Reg. No.															

Question Paper Code	13268

B.E. / B.Tech. / M.Tech - DEGREE EXAMINATIONS, NOV / DEC 2024

Seventh Semester

Information Technology

(Common to Computer Science and Engineering & M.Tech. - Computer Science and Engineering (5years Integrated))

20ITPC701 - CRYPTOGRAPHY AND NETWORK SECURITY

Regulations - 2020

Duration: 3 Hours Max. Marks: 100

PART - A (MCQ) (20 × 1 = 20 Marks)

Answer ALL Questions

		Marks	K – Level	CO
1.	In the OSI Security Architecture, which of the following is an example of a security mechanism? (a) Encryption (b) Authentication (c) Data integrity (d) Traffic padding	1	K1	CO1
2.	Perfect security in cryptography means: (a) The encrypted message is impossible to decrypt without the key, regardless of computational power (b) The encrypted message cannot be decrypted even with the correct key (c) The encryption algorithm is computationally efficient (d) The encryption key is publicly available, but the message cannot be decrypted	1	K2	CO1
3.	Which of the following is the key concept behind public key cryptography? (a) Use of a single key for encryption and decryption (b) Use of two different but mathematically related keys (c) Hiding information within digital images (d) Random number generation for encryption	1	K1	CO1
4.	Euclid's algorithm is primarily used to compute: (a) Least common multiple (LCM) (b) Greatest common divisor (GCD) (c) Modular inverse (d) Prime factorization	1	K1	CO2
5.	In modular arithmetic, what is the inverse of 7mod 26 (under multiplication)? (a) 15 (b) 3 (c) 19 (d) 11	1	K2	CO2
6.	Which of the following is a property of a group in algebraic structures? (a) Associativity (b) Commutativity (c) Distribution (d) Reflexivity	1	K1	CO2
7.	Primality testing is used to: (a) Find prime factors of a number (b) Verify if a number is prime (c) Generate random numbers (d) Calculate logarithms	1	K1	CO3
8.	Which of the following is true about Elliptic Curve Cryptography (ECC)? (a) It requires larger key sizes than RSA for equivalent security (b) It is based on the difficulty of factoring large integers (c) It provides higher security with smaller key sizes compared to RSA (d) It uses symmetric encryption principles	1	K1	CO3
9.	In RSA, the public key consists of: (a) Two prime numbers (b) A modulus and an exponent (c) A shared secret key (d) A hash function and private key	1	K1	CO3
10.	In symmetric key cryptography, key distribution is a challenge because: (a) Keys need to be exchanged securely before communication (b) The encryption algorithm is vulnerable to attacks (c) It requires public keys to be shared with all users (d) The key size must be large enough to prevent brute-force attacks	1	K1	CO4
11.	Identify the key size used in the Simplified Data Encryption Standard (SDES). (a) 8 bits (b) 10 bits (c) 16 bits (d) 56 bits	1	K1	CO4

12.	Find out the primary purpose of the different modes of operation in block ciphers. (a) To allow the encryption of data streams of variable lengths (b) To decrease the size of the encryption key (c) To protect against known-plaintext attacks (d) To reduce the complexity of encryption algorithms	*1*	*K1*	*CO4*
13.	Indicate the primary purpose of an authentication function. (a) To ensure data confidentiality (b) To verify the identity of a user or entity (c) To provide data encryption (d) To generate cryptographic keys	*1*	*K1*	*CO5*
14.	Which of the following is true about Message Authentication Code (MAC)? (a) It is used to provide non-repudiation (b) It ensures both data integrity and authenticity (c) It is reversible like encryption (d) It only ensures data confidentiality	*1*	*K1*	*CO5*
15.	In the Kerberos authentication system, what does the Ticket Granting Ticket (TGT) allow? (a) It allows the user to access all resources without re-authentication (b) It grants the user access to a specific service (c) It allows the user to request service tickets from the Ticket Granting Server (TGS) (d) It provides encryption for the user's communication	*1*	*K1*	*CO5*
16.	X.509 certificates are primarily used for which purpose? (a) Encrypting network traffic (b) Providing digital certificates for public key infrastructure (PKI) (c) Securing passwords (d) Managing session keys for symmetric encryption	*1*	*K1*	*CO5*
17.	Firewalls are primarily used to: (a) Encrypt data (b) Prevent unauthorized access to a network (c) Scan for viruses (d) Provide email security	*1*	*K1*	*CO6*
18.	The internal code of any software that will set of a maliciousfunction when specified conditions are met, is called (a) logic bomb (b) trap door (c) code stacker (d) none of the mentioned	*1*	*K1*	*CO6*
19.	_____ Protocol is used to secure email communication by providing encryption, digital signatures, and key management. (a) PGP (Pretty Good Privacy) (b) HTTP (c) FTP (d) SSH	*1*	*K1*	*CO6*
20.	IP Security (IPsec) operates at which layer of the OSI model? (a) Application Layer (b) Network Layer (c) Transport Layer (d) Data Link Layer	*1*	*K1*	*CO6*

PART - B (10 × 2 = 20 Marks)

Answer ALL Questions

21.	Infer the primary goal of steganography.	*2*	*K1*	*CO1*
22.	Identify the different levels of security needed within an organization.	*2*	*K2*	*CO1*
23.	Write Euclid's algorithm to compute the GCD of two numbers.	*2*	*K1*	*CO2*
24.	List different algebraic structures used in cryptography.	*2*	*K1*	*CO2*
25.	Difference between private key and public key algorithm with suitable example.	*2*	*K2*	*CO3*
26.	What is meant by one-way property in hash function?	*2*	*K1*	*CO3*
27.	Differentiate stream cipher and block cipher with example.	*2*	*K2*	*CO4*
28.	List the evaluation criteria defined by NIST for AES.	*2*	*K1*	*CO4*
29.	Differentiate MAC and Hash function.	*2*	*K2*	*CO5*
30.	Indicate the design goals of firewalls.	*2*	*K1*	*CO6*

PART - C (6 × 10 = 60 Marks)

Answer ALL Questions

31.	a)	Illustrate the functionalities of OSI Security architecture model with neat diagram.	*10*	*K2*	*CO1*
		OR			
	b)	Demonstrate the process of classical cryptosystems and its types.	*10*	*K2*	*CO1*
32.	a)	Describe how algebraic structures are applied in cryptographic algorithms.	*10*	*K2*	*CO2*
		OR			
	b)	Relate the strengths and limitations of using modular arithmetic in encryption techniques.	*10*	*K2*	*CO2*
33.	a)	Using RSA algorithm, Find n, d if p=11, q=3, e=3. Encrypt "HelloWorld" Message. If user A has private key XA=3. What is A's public key YA?	*10*	*K3*	*CO3*
		OR			
	b)	State the Chinese Remainder Theorem and find X for the given set of congruent equations X≡2 mod 3, X≡3 mod 5 and X≡2 mod 7.	*10*	*K3*	*CO3*
34.	a)	Explain about AES encryption and Decryption in detail. Compare the substitution method in DES and AES.	*10*	*K2*	*CO4*
		OR			
	b)	Sketch the general structure of DES and examine the encryption decryption process.	*10*	*K2*	*CO4*
35.	a)	Illustrate the process of deriving eighty 64-bitwords 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.	*10*	*K3*	*CO5*
		OR			
	b)	Give the format for X.509 certificate. How are users certificates obtained?	*10*	*K3*	*CO5*
36.	a)	Explain the Cryptographic algorithms used in S/MIME and describe S/MIME certification processing.	*10*	*K2*	*CO6*
		OR			
	b)	How does PGP provide authentication and confidentiality for email services and for file transfer applications? Draw the block diagram and explain the components.	*10*	*K2*	*CO6*