Total No. of Questions: 6 *Total No. of Printed Pages:3*

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2022

CS3EY02 Cryptography

Programme: B.Tech. Branch/Specialisation: CSE All

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.

Q.1 i. In cryptography, what is cipher? **1**

(a) algorithm for performing encryption and decryption
(b) encrypted message
(c) both algorithm for performing encryption and decryption and encrypted message
(d) decrypted message

ii. Which of the following is not the primary objective of cryptography? **1**

(a) Confidentiality (b) Data Integrity
(c) Data Redundancy (d) Authentication

iii. In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____. **1**

(a) 11 (b) 13 (c) 16 (d) 17

iv. Quantum cryptography is the science of exploiting quantum mechanical properties to perform _____. **1**

(a) Cryptographic system (b) Cryptographic tasks
(c) Decryption system (d) None of these

v. For a network with N nodes, how many master keys are present? **1**

(a) N(N-1)/2 (b) N
(c) N(N+1)/2 (d) N/2

vi. In asymmetric key cryptography, the private key is kept by _____. **1**

(a) Sender
(b) Receiver
(c) Sender and receiver
(d) All the connected devices to the network

P.T.O.

vii. To authenticate using Kerberos, you must add the Kerberos user principals to MongoDB to the _____ database. **1**
(a) $internal (b) $external
(c) $extern (d) None of these

viii. Which one of the following is not a public key distribution means? **1**
(a) Public-Key Certificates
(b) Hashing Certificates
(c) Publicly available directories
(d) Public-Key authority

ix. The strong method for authentication is- **1**
(a) Message digest algorithms
(b) Encryption techniques
(c) Digital signature
(d) None of these

x. S/MIME provide_____. **1**
(a) Digital Signature (b) Encryption
(c) Integrity (d) All of these

Q.2 i. What is cryptography? Explain it. **2**
ii. What are different types of encryption techniques? **3**
iii. Explain symmetric and asymmetric encryption techniques. **5**
OR iv. What are difference between cryptoanalysis and cryptography? **5**

Q.3 i. What is quantum cryptography? **2**
ii. Describe RSA algorithm with related diagram and example. **8**
OR iii. Explain ECC algorithm. What is difference between ECC and RSA/DSA algorithms of key sizes in terms of computational effort for cryptanalysis? **8**

Q.4 i. What is key management in cryptography? **3**
ii. Explain in key management including creation, distribution, and verification. **7**
OR iii. Define revocation and destruction in key management. **7**

Q.5 i. What is cloud security and VPNs? **4**
ii. Explain major key distribution methods and algorithms including Kerberos, ISAKMP. **6**

OR iii. Explain Public Key Infrastructure (PKI) and System architecture requirements for implementing cryptographic functions. **6**

Q.6 Write a short note on any two:
i. Biometric authentication **5**
ii. SSO **5**
iii. Email security **5**

******

Marking Scheme
CS3EY02 Cryptography

Q.1	i.	In cryptography, what is cipher? (a) algorithm for performing encryption and decryption		**1**
	ii.	Which of the following is not the primary objective of cryptography? (c) Data Redundancy		**1**
	iii.	In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of A is 35. Then the private key of A is _____. (a) 11		**1**
	iv.	Quantum cryptography is the science of exploiting quantum mechanical properties to perform _____. (b) Cryptographic tasks		**1**
	v.	For a network with N nodes, how many master keys are present? (a) N(N-1)/2		**1**
	vi.	In asymmetric key cryptography, the private key is kept by _____. (b) Receiver		**1**
	vii.	To authenticate using Kerberos, you must add the Kerberos user principals to MongoDB to the _____ database. (b) $external		**1**
	viii.	Which one of the following is not a public key distribution means? (b) Hashing Certificates ty		**1**
	ix.	The strong method for authentication is- (c) Digital signature		**1**
	x.	S/MIME provide_____. (d) All of these		**1**
Q.2	i.	Cryptography		**2**
	ii.	Types of encryption techniques		**3**
	iii.	Symmetric encryption techniques	2.5 marks	**5**
		Asymmetric encryption techniques.	2.5 marks	
OR	iv.	Cryptoanalysis	2.5 marks	**5**
		Cryptography	2.5 marks	
Q.3	i.	Quantum cryptography		**2**
	ii.	RSA algorithm	2 marks	**8**
		Diagram and example.	4 marks	
		Explanation	2 marks	
OR	iii.	ECC algorithm	4 marks	**8**
		Difference between ECC and RSA/DSA algorithms	4 marks	
Q.4	i.	Key management in cryptography		**3**
	ii.	Key management including		**7**
		Creation	2 marks	
		Distribution	3 marks	
		Verification	2 marks	
OR	iii.	Revocation	3.5 marks	**7**
		Destruction in key management	3.5 marks	
Q.5	i.	Cloud security	2 marks	**4**
		VPNs	2 marks	
	ii.	Kerberos	3 marks	**6**
		ISAKMP	3 marks	
OR	iii.	Public Key Infrastructure (PKI)	3 marks	**6**
		Requirements for implementing cryptographic functions	3 marks	
Q.6		Write a short note on any two:		
	i.	Biometric authentication As per the explanation		**5**
	ii.	SSO As per the explanation		**5**
	iii.	Email security As per the explanation		**5**

******