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

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

Faculty of Engineering

End Sem (Odd) Examination Dec-2017

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. In computer security, ______ means that compute system assets can be modified only by authorized parities. **1**

(a) Confidentiality (b) Integrity
(c) Availability (d) Authenticity

ii. A ______ is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs. **1**

(a) Worm (b) Virus (c) Zombie (d) Trap doors

iii. A substitution cipher substitutes one symbol with **1**

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

iv. Cryptography algorithms (ciphers) are divided into **1**

(a) Two groups (b) Four groups
(c) One single group (d) None of these

v. The sender and receiver of the message have the same secret key in- **1**

(a) Asymmetric key cryptography
(b) Steganography
(c) Symmetric Key cryptography
(d) None of these

vi. What is the maximum size of the key in blowfish algorithm? **1**

(a) 256 bits (b) 512 bits (c) 56 bytes (d) 48 bytes

vii. An asymmetric-key (or public-key) cipher uses **1**

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

P.T.O.

viii. In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if message is **1**

(a) Short (b) Long (c) Flat (d) Thin

ix. TCP protocol is used for **1**

(a) Application layer (b) Physical layer
(c) Transport layer (d) None of these

x. A ______ provides privacy for LANs that must communicate through the global Internet. **1**

(a) VPP (b) VNP (c) VNN (d) VPN

Q.2 i. Define Network security **2**

ii. Mention important principles of security. **3**

iii. Write brief note on: Types of attacks on network **5**

OR iv. Explain working of antiviruses. What are its limitations and advantages? **5**

Q.3 i. Write differences between plain text and cipher text. **2**

ii. Explain: Playfair cipher and Hill cipher. **8**

OR iii. Explain: Transposition techniques and Rail-Fence technique. **8**

Q.4 i. Write brief note on : AES **3**

ii. Write brief note on : DES **7**

OR iii. Write brief note on : IDEA **7**

Q.5 i. Explain Knapsack problem. **4**

ii. Write a brief note on Digital signature. **6**

OR iii. Write a short note on : RSA **6**

Q.6 Attempt any two:

i. Explain what is Firewalls? Write how many types of firewall are there? What are its limitations? **5**

ii. Write a brief note on :SSL **5**

iii. What do you mean by Email Security? Explain with examples. **5**

******

CA5EL28 Network Security

Marking Scheme

Q.1 i. In computer security, ______ means that compute system assets can be modified only by authorized parities. **1**

(b) Integrity

ii. A ______ is a program that can infect other programs by modifying them, the modification includes a copy of the virus program, which can go on to infect other programs. **1**

(b) Virus

iii. A substitution cipher substitutes one symbol with **1**

(b) Others

iv. Cryptography algorithms (ciphers) are divided into **1**

(a) Two groups

v. The sender and receiver of the message have the same secret key in- **1**

(c) Symmetric Key cryptography

vi. What is the maximum size of the key in blowfish algorithm? **1**

(c) 56 bytes

vii. An asymmetric-key (or public-key) cipher uses **1**

(b) 2 Key

viii. In Asymmetric-Key Cryptography, although RSA can be used to encrypt and decrypt actual messages, it is very slow if message is **1**

(b) Long

ix. TCP protocol is used for **1**

(c) Transport layer

x. A ______ provides privacy for LANs that must communicate through the global Internet. **1**

(d) VPN

Q.2 i. Define Network security **2**

ii. Mention important principles of security. **3**

iii. Write brief note on: Types of attacks on network **5**

OR iv. Explain working of antiviruses - 2 marks **5**

Limitations – 1.5 marks

Advantages – 1.5 marks

Q.3 i. Write differences between plain text and cipher text. **2**

ii. Explain: Playfair cipher – 4 marks **8**

Hill cipher – 4 marks

OR iii. Explain: Transposition techniques – 4 marks **8**

Rail-Fence technique. – 4 marks

Q.4 i. Write brief note on : AES **3**

ii. Write brief note on : DES **7**

OR iii. Write brief note on : IDEA **7**

Q.5 i. Explain Knapsack problem. **4**

ii. Write a brief note on Digital signature. **6**

OR iii. Write a short note on : RSA **6**

Q.6 Attempt any two:

i. Explain what is Firewalls? – 2 marks **5**

Write how many types of firewall are there? – 2 marks

What are its limitations? – 1 mark

ii. Write a brief note on :SSL **5**

iii. What do you mean by Email Security? – 3 marks **5**

Explain with examples. – 2 marks

******