Reg. No.																

Question Paper Code	14076

M.Tech. - DEGREE EXAMINATIONS, NOV / DEC 2025

Eighth Semester

M.Tech. - Computer Science and Engineering (5 Years Integrated)

20CJEL807 - APPLIED CRYPTOGRAPHY

Regulations - 2020

Duration: 3 Hours | Max. Marks: 100

PART - A (MCQ) (10 × 1 = 10 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	What does HTTPS provide in web security? (a) Authentication and confidentiality (b) Developers (c) Customers (d) None of the mentioned	1	K1	CO1
2.	How does a digital signature ensure non-repudiation? (a) By encrypting data in transit (b) By verifying the integrity of data (c) By providing evidence of the sender's identity (d) By monitoring for unauthorized access	1	K1	CO1
3.	Intel digital random number generator uses which among the following methods to generate random bits? (a) pulse detectors of ionizing radiating events (b) gas discharge tubes (c) wind resistance (d) thermal noise	1	K2	CO2
4.	Which cipher is part of the 5G standard and used for encryption? (a) RC4 (b) ZUC (c) AES (d) Twofish	1	K1	CO2
5.	Which algorithm is commonly used for digital signatures? (a) AES (b) RC4 (c) RSA (d) DES	1	K1	CO3
6.	Which of the following is an advantage of ECC? (a) Requires large key size (b) High computational cost (c) Efficient for mobile and IoT devices (d) Poor security	1	K1	CO3
7.	Which of the following describes electronic cash? (a) A debit card payment system (b) A customer buys electronic coins digitally signed by a bank (c) A credit card payment system (d) RSA cryptography is used in transactions	1	K1	CO4
8.	Which of the following is NOT a property of zero-knowledge proofs? (a) Completeness (b) Soundness (c) Confidentiality (d) Zero-knowledge	1	K1	CO4
9.	Which theorem is fundamental to quantum cryptography? (a) Pythagorean theorem (b) No-cloning theorem (c) Fermat's theorem (d) Euler's theorem	1	K1	CO5
10.	Which classical cryptographic algorithms are most vulnerable to quantum attacks? (a) AES and SHA-256 (b) RSA and ECC (Elliptic Curve Cryptography) (c) Blowfish and Twofish (d) DES and MD5	1	K1	CO5

PART - B (12 × 2 = 24 Marks)

Answer ALL Questions

		Marks	K – Level	CO
11.	What is a digital signature?	2	K1	CO1
12.	List any two security services in cryptography.	2	K1	CO1
13.	Classify the main security weakness of the A5/1 cipher used in GSM encryption.	2	K2	CO2
14.	What is the Feistel structure in DES?	2	K1	CO2
15.	Write the general equation of an elliptic curve used in cryptography.	2	K1	CO3
16.	What is meant by a hash function?	2	K1	CO3

17.	Name the three main properties of zero-knowledge proofs.	2	K1	CO4
18.	What is the primary feature of anonymous electronic cash systems?	2	K1	CO4
19.	What are some applications of lattice-based cryptography?	2	K1	CO5
20.	Identify the reason for multivariate cryptography considered post-quantum secure.	2	K2	CO5
21.	What is a pseudo-random number?	2	K1	CO1
22.	Infer the security focus of the ZUC cipher, and how does it contribute to the 5G standard.	2	K2	CO2

PART - C (6 × 11 = 66 Marks)

Answer ALL Questions

23.	a)	Explain the role of elementary number theory in cryptography. Discuss how prime numbers and modular arithmetic contribute to encryption techniques.	11	K2	CO1
		OR			
	b)	Compare and contrast symmetric and asymmetric encryption in ensuring confidentiality. Provide examples of cryptosystems used in each case.	11	K2	CO1
24.	a)	Discuss the evolution of stream ciphers in mobile communication with reference to SNOW 3G and ZUC.	11	K2	CO2
		OR			
	b)	Explain the architecture and steps of the DES encryption algorithm.	11	K2	CO2
25.	a)	Describe in detail about Elliptic Curve Cryptography with suitable examples.	11	K2	CO3
		OR			
	b)	How does hashing contribute to the security of digital signatures? Explain in detail.	11	K2	CO3
26.	a)	Examine why key rotation is important in cryptographic systems, and explain how applying regular key rotation can reduce security risks. Also describe a practical method you would use to implement periodic key rotation in an organization.	11	K3	CO4
		OR			
	b)	Analyze the use of cryptographic techniques in ensuring the security and anonymity of e-cash transactions. Provide examples of such techniques.	11	K3	CO4
27.	a)	Explain the concept of multivariate cryptography and its departure from traditional encryption methods.	11	K2	CO5
		OR			
	b)	Discuss the significance of the Learning With Errors (LWE) problem in lattice-based cryptography.	11	K2	CO5
28.	a)	Discuss RC4 as a stream cipher. Explain its working and the security vulnerabilities associated with it.	11	K2	CO2
		OR			
	b)	Explain the ChaCha20 stream cipher, including its design, working, and applications.	11	K2	CO2