Total No. of Questions: 6 *Total No. of Printed Pages:2*

Enrollment No.....

Faculty of Engineering

End Sem (Even) Examination May-2019

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. In Encryption, which key is used: **1**
(a) Public key (b) Private key
(c) Both (a) and (b) (d) None to these

ii. Authentication is done by: **1**
(a) Conventional encryption (b) Scrambling data
(c) Both (a) and (b) (d) None to these

iii. CBCM stands for **1**
(a) Cipher Block Chaining Mode
(b) Cipher Block Crypto Mode
(c) Cipher block Chaining method
(d) Cipher block Crypto method

iv. Encryption protects against: **1**
(a) Attacks (b) Loss of data
(c) Both (a) and (b) (d) None to these

v. Output message in cryptography is called **1**
(a) Plain text (b) Cipher text
(c) Both (a) and (b) (d) None to these

vi. The most widely used public key algorithm are **1**
(a) RSA (b) Diffie Hellman
(c) Both (a) and (b) (d) None to these

vii. Secure hash algorithm developed by: **1**
(a) NIST (b) IEEE (c) ANSI (d) None to these

viii. DSS stands for: **1**
(a) Digital signature standard
(b) Digital sound system
(c) Digital simulation schemes
(d) None to these

ix. IPSEC is designed to provide the security at **1**
(a) Session layer (b) Transport layer
(c) Application layer (d) Network layer

x. In tunnel mode IPSEC protects the **1**
(a) Entire IP packet (b) IP header
(c) IP payload (d) None of these

Q.2 i. What are the different types of security attacks? **2**

ii. Compare substitution ciphers with transposition ciphers. **3**

iii. Consider the following: **5**
Plaintext: “PROTOCOL”
Secret key: “NETWORK”
What is the corresponding cipher text using play fair cipher method?

OR iv. What is the need for information security in existing system? **5**

Q.3 i. Write about strength of DES algorithm. **2**

ii. Explain the AES algorithm in detail with diagram. **8**

OR iii. Consider a Diffie-Hellman scheme with a common prime q=11, and a primitive root α=2. **8**
(a) If user “A“ has public key YA=9, what is A ’s private key XA.
(b) If user “B“ has public key YB=3, what is shared secret key K.

Q.4 i. List the advantages of elliptic-curve cryptography. **3**

ii. Write short notes on key distribution mechanism for asymmetric key. **7**

OR iii. In an RSA system, the public key of a given user is e=31, n=3599. **7**
What is the private key of this user?

Q.5 i. What is a digital signature? **4**

ii. Explain HMAC algorithm using diagram. **6**

OR iii. Explain the role of hashing algorithms in maintaining trust and integrity. **6**

Q.6 Attempt any two:

i. Write different types of firewalls. **5**

ii. Explain PGP trust model. **5**

iii. Explain MIME context types. **5**

******

Marking Scheme
IT3EI08 Information Security

Q.1	i.	In Encryption, which key is used: (a) Public key		**1**
	ii.	Authentication is done by: (a) Conventional encryption		**1**
	iii.	CBCM stands for (a) Cipher Block Chaining Mode		**1**
	iv.	Encryption protects against: (d) None to these		**1**
	v.	Output message in cryptography is called (b) Cipher text		**1**
	vi.	The most widely used public key algorithm are (c) Both (a) and (b)		**1**
	vii.	Secure hash algorithm developed by: (a) NIST		**1**
	viii.	DSS stands for: (a) Digital signature standard		**1**
	ix.	IPSEC is designed to provide the security at (d) Network layer		**1**
	x.	In tunnel mode IPSEC protects the (a) Entire IP packet		**1**
Q.2	i.	Types of security attacks (at least two)		**2**
	ii.	Substitution ciphers with transposition ciphers. At least two differences 1.5 marks for each	(1.5 marks * 2)	**3**
	iii.	Consider the following: Plaintext: “PROTOCOL” Secret key: “NETWORK” Drawing matrix Final ciphertext by using rules	 2.5 marks 2.5 marks	**5**
OR	iv.	Need for information security in existing system At least five 1 mark for each reason	 (1 mark * 5)	**5**
Q.3	i.	Strength of DES algorithm. At least two strength1 mark for each	 (1 mark * 2)	**2**
	ii.	AES algorithm Stepwise diagram. Explanation	 6 marks 2 marks	**8**
OR	iii.	(a) If user “A“ has public key YA=9, what is A ’s private key XA. 4 marks (b) If user “B“ has public key YB=3, what is shared secret key K. 4 marks		**8**
Q.4	i.	At least two advantages of elliptic-curve cryptography. 1.5 marks for each	(1.5 marks * 2)	**3**
	ii.	Key distribution mechanism for asymmetric key. At least three key distribution		**7**
OR	iii.	In an RSA system, the public key of a given user is e=31, n=3599. What is the private key of this user? Formulas Calculating private key	 2.5 marks 4.5 marks	**7**
Q.5	i.	Digital signature Definition Explanation	 2 marks 2 marks	**4**
	ii.	HMAC algorithm Diagram.	3 marks 3 marks	**6**
OR	iii.	Role of hashing algorithms in maintaining trust and integrity. At least three points with explanation 2 marks for each	 (2 marks * 3)	**6**
Q.6		Attempt any two:		
	i.	At least two types of firewalls. 2.5 marks for each	 (2.5 marks *2)	**5**
	ii.	PGP trust model. Explanation Model/diagram	 2.5 marks 2.5 marks	**5**
	iii.	MIME context types. Definition Explanation of functioning, features and working	 2 marks 3 marks	**5**

******