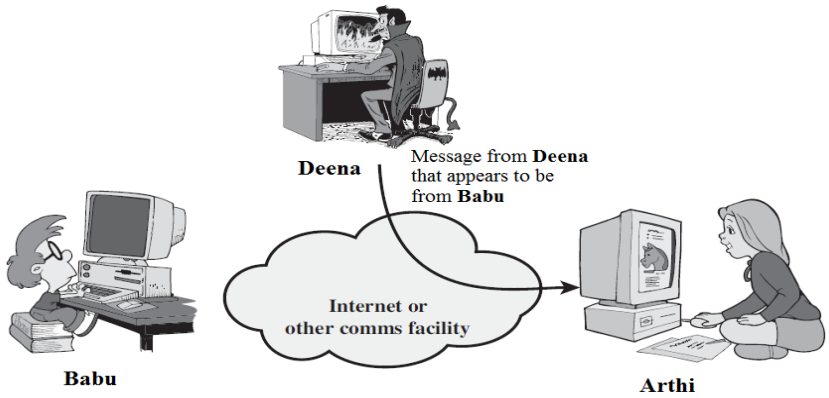
1702CS701 Cryptography and Network Security

Academic Year:	2021-2022	**Question Bank**	Programme:	B.E CSE
Year / Semester:	IV/VII		Course Coordinator:	Mr.G.Arul Selvan

Course Objectives	Course Outcomes:
1. To know the principles and methods of conventional and advanced encryption algorithms. 2. To learn the techniques used for message authentication and confidentiality maintenance 3. To understand the network security tools and applications.	On completion of the course, students will be able to CO1:Explain the fundamental principles of cryptographic techniques CO2:Analyze the cryptographic algorithms for symmetric ciphers. CO3: Evaluate asymmetric key algorithms and acquire knowledge in key management. CO4: Explain cryptographic data integrity algorithms. CO5: Identify the issues and protocols in network security.

PART – A (2 Mark Questions With Key)

S.No	Questions	Mark	COs	BTL
	UNIT I – INTRODUCTION			
1	**What does the OSI security architecture provide?**		1	K1
	The OSI security architecture focuses on security attacks, mechanisms, and services.	2		
2	**Define Security attack, Security mechanism, and Security service.** • **Security attack:** Any action that compromises the security of information owned by an organization. • **Security mechanism:** A process that is designed to detect, prevent, or recover from a security attack. • **Security service:** A communication service that enhances the security of the data processing systems and the information transfers of an organization. • The services are intended to counter security attacks, and they make use of one or more security mechanisms to provide the service.	2	1	K1
3	**Define a threat.**		1	K1
	A **potential for violation of security**, which exists when there is a circumstance, capability, action, or ***event that could breach security and cause harm***. That is, a threat is a ***possible danger that might exploit vulnerability.***	2		
4	**Define an attack.**		1	K1
	An ***assault on system security that derives from an intelligent threat***; that is, an intelligent act that is a deliberate attempt ***to evade security services and violate the security policy*** of a system.	2		
5	**Distinguish between active attack and passive attack.**		1	K1
	• **Active Attacks:** Active attacks ***involve some modification of the data stream*** or the creation of a false stream. It can be subdivided into four categories. (i) Masquerade, (ii) Replay, (iii) Modification of messages, (iv) Denial of Service (DoS)	2		

	• **Passive Attacks:** Passive ***attacks are in the nature of eavesdropping on, or monitoring of transmissions.*** The goal of the opponent is to obtain information that is being transmitted. Two types of passive attacks are, (i) Release of message contents (ii) Traffic Analysis			
6	**What do you mean by traffic analysis attack?**		1	K1
	▪ Observe the pattern of these messages. ▪ The opponent could determine the location and identity of communicating hosts and could observe the frequency and length of messages being exchanged. ▪ This information might be useful in guessing the nature of the communication that was taking place.	2		
7	**What is a masquerade attack?**			
	• A **masquerade** takes place when ***one entity pretends to be a different entity***. A masquerade attack usually includes one of the other forms of active attack. • For example, authentication sequences can be captured and replayed after a valid authentication sequence has taken place, thus enabling an authorized entity with few privileges to obtain extra privileges by ***impersonating an entity*** that has those privileges.  	2	1	K1
8	**What is denial of service (DoS) attack?**		1	K1
	▪ The **denial of service (DoS)** attack ***prevents or inhibits the normal use or management of communications facilities.*** This attack may have a specific target; for example, an entity may suppress all messages directed to a particular destination (e.g., the security audit service). ▪ Another form of service denial is the ***disruption of an entire network***, either by ***disabling the network or by overloading it with messages*** so as to degrade performance.	2		
9	**What do you mean by nonrepudiation?**		1	K1
	Nonrepudiation prevents ***either sender or receiver from denying a transmitted message***. Thus, when a message is sent, ***the receiver can prove that the alleged sender in fact sent the message.*** Similarly, when a message is received, ***the sender can prove that the alleged receiver in fact received the message.***	2		
10	**Define Substitution. What are the different substitution techniques involved in classic encryption technique?**		1	K1

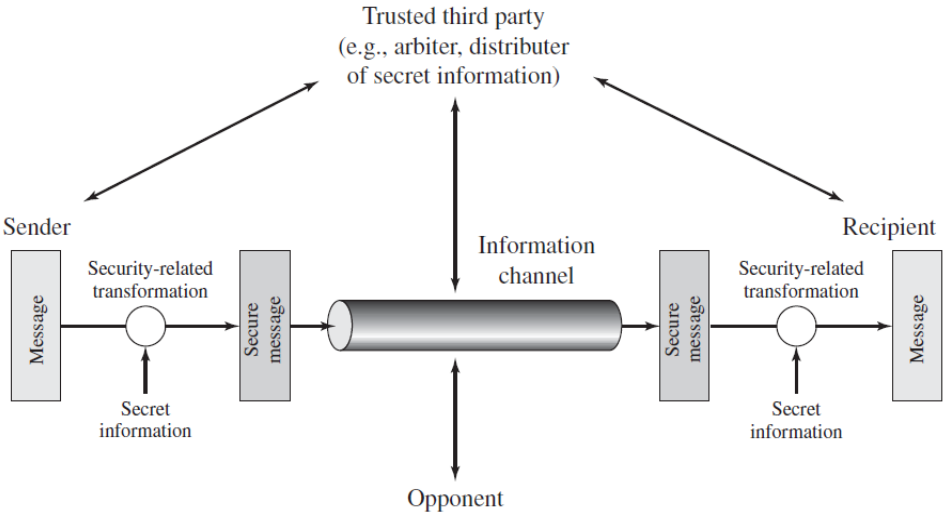
	A substitution technique is one in which the letters of plaintext are replaced by other letters or by numbers or symbols. If the plaintext is viewed as a sequence of bits, then substitution involves replacing plaintext bit patterns with ciphertext bit patterns. **Types:** Caeser Cipher, Mono alphabetic cipher, Playfair cipher, Hill cipher, poly alphabetic cipher, Vigenere cipher,	2		
11	**What is an encipherment?**		1	K1
	The use of mathematical algorithms to ***transform data into a form that is not readily intelligible***. The transformation and subsequent recovery of the data depend on an algorithm and zero or more encryption keys.	2		
12	**Define the Caesar cipher**		1	K1
	The Caesar cipher involves replacing each letter of the alphabet with the letter standing three places down the alphabet .The alphabet is wrapped around, so that the letter following Z is A. **C = E (p) = (p + 3) mod (26)** The general Caesar cipher algorithm is **C = E (p) = (p + k) mod (26)** Where k takes the value in the range 1 to 25 The decryption algorithm is **p = D(C) = (C - k) mod (26)**	2		
13	**Write Euclid's algorithm for computing GCD.**		1	K1
	Euclid(a, b) while b != 0 r ← a mod b a ← b b ← r end while return a	2		
14	**Find the GCD of 2740 and 1760, using Euclidean algorithm.**		1	K1
	The GCD of two numbers say *a* and *b* can be found using the following formula ***gcd(a,b) =gcd(b,a mod b)*** GCD(2740,1760) = gcd(1760, 2740 mod 1760)= gcd(1760,980)=980	2		
15	**What is the difference between a monoalphabet cipher and a polyalphabetic cipher?**		1	K1
	• Monoalphabetic cipher is a monoalphabetic cipher is a substitution cipher in which the cipher alphabet is fixed through the encryption process. All of the substitution ciphers we have seen prior to this hand-out are monoalphabetic; these ciphers are highly susceptible to frequency analysis. • Polyalphabetic Cipher is a polyalphabetic cipher is a substitution cipher in which the cipher alphabet changes during the encryption process.	2		
16	**Differentiate conventional (symmetric) from public key (asymmetric) encryption.**		2	K1

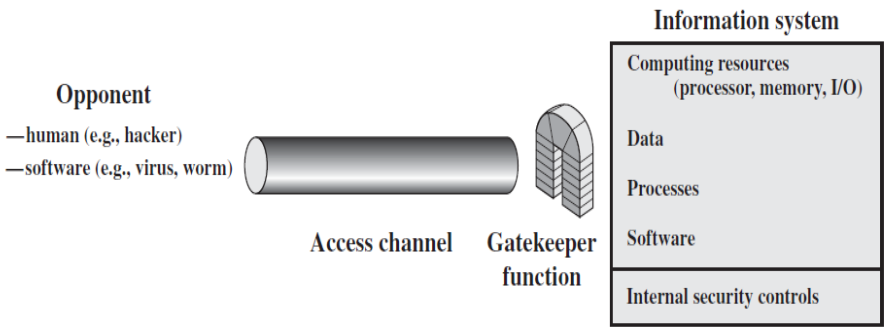
	<table><tr><th>Conventional Encryption</th><th>Public-Key Encryption</th></tr><tr><td>Needed to Work: 1. The same algorithm with the same key is used for encryption and decryption. 2. The sender and receiver must share the algorithm and the key.</td><td>Needed to work: 1. One algorithm is used for encryption and decryption with a pair of keys, one for encryption and one for decryption. 2. The sender and receiver must each have one of the matched pair of keys (not of the same one).</td></tr><tr><td>Needed for Security: 1. The key must be kept secret. 2. It must be impossible or atleast impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus samples of ciphertext must be insufficient to determine the key.</td><td>Needed for security: 1. One of the two keys must be kept secret. 2. It must be impossible or at least impractical to decipher a message if no other information is available. 3. Knowledge of the algorithm plus one of the keys plus samples of the ciphertext must be insufficient to determine the other key.</td></tr></table>	2		
17	**What is Brute-force attack?**		2	K1
	The attacker tries every possible key on a piece of cipher text until an intelligible translation into plain text is obtained. On average, half of possible keys must be tried to achieve success. It is a trial and error method used by application programs to decode encrypted data or keys through exhaustive effort rather than employing intellectual strategies.	2		
18	**What is a transposition cipher?**		2	K1
	Transposition cipher is a cipher, which is achieved by performing some sort of permutation on the plaintext letters. Eg: Rail fence Technique In this technique plaintext is written down as a sequence of diagonals and then read off as a sequence of rows.	2		

PART – B (12 Mark Questions with Key)

S.No	Questions	Mark	COs	BTL
1	**Explain in detail the different categories of attacks on crypto systems.**	12	1	K2
	Definition of Security attack. **Passive attacks** - in the nature of eavesdropping on, or monitoring of, transmissions. **(i) Release of message contents** - learning the contents of transmissions. **(ii)Traffic analysis** – extract information from the message by observing the pattern. **Active attacks** - involve some modification of the data stream or the creation of a false stream. **a) Masquerade - one entity pretends to be a different entity.** **b) Replay** -the passive capture of a data unit and its subsequent retransmission to			

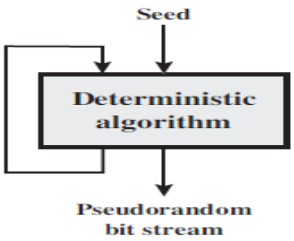
	produce an unauthorized effect. **c) Modification of messages - simply means that some portion of a legitimate message is altered or those messages are delayed or reordered.** **d)** The **denial of service** prevents or inhibits the normal use or management of communications facilities. (Explain each type with illustration)			
2	**List and explain security services with reference to the ITU-T recommendation X.800.**	12	1	K2
	AUTHENTICATION - Peer Entity Authentication - Data-Origin Authentication **ACCESS CONTROL** **DATA CONFIDENTIALITY** - Connection Confidentiality - Connectionless Confidentiality - Selective-Field Confidentiality - Traffic-Flow Confidentiality **DATA INTEGRITY** - Connection Integrity with Recovery - Connection Integrity without Recovery - Selective-Field Connection Integrity - Connectionless Integrity - Selective-Field Connectionless Integrity **NONREPUDIATION** - Nonrepudiation, Origin - Nonrepudiation, Destination (Explain each title and subtitle)			
3	**List and explain different security mechanisms with reference to the ITU-T recommendation X.800.**	12	1	K2
	SPECIFIC SECURITY MECHANISMS - appropriate protocol layer in order to provide some of the OSI security services. - Encipherment - Digital Signature - Access Control - Data Integrity - Authentication Exchange - Traffic Padding - Routing Control - Notarization			

	PERVASIVE SECURITY MECHANISMS - not specific to any particular OSI security service or protocol layer. - Trusted Functionality - Security Label - Event Detection - Security Audit Trail - Security Recovery (Explain each title and subtitle)			
4	**Explain the network security and network access model in detail with a neat diagram.**	12	1	K2
	Model for Network Security: Two components: • A security-related transformation scrambles the message – encryption – digital signature • Some secret information - an encryption key  **A trusted third party** - responsible for distributing the secret information - keeping it from any opponent. (arbitrate disputes between the two principals the sender and receiver) **Four tasks:** 1) Design an algorithm for encryption and decryption. 2) Generate the secret information - the key. 3) Develop methods for the distribution and sharing of the secret information. 4) Specify a protocol to be used by the two principals - to achieve a particular security service. **Network Access Security Model** **The hacker** - breaking and entering a computer system - penetrate systems – accessed through networks			

	The intruder - a disgruntled employee who wishes to do damage - a criminal who seeks to exploit computer assets for financial gain.  **Threat** - Potential for security violation - Breach (violate) security and cause harm. - **Information access threats:** Intercept or modify data. **Service threats:** Exploit service flaws (weakness / faults)			
5	**(i) Explain in detail about playfair cipher.** **(ii) Using Playfair Cipher with** Key= occurrence **, Encrypt the following :** "MUST SEE YOU OVER CADAGEN WEST. COMING AT ONCE".	12	1	K2
6.		12	1	K2
PART – C (20 Mark Questions with Key)				
1	**Explain in detail about OSI security architecture.** The OSI security architecture focuses on • security attacks, • mechanisms, and • Services.	20	1	K2
2	**1. (i).Explain in detail about Hill cipher.** **(ii) Encrypt & Decrypt the message "PAY" using hill cipher with the following key matrix and show the decryption to get original plain text.** $K = \begin{matrix} 17 & 17 & 5 \\ 21 & 18 & 21 \\ 2 & 2 & 19 \end{matrix}$	20	1	K2

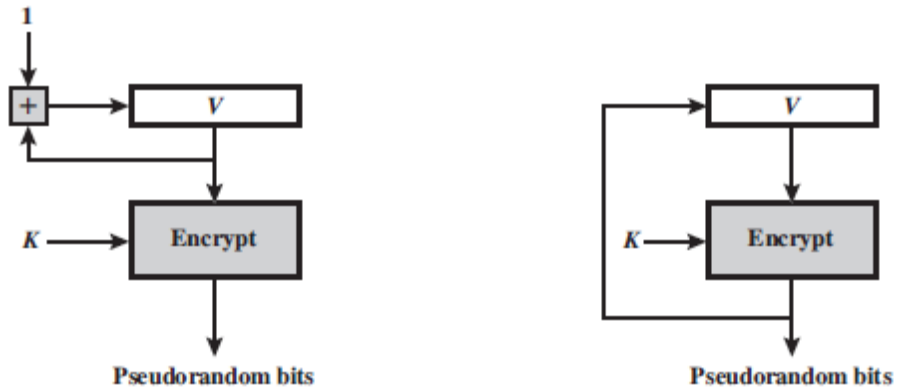
PART – A (2 Mark Questions With Key)				
S.No	**Questions**	**Mark**	**COs**	**BTL**
UNIT II – SYMMETRIC CIPHERS				
1	**What do you mean by symmetric key cryptography?** ▪ Symmetric encryption is a form of cryptosystem in which ***encryption and decryption are performed using the same key***. It is also known as conventional encryption. ▪ Symmetric encryption transforms plaintext into ciphertext using a secret key and	2	2	K1

	an encryption algorithm. Using the same key and a decryption algorithm, the plaintext is recovered from the ciphertext.			
2	**Define stream cipher and block cipher**.	2	2	K1
	A stream cipher is one that encrypts a digital data stream one bit or one byte at a time. Eg: Caeser cipher A block cipher is one in which a block of plaintext is treated as a whole and used to produce a cipher text block of equal block. a block size of 64 or 128 bits is used. Eg: DES.			
3	Define Substitution and Permutation		2	K1
	Substitution: Each plaintext element or group of elements is uniquely replaced by a corresponding ciphertext element or group of elements. **Permutation:** A sequence of plaintext elements is replaced by a permutation of that sequence. That is, no elements are added or deleted or replaced in the sequence, rather the order in which the elements appear in the sequence is changed.	2		
4	**What is differential cryptanalysis?**	2	2	K2
	Differential cryptanalysis is a technique in which chosen plaintexts with particular XOR difference patterns are encrypted. The difference patterns of the resulting ciphertext provide information that can be used to determine the encryption key.			
5	**What is linear cryptanalysis?**	2	2	K1
	This attack is based on finding linear approximations to describe the transformations performed in DES. This method can find a DES key given 243 known plaintexts, as compared to 2^{47} chosen plaintexts for differential cryptanalysis. Although this is a minor improvement, because it may be easier to acquire known plaintext rather than chosen plaintext, it still leaves linear cryptanalysis infeasible as an attack on DES. So far, little work has been done by other groups to validate the linear cryptanalytic approach.			
6	Write about Mix Columns.		2	K1
	• Mix Column is substitution that makes use of arithmetic over GF (2^8). Mix Column Operates on each column individually. • Each byte of a column is mapped into a new value that is a function of all four bytes in the column. • The Mix Column Transformation combined with the shift row transformation ensures that after a few rounds, all output bits depend on all input bits.	2		
7	**What is the avalanche effect?**			
	In cryptography, the avalanche effect refers to a desirable property of cryptographic algorithms, typically block ciphers and cryptographic hash functions. The avalanche effect is evident if, when an input is changed slightly (for example, flipping a single bit) the output changes significantly (e.g., half the output bits flip). In the case of high-quality block ciphers, such a small change in either the key or the plaintext should cause a drastic change in the ciphertext.	2	2	K1
8	**What is the difference between Sub Bytes and Sub Word?**		2	K1
	Sub Bytes: Sub Bytes uses an S-box to perform a byte-by-byte substitution of the block. Sub Word: Sub Word performs a byte substitution on each byte of its input word, using the Sbox.	2		
9	**List the strength of DES**		2	K1
	• The use of 56 bit keys.	2		

	• Nature of the DES algorithm. • Timing attack			
10	**What is the purpose of the State array?**		2	K1
	The input to the encryption and decryption algorithms is a single 128-bit block. A single 128-bit block is depicted as a square matrix of bytes. This block is copied into the State array, which is modified at each stage of encryption or decryption. After the final stage, State is copied to an output matrix.	2		
11	**Write about Add Round Key.**		2	K1
	• In Add Round Key, the 128 bits of State are bit wise XOR with the 128 bits of the round key. • The operation is viewed as a column wise operation between the 4 bytes of a State • Column and one word of the round key; it can also be viewed as a byte-level operation. • The Add Round Key transformation is as simple as possible and affects every bit of State.	2		
12	**Describe about the Key Expansion Algorithm**		2	K1
	• The AES key expansion algorithm takes as input a 4-word (16-byte) key and produces linear array of 44 words (156 bytes). • This is sufficient to provide a 4-word round key for the initial Add Round Key stage and each of the 10 rounds of the cipher.	2		
13	**What is the difference between Shift Rows and Rot Word?**		2	K1
	Shift Rows: Shift Row is simple permutation. It shifts the rows circularly left or right. Rot Word: Rot word performs a one-byte circular left shift on a word. This means that an input word [b0, b1, b2, b3] is transformed into [b1, b2, b3, b0].	2		
14	**What is Pseudorandom number generator?**		2	K1
	An algorithm that is used to produce an open-ended sequence of bits is referred to as a PRNG.A common application for an open-ended sequence of bits is as input to a symmetric stream cipher.  	2		
15	**List the two types of algorithms for PRNGs.**		2	K1
	• Linear Congruential Generators • Blum Blum Shub Generator	2		

PART – B (12 Mark Questions with Key)

S.No	Questions	Mark	COs	BTL
1	**Explain in detail about Feistel structure with neat sketch**	12	2	K2
2	**Explain about block cipher design principles.**	12	2	K1

	Design criteria about • S boxes. • Permutations. • Number of rounds.			
3	**Explain about differential cryptanalysis and l jinear cryptanalysis**	12	2	K2
4	**Explain about Pseudorandom number generator using** **a) Linear Congruential Generators** **b) Blum Blum Shub Generator**	12	2	K2
5	**Explain about Pseudorandom number generator using block cipher modes of operations.**	12	2	K2
	Two approaches that use a block cipher to build a PNRG have gained widespread acceptance: • the CTR mode and • the OFB mode  (a) CTR mode (b) OFB mode Figure 7.3 PRNG Mechanisms Based on Block Ciphers			
6.	With an algorithm explain about RC5	12	2	K2
	PART – C (20 Mark Questions with Key)			
1	**Show the entire encryption and decryption process of block of messages using data encryption standard.**	20	2	K2
	DES Encryption ✓ General depiction of DES Encryption Algorithm (Figure) ✓ Initial Permutation ✓ Single Round of DES Algorithm (Figure) ✓ Calculation of F(R, K) ✓ Key Generation **DES Decryption**			
2	**Explain AES algorithm with all its round functions in detail**	20	2	K2

PART – A (2 Mark Questions With Key)				
S.No	**Questions**	**Mark**	**COs**	**BTL**

UNIT III –A SYMMETRIC CIPHERS & KEY MANAGEMENT

1	**What is an asymmetric or public key encryption?** ➢ Asymmetric algorithms rely on **two keys, o**ne key for **encryption** and a ***different but related key for decryption.*** ➢ These algorithms have the following important characteristic. (i) It is computationally infeasible to determine the decryption key given only knowledge of the cryptographic algorithm and the encryption key. (ii)Either of the two related keys can be used for encryption, with the other used for decryption.	2	3	K1
2	**Define Fermat's Theorem** Fermat's theorem states the following: If is prime and is a positive integer not divisible by , then $a^{p-1} \equiv 1 \pmod{p}$ An alternative form of Fermat's theorem is also useful: If is prime and is a positive integer, then $a^p = a \pmod{p}$	2	3	K1
3	**Define relatively prime.** The two numbers are relatively prime if they have no prime factors in common; that is, their only common divisor is 1.This is equivalent to saying that two numbers are relatively prime if their greatest common divisor is 1.	2	3	K1
4	**What is Euler's totient function?** Euler's totient function, written **Φ** (n) , and defined as the number of positive integers less than and relatively prime to . By convention, **Φ** (1) = 1.	2	3	K1
5	**Determine Φ(37) and Φ(35)** • Because 37 is prime, all of the positive integers from 1 through 36 are relatively prime to 37.Thus **Φ(37)=36** • To determine **Φ(35)** , we list all of the positive integers less than 35 that are relatively prime to it: There are 24 numbers on the list, so f(35) = 24. 1, 2, 3, 4, 6, 8, 9, 11, 12, 13, 16, 17, 18, 19, 22, 23, 24, 26, 27, 29, 31, 32, 33, 34 **Φ(35)** =24	2	3	K1
6	**Define Euler's Theorem** Euler's theorem states that for every and that are relatively prime: $a^{\phi(n)} \equiv 1 \pmod{n}$	2	3	K1
7	**Define Discrete Logarithm.** • For any integer $\boldsymbol{y}$, primitive root $\boldsymbol{g}$ of a prime number p, we can find a unique exponent $\boldsymbol{x}$ such that, $\boldsymbol{y} = \boldsymbol{g^x} (\mathbf{mod}) \mathbf{p}$, Where $\mathbf{0} \leq \boldsymbol{x} \leq (\boldsymbol{p} - \mathbf{1})$. • This exponent $\boldsymbol{x}$ is referred to as the discrete logarithm of the number $\boldsymbol{y}$ for the base $\boldsymbol{g}(\boldsymbol{mod})\boldsymbol{p}$. • It is denoted by $\boldsymbol{dlog}_{\boldsymbol{g,p}}(\boldsymbol{y})$.	2	3	K1
8	**Define Chinese Remainder Theorem** the CRT says it is possible to reconstruct integers in a certain range from their residues modulo a set of pairwise relatively prime moduli.	2	3	K1

9	**In a public key system using RSA, you intercept the cipher text C=11 sent to a user whose public key is d=5, n=21, What is the plain text M?**	2	3	K1
	$\boldsymbol{M} = C^d \bmod n$ $= 11^5 \bmod 21$ $= 161051 \bmod 21$ $\boldsymbol{M = 2}$			
10	**In a public key system using RSA, the value of e is chosen as 5, and $\Phi(n) = 12$. Compute the value of private key component d.**	2	3	K1
	• In RSA crypto system, the values e and d are multiplicative inverse mod $\Phi(n)$. • Therefore, $\boldsymbol{e \times d \bmod \Phi(n) = 1}$ • Check for different values of $\boldsymbol{d}$ in this equation. The number which satisfies this e $\boldsymbol{5 \times d \bmod 12 = 1}$ (Or) Use extended Euclidean algorithm.			
11	**What is a primitive root of a number?**	2	3	K1
	For a prime number **p**, if **a** is a primitive root of **p**, then **a, a^2, a^3,…., a^{p-1}** are distinct $(\boldsymbol{mod\ p})$. We can define a primitive root of a number p as one whose powers generate all the integers from 1 to p-1. That is p, if a is a primitive root of the prime number p then the number			
12	**Given $q = 71, \alpha = 17,\ X_A = 5$, compute A's public key for Diffie-Hellman key exchange.**	2	3	K1
	$Y_A = \alpha^{X_A} (\text{mod}) q$ $Y_A = \alpha^{X_A} (\text{mod}) q$ $Y_A = 17^5 (\text{mod}) 71$ $Y_A = 1419857 (\text{mod}) 71$ $Y_A = \mathbf{70}$			
13	**What is the meaning of the expression a divides b?**	2	3	K1
	Integer a is said to be a divisor of integer b if there is no remainder on division			
14	**What are the various possible attacks on RSA?**	2	3	K1
	• **Brute force:** This involves trying all possible private keys. • **Mathematical attacks:** There are several approaches, all equivalent in effort to factoring the product of two primes. • **Timing attacks:** These depend on the running time of the decryption algorithm. • **Chosen ciphertext attacks:** This type of attack exploits properties of the RSA algorithm.			
15	**What do you understand by public key infrastructure (PKI)?**		2	K1
	A set of policies, processes, server platforms, software and workstations used for the	2		

Primitive roots of 5

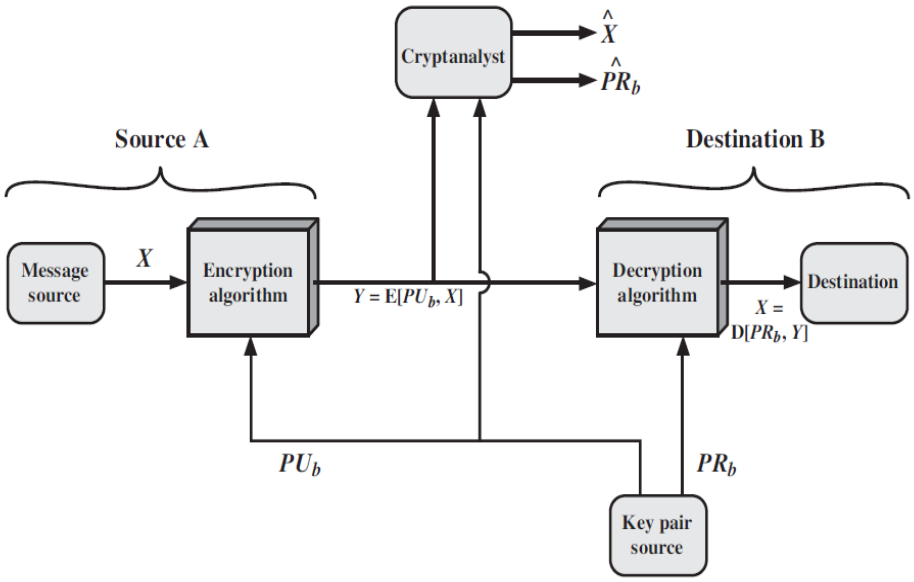
a^p mod 5

a	a^1	a^2	a^3	a^4	Remarks
1	1	1	1	1	
2	2	4	3	1	(Powers of **a**) mod **n** are distinct, 2 is a primitive root.
3	3	4	2	1	(Powers of **a**) mod **n** are distinct, 3 is a primitive root.
4	4	1	4	1	

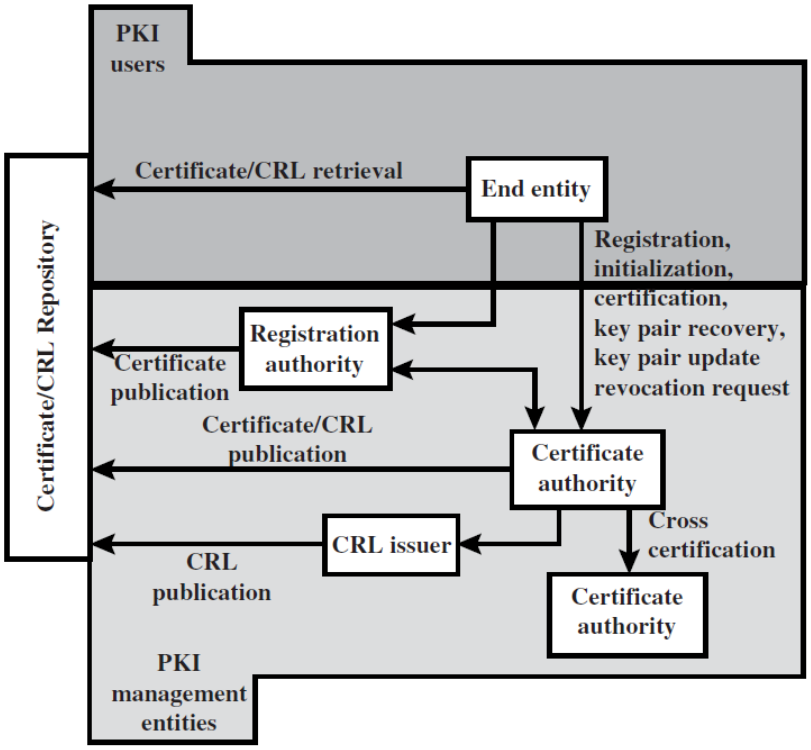
	purpose of administering certificates and public-private key pairs, including the ability to issue, maintain, and revoke public key certificates.			
16	**What is a one-way function?**	2	3	
	A one-way function is one that maps a domain into a range such that every function value has a unique inverse, with the condition that the calculation of the function is easy, whereas the calculation of the inverse is infeasible: $Y = f(X)$ easy $X = f^{-1}(Y)$ infeasible			
17	**What is trap-door one-way function?**	2	3	K1
	a trap-door one-way function, which is easy to calculate in one direction and infeasible to calculate in the other direction unless certain additional information is known. A trapdoor one-way function is a family of invertible functions f_k, such that $Y = f_k(X)$ easy, if k and X are known $X = f_k^{-1}(Y)$ easy, if k and Y are known $X = f_k^{-1}(Y)$ infeasible, if Y is known but k is not known			
18	**List the procedure for picking a prime number**	2	3	K1
	1. Pick an odd integer n at random (e.g., using a pseudorandom number generator). **2.** Pick an integer $a < n$ at random. **3.** Perform the probabilistic primality test, such as Miller-Rabin, with a as a parameter. If n fails the test, reject the value n and go to step 1. **4.** If n has passed a sufficient number of tests, accept n; otherwise, go to step 2.			
19	**What is Diffie Hellman key exchange**	2	3	K1
	A simple public-key algorithm is Diffie-Hellman key exchange. This protocol enables two users to establish a secret key using a public-key scheme based on discrete logarithms. The protocol is secure only if the authenticity of the two participants can be established.			
20	**List the various techniques for distribution of public keys**	2	3	K1
	• Public announcement • Publicly available directory • Public-key authority • Public-key certificates			
21	**What is the purpose of the X.509 standard?**	2	3	K1
	X.509 defines a framework for the provision of authentication services by the X.500 directory to its users. The directory may serve as a repository of public-key Certificates. Each certificate contains the public key of a user and is signed with the private key of a trusted certification authority			
22	**How is an X.509 certificate revoked?**	2	3	K1
	It may be desirable on occasion to revoke a certificate before it expires, for one of the following reasons. 1. The user's private key is assumed to be compromised. 2. The user is no longer certified by this CA. Reasons for this include that the subject's name has changed, the certificate is superseded, or the certificate was not issued in conformance with the CA's policies. 3. The CA's certificate is assumed to be compromised.			

PART – B (12 Mark Questions with Key)

S.No	Questions	Mark	COs	BTL
1	**Explain the public key cryptosystem in detail. Enumerate the requirements for public-key cryptography.**	12	3	K2

	 **Requirements for public-key cryptography.** **1.** It is computationally easy for a party B to generate a pair (public key PU_b, private key PR_b). **2.** It is computationally easy for a sender A, knowing the public key and the message to be encrypted, M, to generate the corresponding ciphertext: $C = E(PU_b,M)$ **3.** It is computationally easy for the receiver B to decrypt the resulting ciphertext using the private key to recover the original message:$M = D(PR_b, C) = D[PR_b, E(PU_b,M)]$ **4.** It is computationally infeasible for an adversary, knowing the public key, PU_b, to determine the private key, PR_b. **5.** It is computationally infeasible for an adversary, knowing the public key, PU_b, and a ciphertext, C, to recover the original message, M. We can add a sixth requirement that, although useful, is not necessary for all public-key applications: **6.** The two keys can be applied in either order: $M = D [PU_b, E(PR_b,M)] = D[PR_b, E(PU_b,M)]$			
2	**(i) State and Explain Miller-Robin algorithm and** **(ii) Test whether 19 is a prime number or not.**	4 8	3	K1
3	**(i) State and Explain Chinese Remainder Theorem** **(ii) find X for the given set of congruent equations using CRT** **X≡ 2(mod 3)** **X≡3(mod5)** **X≡2(mod7)**	5 7	3	K2

4	**(i) Discuss how Diffie-Hellman key exchange algorithm enable two users to securely exchange a key that can then be used for subsequent encryption of messages.** **(ii)Consider Diffie-Hellman scheme with a common prime $q = 11$ and $\alpha = 2$. Users A and B have private keys $X_A = 9$; $X_B = 3$; respectively. Find the value of Y_A, Y_B and K. Verify that the shared secret key is rightly available for A and B.**	6 6	3	K3
	• Global Public Elements • User A Key Generation • User B Key Generation • Calculation of Secret Key by User A • Calculation of Secret Key by User B • Answer: $Y_A = 6$; $X_B = 8$; $K = 3$			
5	**Explain the Key management in detail**	12	3	K2
	One of the major roles of public-key encryption has been to address the problem of key distribution. There are actually two distinct aspects to the use of public-key cryptography in this regard: ● The distribution of public keys ● The use of public-key encryption to distribute secret keys **Distribution of Public Keys** Several techniques have been proposed for the distribution of public keys. Virtually all these proposals can be grouped into the following general schemes: ● Public announcement ● Publicly available directory ● Public-key authority ● Public-key certificates			
6.	**Explain the public key infrastructure with a neat sketch.**	12	3	K2
	Definition public-key infrastructure. **Key elements of the PKIX model.** • End entity • Certification authority (CA) • Registration authority (RA) • CRL issuer • Repository			



PKIX Management Functions

- Registration:
- Initialization
- Certification
- Key pair recovery
- Key pair update
- Revocation request
- Cross certification

PKIX Management Protocols

PART – C (20 Mark Questions with Key)

1	**(i) Describe the mathematical foundation of RSA algorithm.** **(ii) Write the algorithm for RSA.** **(iii) Perform encryption and decryption using RSA algorithm for the following values.** **(i)** $p = 7, q = 11, e = 17;\ M = 8$ **(or)** **(ii)** $p = 17, q = 11, e = 7;\ M = 88$ **(or)** **(iii)** $p = 3, q = 11, e = 7;\ M = 5$ **(solve any one problem)**	5 5 10	3	K3
	Answer: **(i)** $n = 77;\ \Phi(n) = 60;\ d = 53;\ C = 57$ **(ii)** $n = 187;\ \Phi(n) = 160;\ d = 23;\ C = 11$ **(iii)** $n = 33;\ \Phi(n) = 20;\ d = 3;\ C = 14$			

2	**(i)What is the purpose of the X.509 standard?** **(ii) How is an X.509 certificate revoked?** **(iii) Write about X.509 authentication service?**	20	3	K2

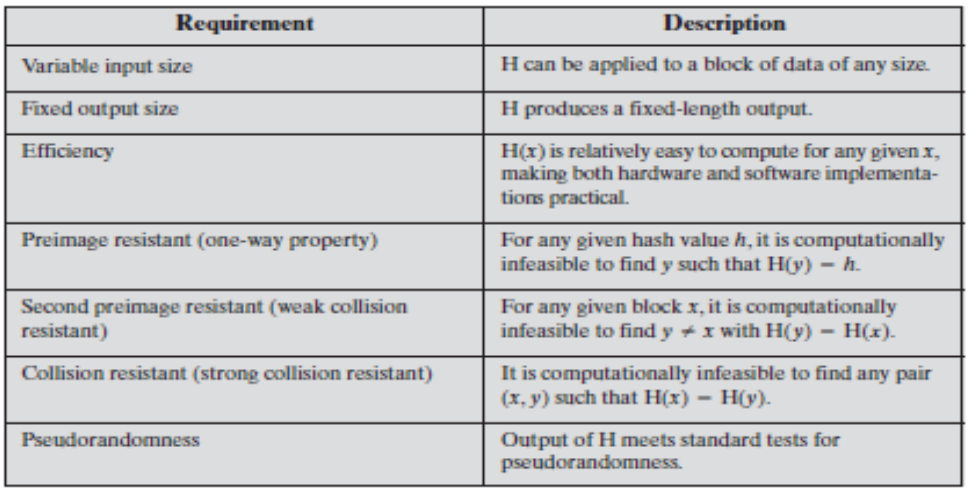
PART – A (2 Mark Questions With Key)				
S.No	**Questions**	**Mark**	**COs**	**BTL**
	UNIT IV-CRYPTOGRAPHIC DATA INTEGRATY ALGORITHMS			
1	**Define a cryptographic hash function.** A hash function H accepts a variable-length block of data as input and produces a fixed-size hash value h = H(M).	2	4	K1
2	**What are the properties of a good hash function?** • A "good" hash function has the property that the results of applying the function to a large set of inputs will produce outputs that are evenly distributed and apparently random. • The principal object of a hash function is data integrity. • A change to any bit or bits in results, with high probability, in a change to the hash code	2	4	K1
3	**List the applications of cryptographic hash function.** ➢ **Message authentication** – here hash function value is often referred to as a **message digest**. Message authentication is achieved using a **message authentication code (MAC)**, also known as a **keyed hash function.** ➢ **Digital signatures.** ➢ Used to create a **one-way password file**. ➢ Can be used for ***intrusion detection*** and ***virus detection.*** ➢ Used to construct a **pseudorandom function** (PRF) or a **pseudorandom number generator (PRNG).** ➢ A common application for a hash-based PRF is for the **generation of symmetric keys**	2	4	K1
4	**What is a message authentication code (MAC)?** • A MAC takes a variable-length message and a secret key as input and produces an authentication code. • A recipient in possession of the secret key can generate an authentication code ***to verify the integrity of the message***.	2	4	K1
5	**Define one way property, weak collision resistance and strong collision resistance of hash function.** For any given value h, it is computationally infeasible to find x such that H(x) = h - one way property. For any given block x, it is computationally infeasible to find y ≠ x with H(y) = H(x) weak collision resistance. It is computationally infeasible to find any pair (x, y) such that H(x) = H(y) – strong collision property.	2	4	K1
6	**What is the meet in the middle attack?** This is the cryptanalytic attack that attempts to find the value in each of the range and domain of the composition of two functions such that the forward mapping of one through the first function is the same as the inverse image of the other through the second function-quite literally meeting in the middle of the composed function.	2	4	K1

7	**List the Requirements for a Cryptographic Hash Function H**			
	<table><tr><th>Requirement</th><th>Description</th></tr><tr><td>Variable input size</td><td>H can be applied to a block of data of any size.</td></tr><tr><td>Fixed output size</td><td>H produces a fixed-length output.</td></tr><tr><td>Efficiency</td><td>$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.</td></tr><tr><td>Preimage resistant (one-way property)</td><td>For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.</td></tr><tr><td>Second preimage resistant (weak collision resistant)</td><td>For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.</td></tr><tr><td>Collision resistant (strong collision resistant)</td><td>It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.</td></tr><tr><td>Pseudorandomness</td><td>Output of H meets standard tests for pseudorandomness.</td></tr></table>	2	4	K1
8	**What are the two categories of attacks on hash function**	2	4	K1
	Brute-force attacks and cryptanalysis. A brute-force attack does not depend on the specific algorithm but depends only on bit length. In the case of a hash function, a brute-force attack depends only on the bit length of the hash value. A cryptanalysis, in contrast, is an attack based on weaknesses in a particular cryptographic algorithm.			
9	**What is the role of a compression function in a hash function?**	2	4	K1
	The hash algorithm involves repeated use of a **compression function**, f, that takes two inputs (an -bit input from the previous step, called the *chaining variable*, and a -bit block) and produces an -bit output. At the start of hashing, the chaining variable has an initial value that is specified as part of the algorithm. The final value of the chaining variable is the hash value. Often, hence the term ***compression.***			
10	**What is meant by Birthday attacks?**	2	4	K1
	It is a one type of attack .it means an opponent would have try about $2^{(\text{hashcode size-1})}$ messages to find one that matches the hash code of intercepted message. **Ex**: if encrypted hash code c is transmitted with corresponding un encrypted message m, then opponent need to find m, **h(m')=h(m)** to substitute another message and fool the receiver. An average opponent tries 263 to find one matches of hash code			
11	**Define the classes of message authentication function**	2	4	K1
	• **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator • **Message encryption:** The ciphertext of the entire message serves as its authenticator • **Message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator			
12	**Define digital signature.**	2	4	K1
	A digital signature is an authentication mechanism that enables the creator of a message to attach a code that acts as a signature. Typically the signature is formed by taking the hash of the message and encrypting the message with the creator's private key. The signature guarantees the source and integrity of the message.			

13	**What requirements should a digital signature scheme satisfy?**	2	4	K1
	On the basis of the properties and attacks just discussed, the following requirements for a digital signature. • The signature must be a bit pattern that depends on the message being signed. • The signature must use some information unique to the sender to preventboth forgery and denial. • It must be relatively easy to produce the digital signature. • It must be relatively easy to recognize and verify the digital signature. • It must be computationally infeasible to forge a digital signature, either by constructing a new message for an existing digital signature or by constructing a fraudulent digital signature for a given message. • It must be practical to retain a copy of the digital signature in storage.			
14	**What are the properties a digital signature should have?**	2	4	K1
	• It must verify the author and the date and time of the signature. • It must authenticate the contents at the time of the signature. • It must be verifiable by third parties, to resolve disputes. Thus, the digital signature function includes the authentication function.			
15	**Define the term direct digital signature**		4	K1
	The term direct digital signature refers to a digital signature scheme that involves only the communicating parties (source, destination). It is assumed that the destination knows the public key of the source.	2		
16	**What do you understand by Kerberos?**	2	4	
	• Kerberos is an authentication service designed for use in a distributed environment. • Kerberos provides a trusted third-party authentication service that enables clients and servers to ***establish authenticated communication***.			
17	**What four requirements were defined for Kerberos?**	2	4	K1
	➢ **Secure:** A network eavesdropper should not be able to obtain the necessary information to impersonate a user. ➢ **Reliable:** For all services that rely on Kerberos for access control, it should ensure availability of the Kerberos service. ➢ **Transparent:** Ideally, the user should not be aware that authentication is taking place. ➢ **Scalable:** The system should be capable of supporting large numbers of clients and servers.			
18	**In the context of Kerberos, what is a realm?**	2	4	K1
	❖ A Kerberos realm is a set of managed ***nodes that share the same Kerberos database***. ❖ The Kerberos database resides on the Kerberos master computer system, which should be kept in a physically secure room. ❖ A read-only copy of the Kerberos database might also reside on other Kerberos computer systems. However, all changes to the database must be made on the master computer system.			
19	**Define a Kerberos Principal.**	2	4	K1
	• **Kerberos principal** is a service or user that is known to the Kerberos system. • Each Kerberos principal is identified by its principal name.			

	• Principal names consist of three parts: ✓a service or user name, ✓an instance name, and ✓a realm name			
20	**What is mean by SET? What are the features of SET?**	2	4	K1
	Secure Electronic Transaction (SET) is an open encryption and security specification designed to protect credit card transaction on the Internet. Features are: 1. Confidentiality of information 2. Integrity of data 3. Cardholder account authentication 4. Merchant authentication			
21	**What are the steps involved in SET Transaction?**	2	4	K1
	1. The customer opens an account 2. The customer receives a certificate 3. Merchants have their own certificate 4. The customer places an order. 5. The merchant is verified. 6. The order and payment are sent. 7. The merchant requests payment authorization. 8. The merchant confirms the order. 9. The merchant provides the goods or services. 10. The merchant requests payment.			

PART – B (12 Mark Questions with Key)

S.No	Questions	Mark	COs	BTL
1	**Explain about Security Requirements for Cryptographic Hash Functions.**	12	4	K2
				

Requirement	Description
Variable input size	H can be applied to a block of data of any size.
Fixed output size	H produces a fixed-length output.
Efficiency	$H(x)$ is relatively easy to compute for any given x, making both hardware and software implementations practical.
Preimage resistant (one-way property)	For any given hash value h, it is computationally infeasible to find y such that $H(y) = h$.
Second preimage resistant (weak collision resistant)	For any given block x, it is computationally infeasible to find $y \neq x$ with $H(y) = H(x)$.
Collision resistant (strong collision resistant)	It is computationally infeasible to find any pair (x, y) such that $H(x) = H(y)$.
Pseudorandomness	Output of H meets standard tests for pseudorandomness.

Brute force attack & Cryptanalysis.

2	**Explain in detail about Applications Of Cryptographic Hash Functions.**	12	4	K2
	➢ Simplified Examples of the Use of a Hash Function for Message Authentication. ➢ Simplified Examples of Digital Signatures			

3	**Explain in detail about message authentication functions**	12	4	K2
	➢ **3 classes of functions –** **Hash function:** A function that maps a message of any length into a fixed length hash value, which serves as the authenticator **Message encryption:** The ciphertext of the entire message serves as its authenticator **Message authentication code (MAC):** A function of the message and a secret key that produces a fixed-length value that serves as the authenticator ➢ **Basic Uses of Message Encryption** ➢ **Basic Uses of Message Authentication code (MAC)**			
4	**Explain how the HMAC algorithm produces authentication code for assuring integrity.**	12	4	K2
	▪ HMAC Design Objectives ▪ HMAC Algorithm with diagram ▪ Security of HMAC			
5	**Describe digital signature algorithm and show how signing and verification is done using DSS**	12	4	K2
	➢ Two approaches of Digital signature- RSA & DSS approach. ➢ Algorithm steps ➢ Signing and verifying with diagram			
6.	**Mention the working principles and key features of SET for E-Commerce Transactions.**	12	4	K2
	➢ The Secure Electronic Transaction (SET) is a protocol designed for protecting credit card transactions over the Internet. It is an industry-backed standard that was formed by MasterCard and Visa (acting as the governing body) in February 1996. ➢ Features of SET. ➢ Participants of SET. ➢ Steps involved in SET Transaction. ➢ Dual Signature. ➢ Payment processing.			
	PART – C (20 Mark Questions with Key)			
1	**Explain SHA-512 Logic and Round function with neat illustration.**	20	4	K2
	SHA-512 Logic Fig: Message Digest Generation Using SHA-512 • Step1: Append padding bits • Step2: Append length • Step3: Initialize hash buffer. • Step4: Process message in 1024-bit (128-word) blocks. • Step5: output **Round function** • Diagram and equations			
2	**Describe in detail about the implementation of Kerberos and explain the Kerberos Encryption techniques.**	20	4	K2
	Answer: give explanation for the following topics. • Requirements of Kerberos			

	• Overview of Kerberos - diagram • A simple authentication dialogue - Kerberos Version 4 • A more secure authentication dialogue - Kerberos Version 4 • Differences between versions 4 and 5			

PART – A (2 Mark Questions With Key)				
S.No	**Questions**	**Mark**	**COs**	**BTL**
	UNIT V-NETWORK AND INTERNET SECURITY			
1	**What is Secure Socket Layer and Transport Layer Security?** • Secure Socket Layer (SSL) provides security services between TCP and applications that use TCP. The Internet standard version is called Transport Layer Service (TLS). • SSL/TLS provides confidentiality using symmetric encryption and message integrity using a message authentication code. • SSL/TLS includes protocol mechanisms to enable two TCP users to determine the security mechanisms and services they will use.	2	5	K1
2	**List the two security services provided by SSL Record Protocol for SSL connections.** ✓**Confidentiality:** The Handshake Protocol defines a shared secret key that is used for conventional encryption of SSL payloads. ✓**Message Integrity:** The Handshake Protocol also defines a shared secret key that is used to form a message authentication code (MAC).	2	5	K1
3	**List the operation of a SSL record protocol.** a. Fragmentation b. Compression c. Add MAC d. Encryption e. Append SSL record header	2	5	K1
4	**Write about SSL connection and Session** ➢ **Connection:** A connection is a transport (in the OSI layering model definition) that provides a suitable type of service. For SSL, such connections are peer-to-peer relationships. The connections are transient. Every connection is associated with one session. ➢ **Session:** An SSL session is an association between a client and a server. Sessions are created by the Handshake Protocol. Sessions define a set of cryptographic security parameters which can be shared among multiple connections. Sessions are used to avoid the expensive negotiation of new security parameters for each connection.	2	5	K1
5	**What is the purpose of HTTPS** HTTPS (HTTP over SSL) refers to the combination of HTTP and SSL to implement secure communication between a Web browser and a Web server. The HTTPS capability is built into all modern Web browsers. Its use depends on the Web server supporting HTTPS communication. For example, search engines do not support HTTPS.	2	5	K1
6	**List and briefly define the parameters that define an SSL session state.**	2	5	K1

	• Session identifier • Peer certificate • Compression method • Cipher spec • Master secret • Is resumable			
7	**List and briefly define the parameters that define an SSL session connection.**			
	• Server and client random • Server write MAC secret • Client write MAC secret • Server write key • Client write key • Initialization vectors • Sequence numbers	2	5	K1
8	**For what applications is SSH useful?**	2	5	K1
	SSH client and server applications are widely available for most operating systems. It has become the method of choice for remote login and X tunneling and is rapidly becoming one of the most pervasive applications for encryption technology outside of embedded systems.			
9	**List and briefly define the SSH protocols.**	2	5	K1
	• **Transport Layer Protocol:** Provides server authentication, data confidentiality, and data integrity with forward secrecy (i.e., if a key is compromised during one session, the knowledge does not affect the security of earlier sessions).The transport layer may optionally provide compression. • **User Authentication Protocol:** Authenticates the user to the server. • **Connection Protocol:** Multiplexes multiple logical communications channels over a single, underlying SSH connection.			
10	**What is Pretty Good Privacy (PGP)?**	2	5	K1
	❖ PGP is an ***open-source, freely available software package for e-mail security***. It provides authentication through the use of digital signature, confidentiality through the use of symmetric block encryption, compression using the ZIP algorithm, and e-mail compatibility using the radix-64 encoding scheme. ❖ PGP incorporates tools for developing a public-key trust model and public-key certificate management			
11	**Mention the services provided by the Pretty Good Privacy (PGP).**	2	5	K1
	❖ Authentication ❖ Confidentiality ❖ Compression ❖ E-mail compatibility ❖ Segmentation and reassembly			
12	**Why does PGP generate a signature before applying compression?**	2	5	K1
	There are two reasons behind it. • It is preferable to sign an uncompressed message so that one can store only the uncompressed message together with the signature for future verification. • If one signed a compressed document, then it would be necessary either to store a compressed version of the message • For later verification or to recompress the message when verification is required. • Even if one were willing to generate dynamically a recompressed message for			

	verification, PGP's compression algorithm presents a difficulty.			
13	**What is R64 conversion?**	2	5	K1
	• Radix-64 is the technique which is used for E-mail compatibility. • In Radix-64, each group of 3 octets of binary data is mapped into4 ASCII characters.			
14	**What is S/MIME**	2	5	K1
	Secure/Multipurpose Internet Mail Extension (S/MIME) is a security enhancement to the MIME Internet e-mail format standard based on technology from RSA Data Security.			
15	**What is RFC 5322?**		5	K1
	• RFC 5322 defines a format for text messages that are sent using electronic mail. It has been the standard for Internet-based text mail messages and remains in common use. • In the RFC 5322 context, messages are viewed as having an envelope and contents. • The envelope contains whatever information is needed to accomplish transmission and delivery. The contents compose the object to be delivered to the recipient.	2		
16	**What are the elements of MIME?**	2	5	
	1. Five new message header fields are defined, which may be included in an RFC 5322 header. These fields provide information about the body of the message. 2. A number of content formats are defined, thus standardizing representations that support multimedia electronic mail. 3. Transfer encodings are defined that enable the conversion of any content format into a form that is protected from alteration by the mail system.			
17	**What are the headers fields define in MIME?**	2	5	K1
	The five header fields defined in MIME are • MIME-Version • Content-Type • Content-Transfer-Encoding • Content-ID • Content-Description			
18	**What is MIME content type &explain?**	2	5	K1
	It is used to declare general type of data. Subtype define particular format for that type of the data. It has 7 content type & 15 subtypes. They are, • Text type • Multipart type • Message type • Image type • Video type. • Audio type. • Application type			
19	**Give examples of applications of IPsec.**	2	5	K1
	• Secure branch office connectivity over the Internet • Secure remote access over the Internet • Establishing extranet and intranet connectivity with partners • Enhancing electronic commerce security:			
20	**What services are provided by IPsec?**	2	5	K1
	• Access control • Connectionless integrity • Data origin authentication			

	• Rejection of replayed packets (a form of partial sequence integrity) • Confidentiality (encryption) • Limited traffic flow confidentiality			
21	**What do you mean by Security Association (SA)? Specify the parameter that identifies the Security Association?**	2	5	K1
	➢ An association is a one-way relationship between a sender and receiver that affords security services to the traffic carried on. ➢ A key concept that appears in both the authentication and confidentiality mechanism for ip is the security association (SA). ➢ A security Association is uniquely identified by 3 parameters: ➢ Security Parameter Index (SPI). ➢ IP Destination Address. ➢ Security Protocol Identifier.			
22	**What is a replay attack?**	2	5	K1
	➢ A **replay attack** is one in which an attacker obtains a copy of an authenticated packet and later transmits it to the intended destination. ➢ The receipt of duplicate, authenticated IP packets may disrupt service in some way or may have some other undesired consequence.			
23	**Why does ESP include a padding field?**	2	5	K1
	The Padding field serves several purposes: **(write any 2 points)** ➢ If an encryption algorithm requires the plaintext to be a multiple of some number of bytes (e.g., the multiple of a single block for a block cipher), the Padding field is used to expand the plaintext (consisting of the Payload Data, Padding, Pad Length, and Next Header fields) to the required length. ➢ The ESP format requires that the Pad Length and Next Header fields be right aligned within a 32-bit word. Equivalently, the ciphertext must be an integer multiple of 32 bits. The Padding field is used to assure this alignment. ➢ Additional padding may be added to provide partial traffic-flow confidentiality by concealing the actual length of the payload.			
24	**What is firewall and its characteristics?**	2	5	K1
	• A firewall is a ***hardware and software running on a host computer***, or ***placed at junction /gateway between two networks***. Generally inserted /placed between LAN and Internet, to protect internet based attacks. • Characteristics of firewall: ❖ Service control ❖ Direction control ❖ User control ❖ Behavior control ❖ Audits and alarms ❖ NAT (Network address translation) – mapping between local and IP address. ❖ Serve as IPSec (IPSecurity)			
25	**What are the types of firewall?**	2	5	K1
	• Packet filtering firewall • Application level gateway • Circuit level gateway			

26	**What are Worms?**	2	5	K1
	A worm is a program that can replicate itself and send copies from computer to computer across network connections. Upon arrival, the worm may be activated to replicate and propagate again.			

PART – B (12 Mark Questions with Key)

S.No	Questions	Mark	COs	BTL
1	**Explain in detail about SSL record protocol and protocol operations.**	12	5	K2
	Answer: give explanation for the following topics. ▪ **SSL connection and Session with parameters.** ▪ SSL Record protocol ▪ Protocol operations			
2	**Explain in detail about transport layer security**	12	5	K2
	Answer: give explanation for the following topics. • Version number • Message Authentication Code • Pseudorandom Function • Alert codes.			
3	**Explain in detail about Secure Shell(SSH) protocols**	12	5	K2
	Answer: give explanation for the following topics. • **Transport Layer Protocol:** Provides server authentication, data confidentiality, and data integrity with forward secrecy (i.e., if a key is compromised during one session, the knowledge does not affect the security of earlier sessions).The transport layer may optionally provide compression. • **User Authentication Protocol:** Authenticates the user to the server. • **Connection Protocol:** Multiplexes multiple logical communications channels over a single, underlying SSH connection.			
4	**Explain Secure / Multipurpose Internet Mail Extension (S/MIME).**	12	5	K2
	Answer: give explanation for the following topics • RFC 5322 • Multipurpose Internet Mail Extensions specification, content types • S/MIME functions.			
5	**Explain in detail about internet security policy**	12	5	K2
	IPsec Architecture Diagram. IPsec policy is determined primarily by the interaction of two databases, • The security association database (SAD) and • The security policy database (SPD).			
6	Explain in detail about Encapsulation security Payload(ESP)	12	5	K2
7	**Describe about the viruses.**	12	5	K2
	Answer: give explanation for the following topics. • Viruses • Phases of viruses -Dormant phase – activated by system event -Propagation phase -Triggering phase – when and what purpose it is trigggered			

	-Execution phase – copying and damaging • Viruses classification. • Macro virus • Email virus			
8	**Explain in detail about Worms**	12	5	K2
	• Worm replication methods. • Morris worm. • Worm propagation model. • State of Worm Technology • Worm Countermeasures			
	PART – C (20 Mark Questions with Key)			
1	**Discuss the operational description services provided by PGP.**	20	5	K2
	Answer: give explanation for the following topics. ✓ Authentication only ✓ Confidentiality only ✓ Confidentiality and authentication ✓ E-mail compatibility ✓ Compression ✓ PGP message format			
2	**Explain in detail about** **(i) Firewall characteristics.** **(ii) Types of Firewall.**	08 12	4	K2
	(i) **Firewall characteristics.** • Firewall design goals • Firewall control access • scope of firewall • Firewall limitations (ii) **Firewall Types** • Packet filtering firewall • Application level gateway • Circuit level gateway			