	ii.	What are Message Authentication Codes (MACs)? How can their performance be measured? Propose strategies for troubleshooting inefficiencies in MAC-based security systems.	**6**	03	04	04	02
OR	iii.	In a network security system, HMAC with SHA-512 is used to authenticate 5 million messages per hour. If each HMAC operation takes 200 microseconds, calculate the total computation time for HMACs in an hour. What techniques could you use to improve performance?	**6**	03	03	04	03
Q.6		Attempt any two:					
	i.	Describe the key components of the Kerberos authentication model and the role each plays in the overall security of the system.	**5**	02	02	05	03
	ii.	Explain how the X.509 authentication service verifies the identity of entities and ensures data integrity in a public key infrastructure (PKI).	**5**	02	02	05	03
	iii.	Explain the process of signing and encrypting an email using S/MIME. How does S/MIME ensure the authenticity and privacy of messages?	**5**	03	03	05	03

******

Total No. of Questions: 6 *Total No. of Printed Pages:4*

Enrollment No.....

Faculty of Engineering
End Sem Examination Dec 2024
IT3EL10 Information Security

Programme: B.Tech. Branch/Specialisation: IT

Duration: 3 Hrs. **Maximum Marks: 60**

Note: All questions are compulsory. Internal choices, if any, are indicated. Answers of Q.1 (MCQs) should be written in full instead of only a, b, c or d. Assume suitable data if necessary. Notations and symbols have their usual meaning.

			Marks	**BL**	**PO**	**CO**	**PSO**
Q.1	i.	Which of the following is NOT a security attack? (a) Passive attack (b) Active attack (c) Symmetric attack (d) Man-in-the-middle attack	**1**	01	01	01	01
	ii.	The symmetric cipher model primarily involves- (a) Different keys for encryption and decryption (b) The same key for both encryption and decryption (c) A keyless encryption system (d) Public key infrastructure	**1**	01	01	01	01
	iii.	What is the block size of the Data Encryption Standard (DES)? (a) 64 bits (b) 128 bits (c) 256 bits (d) 32 bits	**1**	01	01	02	01
	iv.	Which algorithm is used to compute the greatest common divisor (GCD) of two numbers? (a) DES Algorithm (b) Euclidean Algorithm (c) AES Algorithm (d) Modular Multiplication	**1**	01	02	02	01

v.	Which of the following algorithms is used for key exchange in public key cryptography? (a) RSA (b) Diffie-Hellman (c) AES (d) DES	**1**	01	01	03	01
vi.	In RSA, what is the fundamental problem that ensures its security? (a) Prime number generation (b) Modular arithmetic (c) Factoring large numbers (d) Diffie-Hellman problem	**1**	01	01	03	02
vii.	When designing an information security policy, which factor must be considered when using Secure Hash Algorithms (SHA)? (a) Length of the message (b) Collision resistance of the algorithm (c) Encryption speed (d) Symmetric key distribution	**1**	01	02	04	02
viii.	When designing an organization's digital signature policy, what should be ensured for compliance with the Digital Signature Standard (DSS)? (a) Use of RSA for all digital signatures (b) Proper implementation of the Digital Signature Algorithm (DSA) (c) Avoidance of key management (d) Ensuring all messages are encrypted	**1**	01	02	04	02
ix.	What is the primary purpose of Kerberos in an authentication application? (a) To encrypt email messages (b) To provide end-to-end network encryption (c) To provide a secure method for authenticating users (d) To filter and block network traffic	**1**	01	02	05	01
x.	Which technology uses digital certificates to verify user identities in a network? (a) Firewalls (b) S/MIME	**1**	01	01	05	01

		(c) X.509 Authentication service (d) Pretty Good Privacy						
Q.2	i.	Define Information security with an example.	**2**	01	01	01	01
	ii.	Describe the role of confidentiality, integrity, and availability in security services.	**3**	02	02	01	01
	iii.	What are the essential services provided by information security? Discuss each with examples.	**5**	02	02	01	03
OR	iv.	How does the Vigenère cipher improve upon the Caesar cipher? Encrypt the message "PAY MORE MONEY" using the key "ATTACK" and show the result.	**5**	03	05	01	03
Q.3	i.	Explain the principles of confusion and diffusion in block ciphers.	**2**	02	02	02	01
	ii.	The AES algorithm uses substitution and permutation steps to ensure security. Describe the AES encryption process, including the key expansion process.	**8**	02	05	02	02
OR	iii.	What is the Euclidean algorithm, and how is it applied in cryptography? Demonstrate its use by finding the GCD of 120 and 35 using the Euclidean algorithm.	**8**	03	03	02	03
Q.4	i.	What is the difference between symmetric and asymmetric key cryptography?	**3**	02	02	03	01
	ii.	Perform encryption and decryption using ECC on the elliptic curve $E_{11}(1,1)$ with the plain text (4,6).	**7**	03	05	03	02
OR	iii.	Explain the working of RSA algorithm. Perform encryption for the plain text 30 using RSA algorithm with the values p=5, q=7 and 13 as the public key. Also check your answer by decrypting the cipher text.	**7**	03	03	03	03
Q.5	i.	What is cryptographic hash function? What are the various security attacks on cryptographic hash function?	**4**	02	02	04	01

Marking Scheme

IT3EL10 (T) Information Security (T)

Q.1	i)	c. Symmetric attack	**1**
	ii)	a. The same key for both encryption and decryption	**1**
	iii)	b. 64 bits	**1**
	iv)	a. Euclidean Algorithm	**1**
	v)	b. Diffie-Hellman	**1**
	vi)	c. Factoring large numbers	**1**
	vii)	b. Collision resistance of the algorithm	**1**
	viii)	b. Proper implementation of the Digital Signature Algorithm (DSA)	**1**
	ix)	c. To provide a secure method for authenticating users	**1**
	x)	c. X.509 Authentication service	**1**
Q.2	i.	Define IS 2M Example 2M	**2**
	ii.	Describe the role of confidentiality, integrity, and availability in security services. **1 mark each**	**3**
	iii.	What are the essential services provided by information security? Discuss each with examples.	**5**
OR	iv.	Vigenère cipher improve upon 2M the Caesar cipher? 3M Answer is PTRMQBEFHNQI	**5**
Q.3	i.	Principles of confusion and diffusion in block ciphers.	**2**
	ii.	AES encryption process, including the key expansion.	**8**
OR	iii.	Euclidean algorithm, 2M Its application in cryptography 2M GCD of 120 and 35 using the Euclidean algorithm is 5 4M	**8**
Q.4	i.	Difference between symmetric and asymmetric key cryptography **1M each**	**3**
	ii.	Encryption 3.5M Decryption 3.5M	**7**
OR	iii.	Explain the working of RSA algorithm. Perform encryption for the plain text 30 using RSA algorithm with the values p=5, q=7 and 13 as the public key. Also check your answer by decrypting the cipher text.	**7**
Q.5	i.	What is cryptographic hash function? 2M What are the various security attacks on cryptographic hash function? 2M	**4**
	ii.	What are Message Authentication Codes (MACs), and how can their performance be measured? 3M Propose strategies for troubleshooting inefficiencies in MAC-based security systems. 3M	**6**
OR	iii.	In a network security system, HMAC with SHA-512 is used to authenticate 5 million messages per hour. If each HMAC operation takes 200 microseconds, calculate the total computation time for HMACs in an hour. 3M What techniques could you use to improve performance? 3M	**6**
Q.6		Attempt any two:	
	i.	Describe the key components of the Kerberos authentication model 2M The role each plays in the overall security of the system. 3M	**5**
	ii.	Explain how the X.509 authentication service verifies the identity of entities and ensures data integrity in a public key infrastructure (PKI).	**5**
	iii.	Explain the process of signing and encrypting an email using S/MIME. 3M How does S/MIME ensure the authenticity and privacy of messages? 2M	**5**

******

P.T.O.