SRM VALLIAMMAI ENGINEERING COLLEGE

(An Autonomous Institution)

SRM Nagar, Kattankulathur – 603 203

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
&
DEPARTMENT OF INFORMATION TECHNOLOGY

QUESTION BANK

VII SEMESTER

1904005- CRYPTOGRAPHY AND NETWORK SECURITY

Regulation – 2019

Academic Year 2022 – 2023
(ODD SEMESTER)

Prepared by

Ms. S. Benila, Assistant Professor (Sr. G) / CSE
Ms. S. Shanthi, Assistant Professor (Sr. G) / CSE
Ms. V. Prema, Assistant Professor (Sr. G) / CSE
Ms. S. Shenbagavadivu, Assistant Professor (Sr. G) / IT
Ms. T. Suganya, Assistant Professor (O. G) / IT

SRM VALLIAMMAI ENGINEERING COLLEGE

SRM Nagar, Kattankulathur – 603 203.

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING

QUESTION BANK

SUBJECT : 1904005- Cryptography and Network Security

SEM / YEAR: VII/IV

UNIT I -INTRODUCTION & NUMBER THEORY

Services, Mechanisms and attacks-the OSI security architecture-Network security model-Classical Encryption techniques (Symmetric cipher model, substitution techniques, transposition techniques, steganography). FINITE FIELDS AND NUMBER THEORY: Modular arithmetic-Euclid’s algorithm- Prime numbers-Fermat’s and Euler’s theorem-Testing for primality -The Chinese remainder theorem- Discrete logarithms

PART – A

Q.No	Questions	BT	Competence
1	Differentiate active attacks and passive attacks.	BTL-2	Understanding
2	Define cryptography	BTL-1	Remembering
3	Identify the types of attack.	BTL-3	Applying
4	Define cryptanalysis.	BTL-1	Remembering
5	List out the components of encryption algorithm.	BTL-1	Remembering
6	Compare Substitution and Transposition techniques.	BTL-4	Analyzing
7	Analyse how brute force attack is used in Network?	BTL-4	Analyzing
8	List the four categories of security threats.	BTL-1	Remembering
9	Calculate GCD of 1970 and 1066 using Euclid algorithm.	BTL-3	Applying
10	Define primitive root.	BTL-1	Remembering
11	Give examples for substitution cipher.	BTL-2	Understanding
12	Define Steganography	BTL-1	Remembering
13	Explain why Modular arithmetic has been used in cryptography.	BTL-5	Evaluating
14	Compare threats and attacks.	BTL-4	Analyzing
15	Classify the basic functions used in encryption algorithms.	BTL-3	Applying
16	Describe security mechanism.	BTL-2	Understanding
17	Assess the following cipher text using brute force attack: CMTMROOEOORW (Hint: Algorithm-Rail fence).	BTL-5	Evaluating
18	Generalize why network need security.	BTL-6	Creating
19	Convert the given text “VALLIAMMAI” into cipher text using Rail fence Technique.	BTL-5	Evaluating
20	Plan how many keys are required by two people to communicate via a cipher.	BTL-6	Creating
21	Describe Euler’s theorem.	BTL-2	Understanding
22	Why is asymmetric cryptography bad for huge data? Specify the reason?	BTL-4	Analyzing
23	State Fermat’s theorem	BTL-2	Understanding
24	Find 117 mod 13	BTL-3	Applying

PART – B

1	List and briefly describe categories of passive and active security attacks. (13)	BTL-1	Remembering
2	Explain about the model for network Security with neat diagram. (13)	BTL-2	Understanding
3	Tabulate the substitution Techniques in detail. (13)	BTL-1	Remembering
4	Describe the Transposition Techniques in detail. (13)	BTL-2	Understanding
5	Explain the OSI security architecture in detail. (13)	BTL-1	Remembering
6	i) Discuss Play fair cipher in detail. (6) ii) Encrypt the following using play fair cipher using the keyword MONARCHY. Use X for blank spaces “SWARAJ IS MY BIRTH RIGHT” (7)	BTL-3	Applying
7	i) Apply Caesar cipher and k=5 decrypt the given Cipher text “YMJTYMJWXNIJTKXNQJSHJ”. (5) ii) Apply Vigenere cipher, encrypt the word “explanation” Classical cryptosystems and its types using the key “leg”. (8)	BTL-3	Applying
8	Describe the following encryption methods in detail: (i) Play fair cipher (4) (ii) Railfence cipher (4) (iii)Vigenere cipher (5)	BTL-1	Remembering
9	(i)What is Steganography? Briefly examine any three techniques. (7) (ii)What is mono-alphabetic cipher? Examine how it differs from Caesar cipher? (6)	BTL-4	Analyzing
10	Demonstrate the encryption of the message “PAY” using hill cipher with the following key matrix and show the decryption. (13) $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	BTL-3	Applying
11	Discuss the following (i) Security services. (7) (ii) Security mechanisms. (6)	BTL-2	Understanding
12	Explain briefly the two general approaches to attacking a cipher. (13)	BTL-4	Analyzing
13	State and Describe Fermat’s theorem. (7) Evaluate 3^{21} mod 11 using Fermat’s theorem. (6)	BTL-5	Evaluating

14	State Chinese Remainder theorem
	Find X for the given set of congruent equations using CRT.
	X=2(mod 3)
	X=3(mod 5)
	X=2(mod 7) (13)
		BTL-5	Evaluating

15	Discuss the properties that are satisfied by modular arithmetic. (13)	BTL-2	Understanding
16	State and prove: i) Euler’s theorem. (6) ii) Euclid’s Algorithm. (7)	BTL-4	Analyzing

17	Explain how to test for primality? (6) Compose a solution for 11^{13} mod 53 using modular exponentiation. (7)	BTL-6	Creating

PART – B

1.	Summarize the relationship between security services and security mechanisms. (15)	BTL-5	Evaluating
2.	(i) Rewrite 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. (8) (ii) Encrypt the word “Semester Result” with the keyword “Examination” using play fair cipher. List the rules used (7)	BTL-6	Creating
3.	Encrypt the message “FINALYEAR” at the sender end and decrypt the message at receiver end With using Hill-cipher with the key. (15) $k = \begin{pmatrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{pmatrix}$	BTL-5	Evaluating
4.	(i) Generalize the rules for mono alphabet and poly alphabet substitution methods. (7) (ii) Apply two stage transpositions Cipher on the “treat diagrams as single units” using the keyword sequence”(8)	BTL-6	Creating
5	State and prove the Chinese remainder theorem with an example. (15)	BTL-5	Evaluating

UNIT II - BLOCK CIPHERS & PUBLIC KEY CRYPTOGRAPHY

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**	**BT Level**	**Competence**
1	What is the difference between a block cipher and a stream cipher?	BTL-2	Understanding
2	Define Diffusion.	BTL-1	Remembering
3	Differentiate substitution and permutation.	BTL-4	Analyzing
4	Explain S box in DES Structure.	BTL-2	Understanding
5	List the five modes of operation of block cipher.	BTL-1	Remembering
6	What is called as avalanche effect?	BTL-1	Remembering
7	Compare Forward and reverse substitute byte transformation.	BTL-5	Evaluating
8	Give the strengths of Triple DES.	BTL-2	Understanding
9	Show general design of S-AES encryption cipher.	BTL-1	Remembering
10	Examine Data units used in AES.	BTL-3	Applying
11	Show the four different stages of each round in AES.	BTL-3	Applying

12	Criticise why the middle portion of triple DES a decryption rather than encryption?	BTL-4	Analyzing
13	List the function of state array.	BTL-1	Remembering
14	Point out is it possible to use the DES algorithm to generate message authentication code.	BTL-4	Analyzing
15	Discover the difference between sub bytes and sub words.	BTL-3	Applying
16	Describe the triple encryption. How many keys are used in triple encryption?	BTL-2	Understanding
17	Compare DES and AES.	BTL-4	Analyzing
18	Assess the parameters (block size, key size and no. of rounds) for the threeAES versions.	BTL-5	Evaluating
19	Explain idea of RC4 stream cipher.	BTL-5	Evaluating
20	List the evaluation criteria for AES algorithm.	BTL-1	Remembering
21	Discuss the relationship between the key length and state vector in RC4 algorithm.	BTL-2	Understanding
22	Discover the use of nonce in key distribution.	BTL-3	Applying
23	Discuss the need of key-distribution center.	BTL-6	Creating
24	Explain Hierarchical Multiple KDCs.	BTL-6	Creating
PART – B			
1	Describe in detail, AES algorithm with round functions. (13)	BTL-1	Remembering
2	Describe DES algorithm with neat diagram and explain the steps. (13)	BTL-1	Remembering
2	Explain in detail about (i) Cipher block chaining. (7) (ii) Cipher feedback mode. (6)	BTL-4	Analyzing
3	Explain in detail about (i) Electronic codebook mode (7) (ii) Output feedback mode. (6)	BTL-4	Analying
4	(i) Formulate the single round of DES algorithm. (7) (ii)Design the key generation process of DES. (6)	BTL-6	Creating
5	(i) Describe the RC4 method used for encryption and decryption. (13)	BTL-1	Remembering
6	Examine the General structure of DES with diagrams. (13)	BTL-1	Remembering
7	(i) Analyze how men in middle attack is performed on double Data Encryption Standard. (7) (ii) Explain the substitution bytes transformation and add round key transformation of AES cipher. (6)	BTL-4	Analyzing
8	Describe in detail the key generation in AES algorithm and its key expansion format. (13)	BTL-2	Understanding
9	Discover the purpose of Differential and linear cryptanalysis and explain with neat diagram. (13)	BTL-3	Applying
10	For each of the following elements of DES, indicate the comparable element in AES if available.	BTL-6	Creating

	(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. (13)		
11	Summarize the block cipher design principles. (13)	BTL-2	Understanding
12	Describe the modes of operation in block cipher. (13)	BTL-2	Understanding
13	Discuss Evaluation criteria for AES (13)	BTL-2	Understanding
14	(i) Describe Triple DES and its applications. (7) (ii) Identify the strength of DES algorithm. (6)	BTL-3	Applying
15	Explain the stream generation process in RC4 algorithm. (13)	BTL-5	Evaluating
16	Illustrate the key distribution scenario and explain in detail. (13)	BTL-3	Applying
17	Summarize the following: (i) Hierarchical key control (7) (ii) Decentralized key control. (6)	BTL-5	Evaluating
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. (15)	BTL-5	Evaluating
2	Design the Structure of Simplified DES (S-DES) with Ciphering and Reverse Ciphering. (15)	BTL-6	Creating
3	Explain Key-distribution center with all aspects with neat diagram. (15)	BTL-5	Evaluating
4	Compose public key and secret key distribution mechanisms in detail. (15)	BTL-6	Creating
5	Compare and Contrast the encryption and decryption steps of DES and AES. Which one is more secure? Justify your answer. (15)	BTL-5	Evaluating

UNIT III PUBLIC KEY CRYPTOGRAPHY

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	BT Level	Competence
1	Give the applications of the public key crypto systems.	BTL-2	Understanding
2	Write the roles of public and private key.	BTL-1	Remembering
3	Discover the Difference between public key and conventional encryption.	BTL-3	Applying
4	Write the three broad categories of applications of public key cryptosystems.	BTL-2	Understanding
5	Analyse the purpose of Diffie Hellman key exchange.	BTL-4	Analyzing
6	Define the principle elements of a public key crypto system.	BTL-1	Remembering
7	Examine the requirements for public key cryptosystems.	BTL-1	Remembering

8	List four general characteristics of schema for the distribution of the public key.	BTL-1	Remembering
9	Show what requirements must a public key crypto system to fulfil security.	BTL-3	Applying
10	Evaluate the formula for encryption and decryption using RSA algorithm.	BTL-5	Evaluating
11	Generalize elliptic curve cryptography.	BTL-6	Creating
12	Express the key generation process of RSA algorithm.	BTL-2	Understanding
13	Compare public key and private key.	BTL-2	Understanding
14	Explain whether symmetric and asymmetric cryptographic algorithm need key exchange.	BTL-4	Analyzing
15	List four general categories of schemes for the distribution of public keys.	BTL-1	Remembering
16	Draw a neat sketch showing the key distribution scenario	BTL-3	Applying
17	Illustrate the purpose of Diffie Hellman key exchange.	BTL-3	Applying
18	Infer Elliptic Curves over Real Numbers	BTL-4	Analyzing
19	Point out the attacks of RSA cryptosystem	BTL-4	Analyzing
20	Perform encryption and decryption using RSA algorithm for the following.p=7, q=11; e=17; m=8.	BTL-5	Evaluating
21	Define abelian group	BTL-1	Remembering
22	Prepare the counter measures for timing attacks in RSA.	BTL-5	Evaluating
23	Give the role of certificate authority in the exchange of public keys.	BTL-2	Understanding
24	Are strong primes necessary in RSA?	BTL-6	Creating
	PART B		
1	Explain about RSA algorithm highlighting its computational aspects. (13)	BTL-1	Remembering
2	Summarize the security aspects of RSA algorithm. (13)	BTL-2	Understanding
3	Discover the possible threats for RSA algorithm and list their counter measures. (13)	BTL-3	Applying
4	(i) Describe RSA Algorithm. (7) (ii) Estimate the encryption and decryption values for the RSA algorithm parameters.P=7,Q=11,E=17,M=8. (6)	BTL-2	Understanding
5	(i) Apply the mathematical foundations of RSA algorithm. (6) **(ii)** Perform encryption and decryption using RSA algorithm for p=17, q=11,e=7 m=88. (7)	BTL-3	Applying
6	. Perform encryption decryption for the following data. P=17, q=7, e=5, n=119, message=”6”. Use Extended Euclid’s algorithm to find the private key. (13)	BTL-3	Applying
7	Describe Diffie-Hellman key exchange with an example. (13)	BTL-1	Remembering
8	Explain with necessary example the concept of man-in-the-middle attack. (13)	BTL-4	Analyzing
9	Evaluate using Diffie-Hellman key exchange technique. Users A and B use a common prime q=11 and a primitive root alpha=7. (13)	BTL-5	Evaluating

	(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.		
10	(i) Summarize the role of discrete log in the Diffie-Hellman key exchange in exchanging the secret key among two users. (7) (ii) What are elliptic curves? Describe how the elliptic curves are useful for Cryptography? (6)	BTL-2	Understanding
11	With a neat sketch explain the Elliptic curve cryptography with an example. (13)	BTL-1	Remembering
12	User A and B use Diffie-Hellman key exchange a common prime q=71 and a primitive root α = 7. Calculate the following.If user A has private key X_A=5, what is A's public key Y_A. If user A has private key XB=12, what is B's public key YB and what is shared secret key? (13)	BTL-4	Analyzing
13	Generalize the Key generation, encryption, and decryption in ElGamal. (13)	BTL-6	Creating
14	(i) Explain briefly about Diffie-Hellman key exchange algorithm with its pros and cons. (7) (ii) Explain public key cryptography and when is it preferred. (6)	BTL-4	Analying
15	Describe the key management of public key encryption in detail. (13)	BTL-1	Remembering
16	Explain in detail about the public key distribution of secret keys. (13)	BTL-5	Evaluating
17	Summarize the categories of Distribution of public keys. (13)	BTL-2	Understanding
PART C			
1	Consider the elliptic curve E11 (1, 6); that is the curve is defined by $y^2=x^3+x+6$ with a modules of P=11. Calculate all the points in E11 (1, 6). Start by calculation the right hand side of the equation of all the values of n? (15)	BTL-5	Evaluating
2	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 XA = 6, what is Alice's public key YA?(6) ii) If Bob has a private key XB = 10, what is Bob's public key YB? (6) iii)Construct the shared secret key. (3)	BTL-6	Creating

3	i) In a public-key system using RSA, you intercept the cipher text C = 10 sent to a user whose public key is e = 5, n = 35. What is the plaintext M? (8) ii) In an RSA system, the public key of a given user is e =31, n = 3599. Determine the private key of this user? (7)	BTL-6	Creating
4	Discuss the ElGamal cryptosystem and elliptic curve cryptosystem. (15)	BTL-5	Evaluating
5	Explain the techniques for distribution of public keys and the exchange of public key certificates. (15)	BTL-5	Evaluating

UNIT IV - MESSAGE AUTHENTICATION AND INTEGRITY

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**	**BT Level**	**Competence**
1	State any three requirements for authentication.	BTL-1	Remembering
2	Point out the properties a digital signature.	BTL-4	Analyzing
3	What is the role of compression function in hash function?	BTL-1	Remembering
4	Define the term message digest.	BTL-1	Remembering
5	Define the classes of message authentication function.	BTL-1	Remembering
6	List the authentication message requirements.	BTL-1	Remembering
7	How is the security of a MAC function expressed?	BTL-2	Understanding
8	Identify the requirements for message authentication.	BTL-3	Applying
9	Give the two approaches of digital signature.	BTL-2	Understanding
10	Explain the significance of signature function in Digital SignatureStandard (DSS) approach.	BTL-2	Understanding
11	Identify the security services provided by digital	BTL-3	Applying
12	How digital signatures differ from authentication protocols?	BTL-2	Applying
13	How do you specify various types of authentication protocol?	BTL-1	Remembering
14	Explain the purpose of X.509 standard.	BTL-4	Analyzing
15	What is Kerberos? Point out its uses.	BTL-4	Analyzing
16	Identify 4 requirements defined by Kerberos.	BTL-3	Understanding
17	Summarize the Classes of message authentication function.	BTL-5	Evaluating
18	Assume a client C wants to communicate with a server S using Kerberosprotocol. Explain How can it be achieved?	BTL-5	Evaluating

19	Create a simple authentication dialogue used in Kerberos.	BTL-6	Creating
20	Design the role of Ticket Granting Server in inters realm operations ofKerberos.	BTL-6	Creating
21	State hash function.	BTL-4	Analyzing
22	Define bio metrics.	BTL-3	Understanding
23	Demonstrate the authentication applications.	BTL-2	Applying
24	What is DSS? Specify its requirements.	BTL-5	Evaluating
PART – B			
1	(i) Here hash functions are used? What characteristics are needed in secure hash function? (7) (ii) Write about the security of hash functions and MACs. (6)	BTL-1	Remembering
2	Discuss the classification of authentication function in detail. (13)	BTL-1	Remembering
3	Describe SHA 1 in detail with neat diagram. (13)	BTL-1	Remembering
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. (13)	BTL-1	Remembering
5	How Hash function algorithm is designed? Explain their features and properties. (13)	BTL-2	Understanding
6	(i)Explain in detail message authentication code and its requirements. (7) (ii) Illustrate the security of hash functions and MACs. (6)	BTL-2	Understanding
7	Describe Challenge-Response protocols in detail. (13)	BTL-2	Understanding
8	Explain the different approaches to message authentication. (13)	BTL-5	Evaluating
9	Illustrate the steps involved in Signature generation and Verification functions of DSS. (13)	BTL-3	Applying
10	Explain in detail about X.509 authentication services.(13)	BTL-4	Analyzing
11	Explain Client Server Mutual authentication with example flow diagram. (13)	BTL-4	Analyzing
12	What is Kerberos? Explain how it provides authenticated Services. (13)	BTL-4	Analyzing
13	Explain briefly about the architecture and certification mechanisms in Kerberos and X.509. (13)	BTL-3	Applying
14	Generalize the approaches for Digital signature. (13)	BTL-6	Creating

15	Define Kerberos. Explain their requirements and uses in detail. (13)	BTL-3	Applying
16	Describe about the class of message authentication function. (13)	BTL-2	Understanding
17	Briefly explain about the Authentication applications with suitable example. (13)	BTL-5	Evaluating

PART – C

1	With a neat diagram, explain the steps involved in SHA algorithm forencrypting a message with maximum length of less than 2^{128} bits and produces as output a 512-bit message digest. (15)	BTL-5	Evaluating
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. (15)	BTL-6	Creating
3	(i) Enumerate the properties of Hash Function. (8) (ii) Evaluate the authentication protocol and list its limitations. (7)	BTL-5	Evaluating
4	(i) Elaborate the way how the limitations of Kerberos version 4 is overcoming the environmental shortcomings and technical deficiencies. (8) (ii) Elaborate how the encryption is key generated from password in Kerberos. (7)	BTL-6	Creating
5	Explain the digital signature algorithm and evaluate the process of DSS signing and verification. (15)	BTL-5	Evaluating

UNIT V - SECURITY PRACTICE & SYSTEM SECURITY

Electronic Mail security – PGP, S/MIME – IP security – Web Security – SYSTEM SECURITY: Intruders – Malicious software – viruses – Firewalls.

PART – A

Q.No	Questions	BT	Competence
1	Define S/MIME.	BTL-1	Remembering
2	Expand and define SPI.	BTL-1	Remembering
3	Identify the steps involved in SET Transactions.	BTL-1	Remembering
4	Define SET? What are the features of SET?	BTL-1	Remembering
5	Identify the five header fields defined in MIME.	BTL-1	Remembering
6	How can the signed data entity of S/MIME be prepared? Give the steps.	BTL-2	Understanding
7	Differentiate transport and tunnel mode in IPsec.	BTL-2	Understanding
8	Point out the services provided by PGP?	BTL-5	Evaluating
9	Explain the protocols used to provide IP security.	BTL-2	Understanding
10	What is a virus in a computer? Classify the types of viruses.	BTL-3	Applying

11	Classify the various types of firewall and its design goal?	BTL-2	Understanding
12	Identify the three classes of Intruders.	BTL-3	Applying
13	What is a Threat? List their types.	BTL-4	Analyzing
14	State the difference between threats and attacks.	BTL-4	Analyzing
15	Differentiate spyware and virus.	BTL-4	Analyzing
16	Give the advantages of intrusion detection system over firewall.	BTL-2	Understanding
17	Show the design goals of firewalls.	BTL-6	Evaluating
18	Discriminate statistical anomaly detection and rule based detection	BTL-5	Creating
19	Does the firewall ensure 100% security to the system? Comment.	BTL-6	Creating
20	Illustrate the types of threads.	BTL-3	Applying
21	Define IP security.	BTL-1	Remembering
22	Identify the similarities between the IP security and Web security.	BTL-4	Analyzing
23	Argue the importance of firewall.	BTL-6	Evaluating
24	What is electronic mail security?	BTL-3	Applying
PART-B			
1	Describe the working of SET with neat diagram. (13)	BTL-1	Remembering
2	Describe in detail about SSL/TLS. (13)	BTL-1	Remembering
3	Explain the architecture of IPsec in detail in detail with a neat block diagram. (13)	BTL-2	Understanding
4	Describe in detail about S/MIME. (13)	BTL-1	Remembering
5	Discuss authentication header and ESP in detail with their packet format. (13)	BTL-2	Understanding
6	Describe PGP cryptographic functions in detail with suitable block diagrams. (13)	BTL-1	Remembering
7	(i) Discuss transport mode and tunnel mode authentication in IP? (10) (ii)Describe how ESP is applied to both these modes. (3)	BTL-2	Understanding
8	Explain the operational description of PGP. (13)	BTL-4	Analyzing

9	Illustrate the working principle of SET and relate EST for Ecommerce applications. (13)	BTL-3	Applying
10	Explain how firewalls help in the establishing a security framework for an organization.. (13)	BTL-4	Analyzing
11	Generalize the role of intrusion detection system and give the comparison of statistical anomaly detection and rule based intrusion detection system? (13)	BTL-6	Creating
12	Interpret the different types of virus in detail. Suggest scenarios for deploying these types in network. (13)	BTL-3	Applying
13	Explain intrusion detection system (IDS) in detail with suitable diagrams. (13)	BTL-5	Evaluating
14	Illustrate the various types of firewalls with neat diagrams. (13)	BTL-3	Applying
15	Briefly explain about Electronic Email Security in detail. (13)	BTL-4	Analyzing
16	Describe in detail about five header fields defined in MIME. (13)	BTL-2	Understanding
17	Draw the IP security authentication header and describe the functions of each field. (13)	BTL-5	Evaluating
PART-C			
1	Evaluate the performance of PGP. Compare it with S/MIME. (15)	BTL-5	Creating
2	(i) Write the steps involved in the simplified form of the SSL / TLS protocol (8) (ii) Generalize the methodology involved in computing the keys in SSL / TLS protocol. (7)	BTL-6	Creating
3	(i) Explain the various measures that may be used for intrusion detection. (8) (ii) Explain the various roles of firewalls and related terminology in detail. (7)	BTL-5	Evaluating
4	Elaborate how secure electronic transaction (SET) protocol enables e- transactions. Explain the components involved. (15)	BTL-6	Evaluating
5	Briefly explain the concept about malicious software and virus in detail. (15)	BTL-6	Creating