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

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2018

CA5EL28 Network Security

Programme: MCA Branch/Specialisation: Computer Application

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. The network security principle that helps to establish proof of identities. **1**

(a) Integrity (b) Authentication
(c) Access control (d) Confidentiality

ii. A computer program that attaches itself to another legitimate program and causes damage to network or computer system is **1**

(a) Worm (b) Trojan horse
(c) Virus (d) None of these

iii. The matrix theory is used in _____technique. **1**

(a) Hill cipher (b) Playfair cipher
(c) Vigenere cipher (d) Monoalphabetic cipher

iv. The caesar cipher is a _____cipher that has a key of 3. **1**

(a) Transposition (b) Additive
(c) Shift (d) None of these

v. In the DES algorithm, the round key is _____ bit and the Round input is _____bits. **1**

(a) 48,32 (b) 64,32 (c) 56,32 (d) 32,32

vi. The number of tests required to break DES algorithm are **1**

(a) $2.8x10^{14}$ (b) $4.2x10^{9}$ (c) $1.84x10^{19}$ (d) $7.2x10^{16}$

vii. In asymmetric cryptography _____ number of keys required. **1**

(a) 3 (b) 2 (c) 4 (d) 1

P.T.O.

viii. A digital signature is a mathematical technique used to validate _____ and _____ of digital document. **1**

(a) Authenticity, Integrity (b) Authenticity, Confidentiality
(c) Integrity, Confidentiality (d) None of these

ix. IPsec defines two protocols. _____and _____. **1**

(a) AH, SSL (b) PGP, ESP (c) AH, ESP (d) PGP, SSL

x. In SSL Protocol, each upper layer message is fragmented into a maximum of _____ bytes. **1**

(a) 2^{16} (b) 2^{15} (c) 2^{14} (d) 2^{13}

Q.2 i. Discuss various types of legal attacks. **4**

ii. Discuss various security services briefly. **6**

OR iii. How are side channel attacks performed? **6**

Q.3 i. Define homophonic substitution cipher **2**

ii. Why one time pad can only be used once? Justify with an example. **8**

OR iii. Discuss the working of Hill Cipher. **8**

Q.4 i. Define Feistel cipher network. **2**

ii. With the help of an example, distinguish between CBC and CBF modes of operation. **8**

OR iii. Discuss internal structure of IDEA. **8**

Q.5 Attempt any two:

i. Differentiate between symmetric and asymmetric cryptography. **5**

ii. How do you implement digital signatures using hash function? **5**

iii. With p=7; q=11; e=17 and M=8. Perform encryption and decryption using RSA. **5**

Q.6 i. Define IP security. **3**

ii. Discuss SSL handshake protocol. **7**

OR iii. Explain Anomaly based IDS in brief with help of an example. **7**

******

Marking Scheme
CA5EL28 Network Security

Q.1	i.	The network security principle that helps to establish proof of identities. (b) Authentication		**1**
	ii.	A computer program that attaches itself to another legitimate program and causes damage to network or computer system is (c) Virus		**1**
	iii.	The matrix theory is used in _____technique. (a) Hill cipher		**1**
	iv.	The caesar cipher is a _____cipher that has a key of 3. (a) Transposition		**1**
	v.	In the DES algorithm, the round key is _____ bit and the Round input is _____bits. (a) 48,32		**1**
	vi.	The number of tests required to break DES algorithm are (d) $7.2x10^{16}$		**1**
	vii.	In asymmetric cryptography _____ number of keys required. (b) 2		**1**
	viii.	A digital signature is a mathematical technique used to validate _____ and _____ of digital document. (a) Authenticity, Integrity		**1**
	ix.	IPsec defines two protocols. _____and _____. (c) AH, ESP		**1**
	x.	In SSL Protocol, each upper layer message is fragmented into a maximum of _____ bytes. (c) 2^{14}		**1**
Q.2	i.	Two types of legal attacks 2 marks each	(2 marks * 2)	**4**
	ii.	Three security services 2 marks each	(2 marks * 3)	**6**
OR	iii.	Side channel attacks performed		**6**
		Algorithm	3 marks	
		Diagram	3 marks	
Q.3	i.	Homophonic substitution cipher.		**2**
	ii.	One time pad can only be used once	3 marks	**8**
		Justification with an example	5 marks	
OR	iii.	Working of Hill Cipher.		**8**
		Algorithm	4 marks	
		Example	4 marks	
Q.4	i.	Feistel cipher network.		**2**
	ii.	CBC modes + example	4 marks	**8**
		CBF modes + example	4 marks	
OR	iii.	Internal structure of IDEA		**8**
		Algorithm	4 marks	
		Diagram	4 marks	
Q.5		Attempt any two:		
	i.	Four differences b/w symmetric and asymmetric cryptography 1.25 marks each	(1.25 marks * 4)	**5**
	ii.	Implementation of digital signatures using hash function		**5**
	iii.	Encryption and decryption using RSA. Stepwise marking		**5**
Q.6	i.	IP security		**3**
	ii.	SSL handshake protocol.		**7**
		Algorithm	4 marks	
		Diagram	3 marks	
OR	iii.	Anomaly based IDS in brief with help of an example		**7**
		Anomaly	2 marks	
		Algorithm	3 marks	
		Diagram	2 marks	

******