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

Enrollment No......................................

Faculty of Engineering

End Sem (Odd) Examination Dec-2022

IT3EI08 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.

Q.1 i. If modified Caesar Cipher uses key= +4 then what will be the ciphertext of the plaintext:”CRACK IT”? **1**

(a) GVEGO MY (b) GVEGO MX
(c) YNWYG EP (d) YNWYG EQ

ii. A substitution cipher substitutes one symbol with- **1**

(a) Keys (b) Others
(c) Multi Parties (d) Single Party

iii. DES follows- **1**

(a) Hash Algorithm (b) Caesars Cipher
(c) Feistel Cipher Structure (d) SP Networks

iv. How many rounds does the AES-192 perform? **1**

(a) 10 (b) 12 (c) 14 (d) 16

v. The RSA algorithm is a _____________. **1**

(a) Secret key algorithm
(b) Public key cryptographic algorithm
(c) Private key cryptographic algorithm
(d) None of these

vi. Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not- **1**

(a) Authenticated (b) Joined
(c) Submitted (d) Separated

vii. MACs are also called- **1**

(a) Testword (b) Checkword
(c) Testbits (d) None of these

P.T.O.

viii. SHA-1 produces a hash value of- **1**

(a) 256 bits (b) 160 bits (c) 180 bits (d) 128 bits

ix. Kerberos is a _______ authentication protocol. **1**

(a) Test (b) Network (c) Global (d) Private

x. Which of the following is / are the types of firewalls? **1**

(a) Packet filtering firewall (b) Dual homed gateway firewall
(c) Screen host firewall (d) All of these

Q.2 i. What do you mean by integrity of a message? **2**

ii. Define active attacks. Explain Denial of service attack. **3**

iii. Using Playfair Cipher make a 5x5 matrix using the key:”PUZZLE”. Now encrypt the message “THE MEETING IS AT TREFFOREST” using the rules of Playfair cipher. **5**

OR iv. Explain with example: **5**

(a) Columnar Transpositon (b) Steganography

Q.3 i. Write two differences between block ciphers with stream ciphers. **2**

ii. Explain AES Algorithm in detail. Is AES based on Fiestal Structure like DES? Why is AES better than DES? **8**

OR iii. With help of a block diagram explain DES encryption algorithm. Also explain the strength of DES. **8**

Q.4 Attempt any two:

i. Draw a block diagram for public key Cryptography. Write the steps involved in RSA algorithm. **5**

ii. Briefly explain Diffie Hellman key exchange scheme. Also explain man in middle attack. **5**

iii. Explain elliptic curve cryptography in detail. **5**

Q.5 i. Write short notes on: **4**

(a) Hash function (b) Message authentication code

ii. Explain digital signature with its components. Write any two properties of digital signature. **6**

OR iii. Explain SHA-1 algorithm in detail. **6**

Q.6 Attempt any two:

i. What was Kerberos designed for? Explain the architecture of Kerberos. **5**

ii. Define a firewall. Explain two types of firewall in brief. **5**

iii. Explain the working of pretty good privacy for secure communication. **5**

******

Marking Scheme
IT3EI08 Information Security

Q.1	i.	If modified Caesar Cipher uses key= +4 then what will be the ciphertext of the plaintext:”CRACK IT”? **b)GVEGO MX**	**1**
	ii.	A substitution cipher substitutes one symbol with **b)Others**	**1**
	iii.	DES follows **c) Feistel Cipher Structure**	**1**
	iv.	How many rounds does the AES-192 perform? **b) 12**	**1**
	v.	For RSA to work, value of PT must be less than value of **c)n**	**1**
	vi.	Man-in-the-middle attack can endanger security of Diffie-Hellman method if two parties are not **a)Authenticated**	**1**
	vii.	MACs are also called **d) none of the mentioned**	**1**
	viii.	SHA-1 produces a hash value of **b) 160 bits**	**1**
	ix.	Kerberos is a _______ authentication protocol. **b) Network**	**1**
	x.	Which of the following is / are the types of firewall? **a) Packet Filtering Firewall**	**1**
Q.2	i.	What do you mean by Integrity of a message? **2Marks**	**2**
	ii.	Define Active attacks. Explain Denial of service attack. **Active attacks : 1.5 Marks** **Denial of Service attack : 1.5 Marks**	**3**
	iii.	Using Playfair Cipher make a 5x5 matrix using the key:”PUZZLE”. Now encrypt the message “THE MEETING IS AT TREFFOREST” using the rules of Playfair cipher. **For creating a Matrix : 2 Marks** **For encrypting message: 3 marks**	**5**
OR	iv.	Explain with example: (a)Columnar Transpositon (b)Steganography **(2.5+2.5)marks**	**5**
Q.3	i.	Write 2 differences between block ciphers with stream ciphers. **2 marks for 2 differences**	**2**
	ii.	Explain AES Algorithm in detail. Is AES based on Fiestal Structure like DES? Why is AES better than DES? **Explain AES Algorithm in detail. (6Marks)** **Is AES based on Fiestal Structure like DES? (1 Mark)** **Why is AES better than DES? (1 Mark)**	**8**
OR	iii.	With help of a block diagram explain DES Encryption algorithm.Also explain the strength of DES. **With help of a block diagram explain DES Encryption algorithm :- (6 Marks)** **Explain the strength of DES:- (2 Marks)**	**8**
Q.4	i.	Draw a block diagram for Public key Cryptography. Write the steps involved in RSA algorithm. **Draw a block diagram for Public key Cryptography (2Marks)** **Write the steps involved in RSA algorithm. (3Marks)**	**5**
	ii.	Briefly explain Diffie Hellman Key exchange scheme.Also explain Man in middle attack. **Diffie Hellman Key exchange scheme 2.5 marks** **Man in middle attack 2.5 Marks**	**5**
OR	iii.	Explain Elliptic Curve Cryptography in detail. **5 marks**	**5**
Q.5	i.	Write short notes on: a)Hash Function b)Message Authentication Code **(2+2)Marks**	**4**
	ii.	Explain Digital Signature with its components in detail.Write any 2 properties of Digital signature. **Digital Signature with its components in detail : 4 marks** **2 properties of Digital signature : 2Marks**	**6**
OR	iii.	Explain SHA-1 algorithm in detail. : **6 marks**	**6**
Q.6		Attempt any two:	
	i.	What was Kerberos designed for? Explain the architecture of Kerberos. **What was Kerberos designed for: 1 Mark**	**5**

		Explain the architecture of Kerberos: 4 Marks	
	ii.	Define a firewall. Explain 2 types of firewall in brief. **Firewall definition :1 Marks** **2 Types : (2+2)Marks=4 Marks**	**5**
	iii.	Explain the working of Pretty Good Privacy for secure communication. **5Marks**	**5**

******