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

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2022

CB3EL05 Cryptology

Programme: B.Tech. Branch/Specialisation: CSBS

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. Public key cryptography is a _____ cryptosystem. **1**

(a) Symmetric (b) Asymmetric
(c) Both (a) and (b) (d) None of these

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

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

v. Which of the following modes of operation in DES is used for operating? **1**

(a) Cipher feedback mode (CFB)
(b) Cipher block chaining (CBC)
(c) Electronic code book (ECB)
(d) Output feedback modes (OFB)

vi. 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

vii. When a hash function is used to provide message authentication, the hash function value is called to as: **1**
(a) Message field (b) Message digest
(c) Message score (d) Message leap

viii. A hash function is a _____ that converts a numerical input value into another compressed numerical value. **1**
(a) Abstract view (b) Mathematical function
(c) Both (a) and (b) (d) None of these

ix. Which possible attacks in quantum cryptography can take place? **1**
(a) Possible attacks in quantum cryptography and birthday attack
(b) Birthday attack and boomerang attack
(c) Brute force attack and faked-state-attack
(d) Possible attacks in quantum cryptography and faked-state attack

x. 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

Q.2 i. What is cryptography? Explain. **2**
ii. What are basic security services? Explain it. **3**
iii. Explain elementary number theory and pseudo-random bit generation. **5**
OR iv. Write a note on elementary cryptosystems. **5**

Q.3 i. What is symmetric cryptosystems? Explain. **2**
ii. What is a rivest cipher? How does RC4 work? Explain. **8**
OR iii. Explain Salsa and ChaCha? Explain. **8**

Q.4 i. What is block cipher? **3**
ii. Explain DES algorithm with related diagram and example. **7**

OR iii. Explain ECC algorithm with related diagram and example. **7**

Q.5 i. What is use of hash function in cryptography field? **4**
ii. What is digital signature algorithm? Explain with related diagram. **6**
OR iii. Explain types of hash functions with suitable example. **6**

Q.6 Attempt any two:
i. What is zero-knowledge protocol? **5**
ii. What are issues of quantum cryptanalysis? **5**
iii. Explain anonymous cash and micro-payments in electronic commerce term. **5**

******

Marking Scheme
CB3EL05 Cryptology

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.	Public key cryptography is a _____ cryptosystem. (b) Asymmetric		**1**
	iv.	For a network with N nodes, how many master secret keys are present? (a) N(N-1)/2		**1**
	v.	Which of the following modes of operation in DES is used for operating? (c) Electronic code book (ECB)		**1**
	vi.	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**
	vii.	When a hash function is used to provide message authentication, the hash function value is called to as: (b) Message digest		**1**
	viii.	A hash function is a _____ that converts a numerical input value into another compressed numerical value. (b) Mathematical function		**1**
	ix.	Which possible attacks in quantum cryptography can take place? (d) Possible attacks in quantum cryptography and faked-state attack		**1**
	x.	Quantum cryptography is the science of exploiting quantum mechanical properties to perform _____. (b) Cryptographic tasks		**1**
Q.2	i.	Cryptography Explanation	1 mark 1 mark	**2**
	ii.	Three basic security services 1 mark for each		**3**
	iii.	Elementary number theory Pseudo-random bit generation	2.5 marks 2.5 marks	**5**
OR	iv.	Write a note on elementary cryptosystems. As per the explanation		**5**
Q.3	i.	What is symmetric cryptosystems? Explain.		**2**
	ii.	Rivest cipher How does RC4 work	2 marks 6 marks	**8**
OR	iii.	Salsa ChaCha	4 marks 4 marks	**8**
Q.4	i.	What is block cipher?		**3**
	ii.	DES algorithm Diagram Example	3 marks 2 marks 2 marks	**7**
OR	iii.	ECC algorithm Diagram Example	3 marks 2 marks 2 marks	**7**
Q.5	i.	What is use of hash function in cryptography field?		**4**
	ii.	Digital signature algorithm Diagram	3 marks 3 marks	**6**
OR	iii.	At least five types of hash functions with suitable example. 2 marks for each		**6**
Q.6		Attempt any two:		
	i.	Zero-knowledge protocol As per the explanation		**5**
	ii.	At least five points on issues of quantum cryptanalysis		**5**
	iii.	Anonymous cash Micro-payments in electronic commerce term	2.5 marks 2.5 marks	**5**

******