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

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-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. Virus is a computer: **1**
(a) File (b) Program (c) Database (d) Network

ii. A worm _____ modify a program: **1**
(a) Does not (b) Does
(c) May or may not (d) May

iii. DES encrypts blocks of _____ bits: **1**
(a) 32 (b) 56 (c) 64 (d) 128

iv. There are around _____ rounds in DES: **1**
(a) 8 (b) 10 (c) 14 (d) 24

v. The private key _____ **1**
(a) Must be distributed (b) Must be shared with everyone.
(c) Must be kept secret. (d) None of these

vi. RSA _____ be used for digital signatures: **1**
(a) Must not (b) Cannot. (c) Can (d) Should not

vii. _____ is a message digest algorithm: **1**
(a) DES (b) IDEA (c) MD5 (d) ASA

viii. A _____ is used to verify integrity of message: **1**
(a) Message digest (b) Encryption Algorithm
(c) Digital envelope (d) None of these

ix. Kerberoes provides for _____ be used for digital signatures: **1**
(a) Encryption (b) SSO
(c) Remote login (d) Local login

x. A packet filter examins _____ packets: **1**
(a) All (b) No (c) Some (d) Alternate

Q.2 i. Write any two security features we want to achieve in the cyber world. **2**

ii. Explain Ceaser and modified Ceaser cipher technique. **3**

iii. Explain Hill Cipher technique in detail. **5**

OR iv. Explain the concept of Stagenography with a suitable example. **5**

Q.3 i. Define block cipher with example. **2**

ii. Explain the working of Data encryption Standard (DES) in detail. **8**

OR iii. Explain the working of Advanced Encryption Standard (AES) in detail. **8**

Q.4 i. Explain the concept of public key cryptography. **3**

ii. Explain the working of RSA Algorithm with suitable example in detail. **7**

OR iii. Explain the working of Diffie Hellman Key Exchange in detail. **7**

Q.5 i. Explain the concept of Digital signatures in detail. **4**

ii. Explain the working of MD5 algorithm in detail. **6**

OR iii. Write short note on: **6**
(a) Authentication protocols (b) Message authentication codes

Q.6 Attempt any two:

i. Explain the working of Pretty Good Privacy (PGP) in detail. **5**

ii. Explain the working of Kerberoes in detail. **5**

iii. Explain the working of Packet filter firewalls in detail. **5**

******

Marking Scheme
IT3EI08 Information Security

Q.1	i.	Virus is a computer: (b) Program		**1**
	ii.	A worm _____ modify a program: (b) Does		**1**
	iii.	DES encrypts blocks of _____ bits: (c) 64		**1**
	iv.	There are around _____ rounds in DES:		**1**
	v.	The private key _____ (c) Must be kept secret.		**1**
	vi.	RSA _____ be used for digital signatures: (b) Cannot.		**1**
	vii.	_____ is a message digest algorithm: (c) MD5		**1**
	viii.	A _____ is used to verify integrity of message: (a) Message digest		**1**
	ix.	Kerberoes provides for _____ be used for digital signatures: (b) SSO		**1**
	x.	A packet filter examins _____ packets: (a) All		**1**
Q.2	i.	Any two security features we want to achieve in the cyber world. 1 mark for each	(1 mark * 2)	**2**
	ii.	Ceaser cipher technique Modified Ceaser cipher technique	1.5 marks 1.5 marks	**3**
	iii.	Hill Cipher technique Theory Explanation	 2 marks 3 marks	**5**
OR	iv.	Concept of Stagenography Example	2 marks 3 marks	**5**
Q.3	i.	Block cipher Example	1 mark 1 mark	**2**
	ii.	Working of Data encryption Standard (DES) Diagram Theory Number of rounds Round function	 3 marks 2 marks 1 mark 2 marks	**8**
OR	iii.	Working of Advanced Encryption Standard (AES) Diagram Theory with four points	 2 marks 6 marks	**8**
Q.4	i.	Concept of public key cryptography Theory Diagram	 1.5 marks 1.5 marks	**3**
	ii.	Working of RSA Algorithm Example	4 marks 3 marks	**7**
OR	iii.	Working of Diffie Hellman Key Exchange Theory Example	 4 marks 3 marks	**7**
Q.5	i.	Concept of Digital signatures Diagram	2 marks 2 marks	**4**
	ii.	Working of MD5 algorithm Theory Diagram	 2 marks 4 marks	**6**
OR	iii.	Write short note on: (a) Authentication protocols Two protocols 1.5 marks for each (1.5 marks * 2) (b) Message authentication codes Formula Theory	 3 marks 1 mark 2 marks	**6**
Q.6		Attempt any two:		
	i.	Working of Pretty Good Privacy (PGP) Example	4 marks 1 mark	**5**
	ii.	Working of Kerberoes Diagram Theory	 2 marks 3 marks	**5**
	iii.	Working of Packet filter firewalls Diagram Theory	 2 marks 3 marks	**5**

******