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

Enrollment No.....

Faculty of Engineering

End Sem (Odd) Examination Dec-2022

CS3EO04 Network Security

Programme: B.Tech. Branch/Specialisation: CSE

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. Rail Fence Technique is an example of _____. **1**

(a) Substitution (b) Transposition

(c) Product cipher (d) Caesar cipher

ii. The sub key length at each round of DES is_____. **1**

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

iii. The _____ algorithm is used to provide one time session key to users. **1**

(a) RSA (b) DES

(c) Diffie-Hellman (d) None of these

iv. What major problem we face while using symmetric encryption technique? **1**

(a) Distribution of secret key

(b) Time consuming

(c) Complexity

(d) Security

v. When a hash function is used to provide message authentication, the hash function value is referred to as _____. **1**

(a) Message field (b) Message digest

(c) Message score (d) Message leap

vi. Hash function is used to produce _____? **1**

(a) Fingerprint of a file

(b) Useful for message authentication

(c) Both (a) and (b)

(d) None of these

P.T.O.

vii. In the _____ layer of OSI model, packet filtering firewalls are implemented. **1**
(a) Application layer (b) Session layer
(c) Presentation layer (d) Network layer

viii. Which layer filters the proxy firewall? **1**
(a) Application (b) Network
(c) Transport (d) None of these

ix. _____ are the special type of programs used for recording and tracking user's keystroke. **1**
(a) Keylogger (b) Trojans (c) Virus (d) Worms

x. This can invade your computer when you open an attachment. **1**
(a) Malware (b) Fishing
(c) Solicitation scam (d) None of these

Q.2 Attempt any two:

i. Explain Playfair Cipher and its rules for the following example: **5**
Ex: Keyword- "Computer"
Plaintext- "Parrot"

ii. Using Hill Cipher technique encryt and decrypt the plain text "Crypto" using the key: **5**

$$K=\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$$

iii. Draw a neat block diagram and explain the general depiction of DES algorithm. **5**

Q.3 Attempt any two:

i. Explain and elaborate Diffie-Hellman key exchange algorithm with the help of example. **5**

ii. Is quantum cryptography better than elliptic curve cryptography? What are the problems in quantum cryptography? **5**

iii. What is the difference between public key and private key cryptosystem? What are the applications of public and private key cryptosystems? **5**

Q.4 Attempt any two:

i. What is a Message Authentication Code (MAC)? What are the types of message authentication codes? Explain. **5**

ii. Why MD5 is faster than SHA1? Write difference between MD5 and SHA1. **5**

iii. What Is Kerberos? How does Kerberos work? Explain Kerberos authentication. **5**

Q.5 i. What are the applications of secure shell? Also describe electronic mail security. **4**

ii. Write short note on: **6**
(a) IP security (b) Encapsulating security payload
(c) Web security

OR iii. Write short note on: **6**
(a) Transport layer security (b) Secure socket layer

Q.6 i. Explain the terms viruses, worms, backdoors, keyloggers and phishing. **4**

ii. Explain what is firewall? Write characteristics of firewall. **6**

OR iii. Write short note on: **6**
(a) Intrusion Detection (b) Password Management

******

Marking Scheme
CS3EO04 Network Security

Q.1	i)	Rail Fence Technique is an example of .....? **b) Transposition**	**1**
	ii)	The sub key length at each round of DES is_____ **b) 56**	**1**
	iii)	The ___ algorithm is used to provide one time session key to users **c) Diffie-Hellman**	**1**
	iv)	What major problem we face while using symmetric encryption technique: **a) Distribution of secret key**	**1**
	v)	When a hash function is used to provide message authentication, the hash function value is referred to as..... **b) Message Digest**	**1**
	vi)	Hash function is used to produce.....? **b) Useful for message authentication**	**1**
	vii)	In the _____ layer of OSI model, packet filtering firewalls are implemented. **d) Network layer**	**1**
	viii)	Which layer filters the proxy firewall? **a) Application**	**1**
	ix)	_____ are the special type of programs used for recording and tracking user's keystroke. **a) Keylogger**	**1**
	x)	This can invade your computer when you open an attachment? **a) Malware**	**1**
Q.2		Attempt any two.	
	i.	Explain Playfair Cipher **(2.5 marks)**and its rules for the following example: Ex: Keyword- "Computer" **(2.5 marks)** Plaintext- "Parrot"	**5**
	ii.	Using Hill Cipher technique encryt**(2.5 marks)** and decrypt the plain text "Crypto" using the Key**(2.5 marks)** : $K=\begin{pmatrix} 7 & 8 \\ 11 & 11 \end{pmatrix}$	**5**
	iii.	Draw a neat block diagram **(2.5 marks)**and explain the general depiction of DES algorithm. **(2.5 marks)**	**5**

Q.3		Attempt any two.	
	i.	Explain and elaborate**(2.5 marks)** Diffie-Hellman key exchange algorithm with the help of example**(2.5 marks)**.	**5**
	ii.	Is quantum cryptography better than elliptic curve cryptography? **(2.5 marks)**What are the problems in quantum cryptography? **(2.5 marks)**	**5**
	iii.	What is the difference between public key and private key cryptosystem? **(2.5 marks)** What are the applications of public and private key cryptosystems? **(2.5 marks)**	**5**
Q.4		Attempt any two.	
	i.	What is a Message Authentication Code (MAC)? **(2.5 marks)**What are the types of message authentication codes? Explain. **(2.5 marks)**	**5**
	ii.	Why MD5 is faster than SHA1? **(2.5 marks)**Write Difference between MD5 and SHA1. **(2.5 marks)**	**5**
	iii.	What Is Kerberos? **(1 marks)** How Does Kerberos Work? **(2 marks)** Explain Kerberos Authentication. **(2 marks)**	**5**
Q.5			
	i.	What are the applications of Secure Shell? **(2 marks)** Also describe electronic mail security. **(2 marks)**	**4**
	ii.	Write Short Note on: **(2 marks each)** a) IP Security b) Encapsulating Security Payload c) Web Security	**6**
OR	iii.	Write Short Note on: **(3 marks each)** a) Transport Layer Security b) Secure Socket Layer	**6**
Q.6			
	i.	Explain the terms Viruses, worms, backdoors, keyloggers and Phishing. **(1 marks each)**	**4**
	ii.	Explain What is Firewall? **(3 marks)**Write characteristics of Firewall. **(3 marks)**	**6**
OR	iii.	Write Short Note on: **(3 marks each)** a) Intrusion Detection	**6**

		b) Password Management	

******