.	3	BTL2	Understand
5.	Define Euler’s totient function.	3	BTL1	Remember
6.	State Fermat’s little theorem.	3	BTL2	Understand
7.	Mention any two methods for testing prime numbers.	3	BTL1	Remember
8.	Why is asymmetric cryptography bad for huge data? Specify the reason.	3	BTL2	Understand
9.	Compare public key and private key.	3	BTL1	Remember
10.	Explain elliptic curve.	3	BTL2	Understand

11.	Explain whether symmetric and asymmetric cryptographic algorithm need key exchange.	3	BTL1	Remember
12.	Point out the applications of the public key cryptosystem	3	BTL2	Understand
13.	What is key distribution center?	3	BTL1	Remember
14.	Illustrate the purpose of Diffie Hellman key exchange.	3	BTL2	Understand
15.	Explain Elliptic Curves over Real Numbers	3	BTL1	Remember
16.	Explain attacks of RSA cryptosystem	3	BTL2	Understand
17.	What is Diffie-Hellman Key exchange?	3	BTL1	Remember
18.	Write any one technique attacking in RSA.	3	BTL2	Understand
19.	Give the significance of hierarchical key control.	3	BTL1	Remember
20.	Are strong primes necessary in RSA?	3	BTL2	Understand
21.	What is the use of Fermat's Theorem?	3	BTL1	Remember
22.	For long messages, RSA will be applied in blocks. If the block is very small, say it contains only one letter in each block, will the encryption be secure?	3	BTL2	Understand
23.	What is discrete logarithm?	3	BTL1	Remember
24.	State the difference between conventional encryption and public key encryption.	3	BTL2	Understand
	PART – B			
1.	Describe RSA algorithm with an example.	3	BTL3	Apply
2.	Prove the Following (i). If p is a prime and a is a positive integer relatively prime to p, then $a^{p-1} \equiv 1 \pmod p$ (ii). If p is a prime and a is a positive integer, then $a^p \equiv a \pmod p$.	3	BTL4	Analyze
3.	Prove the following (i).If n and a are coprime, then $a\varphi(n) \equiv 1 \pmod n$. (ii) Use Euler's Theorem to find a number *a* between 0 and 9 such that *a* is congruent to 7^{1000} modulo 10. (Note that this is the same as the last digit of the decimal expansion of 7^{1000}.)	3	BTL3	Apply
4.	With a neat sketch explain the Elliptic curve cryptography with an example.	3	BTL4	Analyze
5.	Perform encryption and decryption using RSA algorithm for p=17, q=11,e=7 and m=88.	3	BTL3	Apply
6.	Discuss how discrete logarithm evaluated for a number? What is the role of discrete log in the Diffie - Hellman key exchange in exchanging the secret key among two users?	3	BTL4	Analyze
7.	Explain the Key generation, encryption, and decryption in ElGamal.	3	BTL3	Apply
8.	Find the secret key shared between user A and user B using Diffie- Hellman algorithm for the following q=353; α (primitive root)=3, X_A=45 and X_B=50	3	BTL4	Analyze
9.	Experiment with Taxonomy of potential attacks on RSA.	3	BTL3	Apply
10	Explain Chinese Remainder theorem and find X for the given set of congruent equation using CRT $X \equiv 2 \pmod 3$ $X \equiv 3 \pmod 5$ $X \equiv 2 \pmod 7$	3	BTL4	Analyze
11.	Examine Elliptic Curve Cryptography Simulating ElGamal.	3	BTL3	Apply
12.	Perform encryption and decryption using RSA algorithm for the following: p=7 q=11, e=7, M=9.	3	BTL4	Analyze

13.	Users A and B use the Diffie-Hellman key exchange technique, a common prime q=11 and a primitive root alpha=7. (i) If user A has private key XA=3.What is A's public key YA? (ii) If user B has private key XB=6. What is B's public key YB? (iii) What is the shared secret key? Also write the algorithm.	3	BTL3	Apply
14.	Summarize Chinese Remainder theorem and find X for the given set of congruent equation using CRT $X \equiv 1 \pmod 5$ $X \equiv 2 \pmod 7$ $X \equiv 3 \pmod 9$ $X \equiv 4 \pmod{11}$	3	BTL4	Analyze
15.	Discuss the Diffie-Hellman key exchange algorithm with its merits and demerits.	3	BTL3	Apply
16.	Explain public key cryptography and when it is preferred.	3	BTL3	Apply
17.	What are elliptic curves? And also discuss how the elliptic curves are useful for Cryptography?	3	BTL4	Analyze
	PART C			
1.	Users Alice and Bob use the Diffie-Hellman key exchange technique with a common prime q = 83 and a primitive root α = 5. i) If Alice has a private key $X_A = 6$, what is Alice's public key Y_A? ii) If Bob has a private key $X_B = 10$, what is Bob's public key Y_B? iii) Construct the shared secret key	3	BTL3	Apply
2.	State and prove the Chinese remainder theorem. What are the last two digits of 49^{19}?	3	BTL4	Analyze
3.	In RSA system, the public key of a given user is e= 7 and n =187. (i) What is the private key of this user? (ii) If the intercepted cipher text is c= 11 and sent to a user whose public key is e = 7 and n = 187. What is the plain text?	3	BTL3	Apply
4.	Discuss the ElGamal cryptosystem and elliptic curve cryptosystem.	3	BTL4	Analyze
5.	Consider the group $E_{23}(9,17)$. This is the group defined by the equation $y^2 \bmod 23 = (x^3 + 9x + 17) \bmod 23$. What is the discrete logarithm K of Q = (4,5) to the base P = (16,5)?	3	BTL3	Apply

UNIT IV - MESSAGE AUTHENTICATION AND INTEGRITY				
Authentication requirement – Authentication function – MAC – Hash function – Security of hash function and MAC – SHA –Digital signature and authentication protocols – DSS- Entity Authentication: Biometrics, Passwords, Challenge Response protocols- Authentication applications - Kerberos, X.509				
PART – A				
Q.No	**Questions**	**CO**	**BT Level**	**Competence**
1.	State any three requirements for authentication.	4	BTL1	Remember
2.	Point out the properties a digital signature.	4	BTL2	Understand
3.	What is the role of compression function in hash function?	4	BTL1	Remember
4.	Define the term message digest.	4	BTL2	Understand
5.	Define the classes of message authentication function.	4	BTL1	Remember
6.	List the authentication message requirements.	4	BTL2	Understand
7.	How is the security of a MAC function expressed?	4	BTL1	Remember
8.	Identify the requirements for message authentication.	4	BTL2	Understand

9.	Give the two approaches of digital signature.	4	BTL1	Remember
10.	Explain the significance of signature function in Digital Signature Standard (DSS) approach.	4	BTL2	Understand
11.	Specify any 3 types of authentication protocol.	4	BTL1	Remember
12.	How digital signatures differ from authentication protocols?	4	BTL2	Understand
13.	How do you specify various types of authentication protocol?	4	BTL1	Remember
14.	When are the certificates revoked in X.509?	4	BTL2	Understand
15.	What is Kerberos? Point out its uses.	4	BTL1	Remember
16.	Identify 4 requirements defined by Kerberos.	4	BTL2	Understand
17.	Summarize the Classes of message authentication function.	4	BTL1	Remember
18.	What entities constitute a full service in Kerberos environment?	4	BTL2	Understand
19.	Show how SHA is more secure than MD5.	4	BTL1	Remember
20.	Create a simple authentication dialogue used in Kerberos.	4	BTL2	Understand
21.	What is a Hash in cryptography?	4	BTL1	Remember
22.	Mention the two types of certificates?	4	BTL2	Understand
23.	Is it necessary to recover the secret key in order to attack a MAC algorithm?	4	BTL1	Remember
24.	What is a birthday attack?	4	BTL2	Understand
PART – B				
1.	Where hash functions are used? What characteristics are needed in secure hash function? Write about the security of hash functions and MACs.	4	BTL3	Apply
2.	Describe digital signature algorithm and show how signing and Verification is done using DSS.	4	BTL4	Analyze
3.	Describe SHA2 in detail with neat diagram.	4	BTL3	Apply
4.	What is Digital Signature? Explain how it is created at the sender end and retrieved at receiver end .differentiate digital signature from digital certificate.	4	BTL4	Analyze
5.	How Hash function algorithm is designed? Explain their features and properties.	4	BTL3	Apply
6.	(i)Explain in detail message authentication code and its requirements. (ii)Illustrate the security of hash functions and MACs.	4	BTL4	Analyze
7.	Describe Challenge-Response protocols in detail.	4	BTL3	Apply
8.	List the design objectives of HMAC and explain the algorithm in detail.	4	BTL4	Analyze
9.	Illustrate the steps involved in Signature generation and verification functions of DSS.	4	BTL3	Apply
10	Elaborate in detail about X.509 authentication services.	4	BTL4	Analyze
11.	Explain Client Server Mutual authentication with an example flow diagram.	4	BTL3	Apply
12.	(i)What is Kerberos? Explain how it provides authenticated Services (ii)Explain the format of the X.509 certificate.	4	BTL4	Analyze
13.	Discuss the roles of the different servers in Kerberos protocol. How does the user get authenticated to the different servers?	4	BTL3	Apply
14.	Explain briefly about the architecture and certification mechanisms in Kerberos and X.509.	4	BTL4	Analyze

15.	Suggest and explain about an authentication scheme for mutual authentication between the user and the server which relies on symmetric encryption.	4	BTL3	Apply
16.	Using the schnorr scheme, let q = 83, p = 997 and d= 23. Find the values for e_1 and e_2. Choose r = 11, if M = 400 and h(400) = 100. Find value of S_1,S_2?	4	BTL3	Apply
17.	Discuss the classification of authentication function in detail.	4	BTL4	Analyze
	PART C			
1.	With a neat diagram, explain the steps involved in SHA algorithm for encrypting a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest.	4	BTL3	Apply
2.	Create 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. Show the values of W16, W17, W18 and W19.	4	BTL4	Analyze
3.	(i) Enumerate the properties of Hash Function. (ii) Evaluate the authentication protocol and list its limitations, how the limitations overcome.	4	BTL3	Apply
4.	(i) Elaborate the way how the limitations of Kerberos version 4 is overcome in the environmental shortcomings and technical deficiencies. (ii) Elaborate how the encryption is key generated from password in Kerberos.	4	BTL4	Analyze
5.	Consider a banking application that is expected to provide cryptographic functionalities. Assume that this application is running in top of another application wherein the end customer can perform a single task of fund transfer. The application requires cryptographic requirements based on the amount of transfer. **Transfer Amount** / **Cryptographic functions required** 1-2000 — Message Digest 2001-5000 — Digital Signature 5000 and above — Digital Signature and encryption Suggest the security scheme to be adopted in client and server side to accommodate the above requirements and justify your recommendations.	4	BTL3	Apply

UNIT V - SECURITY PRACTICE AND SYSTEM SECURITY				
Electronic Mail security – PGP, S/MIME – IP security – Web Security - SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls				
PART – A				
Q.No	**Questions**	**CO**	**BT Level**	**Competence**
1.	Define S/MIME.	5	BTL1	Remember
2.	Expand and define SPI.	5	BTL2	Understand
3.	Identify the steps involved in SET Transactions.	5	BTL1	Remember
4.	Define SET? What are the features of SET?	5	BTL2	Understand

5.	Specify the benefits of IPSecurity.	5	BTL1	Remember
6.	What are the major issues derived by Porras about the design of a distributed intrusion detection system?	5	BTL2	Understand
7.	How can the signed data entity of S/MIME be prepared? Give the steps.	5	BTL1	Remember
8.	Differentiate transport and tunnel mode in IPsec.	5	BTL2	Understand
9.	Point out the services provided by PGP?	5	BTL1	Remember
10.	Explain the protocols used to provide IP security.	5	BTL2	Understand
11.	What is a virus in a computer?	5	BTL1	Remember
12.	What are the various types of firewall and its design goal?	5	BTL2	Understand
13.	Mention the three classes of Intruders.	5	BTL1	Remember
14.	What is a Threat? List their types.	5	BTL2	Understand
15.	State the difference between threats and attacks.	5	BTL1	Remember
16.	Differentiate spyware and virus.	5	BTL2	Understand
17.	Give the advantages of intrusion detection system over firewall.	5	BTL1	Remember
18.	Show the design goals of firewalls.	5	BTL2	Understand
19.	Discriminate statistical anomaly detection and rule based detection	5	BTL1	Remember
20.	Does the firewall ensure 100% security to the system? Comment.	5	BTL2	Understand
21.	What is botnets?	5	BTL1	Remember
22.	What is a worm?	5	BTL2	Understand
23.	What is logic bomb?	5	BTL1	Remember
24.	Enlist 4 types of viruses.	5	BTL2	Understand
	PART – B			
1.	Describe the working of SET with neat diagram.	5	BTL3	Apply
2.	Describe in detail about SSL/TLS.	5	BTL4	Analyze
3.	Explain the architecture of IPsec in detail in detail with a neat block diagram.	5	BTL3	Apply
4.	Describe in detail about S/MIME.	5	BTL4	Analyze
5.	Discuss about authentication header and ESP in detail with their packet format.	5	BTL3	Apply
6.	Elaborate on PGP cryptographic functions in detail with suitable block diagrams.	5	BTL4	Analyze
7.	(i) Discuss transport mode and tunnel mode authentication in IP? Describe how ESP is applied to both these modes. (ii) Draw the IP security authentication header and describe the functions of each field.	5	BTL3	Apply
8.	Explain the operational description of PGP.	5	BTL4	Analyze
9.	Illustrate the working principle of SET relate EST for Ecommerce applications.	5	BTL3	Apply
10	Explain how firewalls help in the establishing a security framework for an organization.	5	BTL4	Analyze
11.	Discuss the architecture of distributed intrusion detection system with necessary diagrams.	5	BTL3	Apply
12.	Elaborate the taxonomy of malicious programs	5	BTL4	Analyze
13.	Explain intrusion detection system (IDS) in detail with suitable diagrams.	5	BTL3	Apply
14.	Illustrate the various types of firewalls with neat diagrams.	5	BTL4	Analyze

15.	Compare Authentication Header(AH) and Encapsulating Security Payload (ESP)	5	BTL3	Apply
16.	Analyze various types of virus and its counter measures.	5	BTL4	Analyze
17.	How does screened host architecture for firewall differ from screened subnet firewall architecture? Which offers more security for information assets on trusted network? Explain with neat sketch.	5	BTL3	Apply
	PART C			
1.	Evaluate the performance of PGP. Compare it with S/MIME.	5	BTL3	Apply
2.	(i) Write the steps involved in the simplified form of the SSL / TLS protocol. (ii) Generalize the methodology involved in computing the keys in SSL / TLS protocol.	5	BTL4	Analyze
3.	(i) Explain the various measures that may be used for intrusion detection. (ii) Explain the various roles of firewalls and related terminology in detail.	5	BTL3	Apply
4.	Elaborate how secure electronic transaction (SET) protocol enables e- transactions. Explain the components involved.	5	BTL4	Analyze
5.	Explain the different types of virus in detail. Suggest scenarios for deploying these types in network scenario.	5	BTL3	Apply