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

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

Faculty of Science

End Sem (Odd) Examination Dec-2018

CA3EL05 Information Security

Programme: BCA 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. Output message in Cryptography is called **1**

(a) Plain text (b) Cipher Text

(c) Plain and cipher (d) None of these

ii. Network security ensures: **1**

(a) Detecting attacks (b) Preventing attacks

(c) Recovering attacks (d) All of these

iii. What is the largest disadvantage of the Symmetric Encryption? **1**

(a) More complex and therefore more time-consuming calculation.

(b) Problem of the secure transmission of the Secret Key.

(c) Less secure encryption function.

(d) Isn't used any more

iv. How many rounds does the AES-256 perform? **1**

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

v. For RSA to work, value of P must be less than value of **1**

(a) p (b) q (c) n (d) r

vi. In an efficient algorithm for factoring large number is discovered, which of the following schemes will be known to be not secure? **1**

(a) Diffie-Hellman (b) RSA

(c) AES (d) None of these

P.T.O.

vii. A digital signature is a **1**

(a) Bit string giving identity of a correspondent
(b) A unique identification of a sender
(c) An authentication of an electronic record by tying it uniquely to a key only a sender knows
(d) An encrypted signature of a sender

viii. A hashing function for digital signature **1**

I. Must give a hashed message which is shorter than the original message
II. Must be hardware implementable
III. Two different messages should not give the same hashed message
IV. Is not essential for implementing digital signature

(a) I and II (b) II and III (c) I and III (d) III and IV

ix. CA Stands for: **1**

(a) Certified Auditing (b) Certification Authorities
(c) Cyper Abuses (d) Certified Automation

x. A firewall may be implemented in **1**

(a) Routers which connect intranet to internet
(b) Bridges used in an intranet
(c) Expensive modem
(d) User’s application programs

Q.2 i. What are threats in information security? **2**
ii. Compare substitution ciphers with transposition ciphers **3**
iii. What are the different types of active and passive attacks? **5**
OR iv. Explain the model of network security. **5**

Q.3 i. Write about strength of DES algorithm. **2**
ii. Describe detailed general structure of DES. Explain with steps. **8**
OR iii. Write down AES parameter and explain AES key expansion. **8**

Q.4 i. What properties must a hash function have to be useful for message authentication? **3**

ii. Explain the Diffie-Hellman key distribution scheme with suitable example. **7**
OR iii. Perform encryption and decryption using the RSA algorithm, p=3; q=11; e=7; M=5 **7**

Q.5 i. Explain Diffie-Hellman key exchange algorithm. **4**
ii. Discuss about digital signature algorithm. **6**
OR iii. Describe the basic concept of Kerberos. **6**

Q.6 Attempt any two:
i. What are web security threats? Give countermeasures of web security threats. **5**
ii. Explain secure electronic transaction **5**
iii. What are the types of firewalls? Explain any one type. **5**

******

Marking Scheme
CA3EL05 Information Security

Q.1	i.	Output message in Cryptography is called		**1**
		(b) Cipher Text		
	ii.	Network security ensures:		**1**
		(d) All of these		
	iii.	What is the largest disadvantage of the Symmetric Encryption?		**1**
		(b) Problem of the secure transmission of the Secret Key.		
	iv.	How many rounds does the AES-256 perform?		**1**
		(c) 14		
	v.	For RSA to work, value of P must be less than value of		**1**
		(c) n		
	vi.	In an efficient algorithm for factoring large number is discovered, which of the following schemes will be known to be not secure?		**1**
		(b) RSA		
	vii.	A digital signature is a		**1**
		(c) An authentication of an electronic record by tying it uniquely to a key only a sender knows		
	viii.	A hashing function for digital signature		**1**
		I. Must give a hashed message which is shorter than the original message		
		II. Must be hardware implementable		
		III. Two different messages should not give the same hashed message		
		IV. Is not essential for implementing digital signature		
		(c) I and III		
	ix.	CA Stands for:		**1**
		(b) Certification Authorities		
	x.	A firewall may be implemented in		**1**
		(a) Routers which connect intranet to internet		
Q.2	i.	Any four types of threats in information security		**2**
		0.5 mark each	(0.5 mark * 4)	
	ii.	Any three comparison substitution ciphers with transposition ciphers 1 mark for each	(1 mark * 3)	**3**
	iii.	Types of active and passive attacks		**5**
		Definition of both	3 marks	
		For example, of both	2 marks	
OR	iv.	Model Design of network security	2 marks	**5**
		Explanation	3 marks	
Q.3	i.	Any for strength of DES algorithm		**2**
		0.5 mark for each	0.5 mark * 4)	
	ii.	General structure of DES	4 marks	**8**
		Proper explanation	4 marks	
OR	iii.	AES parameter	3 marks	**8**
		AES key expansion.	5 marks	
Q.4	i.	At least two properties 1.5 marks each	(1.5 marks *2)	**3**
	ii.	Diffie-Hellman key distribution scheme with diagram	5 marks	**7**
		Example	2 marks	
OR	iii.	Calculation of n =1	1 mark	
		Calculation of f(n) = 1	1 mark	
		Encryption	2.5 marks	
		Decryption	2.5 marks	
Q.5	i.	Diffie-Hellman key exchange algorithm.		**4**
		Formula and explanation		
	ii.	Digital signature algorithm.		**6**
		Diagram	2 marks	
		Explanation	4 marks	
OR	iii.	Basic concept of Kerberos.		**6**
		Explanation with diagram		
Q.6		Attempt any two:		
	i.	Definition of web security threats	2 marks	**5**
		Any three countermeasures of web security threats 1 mark for each	3 marks	
	ii.	Secure electronic transaction		**5**
	iii.	Types of firewalls 0.5 mark each (0.5 mark * 4)	2 marks	**5**
		Explanation of any one type	3 marks	

****