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

Enrollment No.....

Faculty of Engineering

End Sem (Even) Examination May-2022

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. The buffer overflow attack is caused by- **1**

(a) A vulnerability in the design of a networking protocol
(b) A vulnerability in the implementation of a networking protocol
(c) A vulnerability in human behavior
(d) A vulnerability in software

ii. A counter measure to eavesdropping on the communication link is the use of- **1**

(a) A cryptographic checksum
(b) Encryption
(c) A login name and password
(d) A fake identity

iii. Secret key cryptography is synonymous with- **1**

(a) Symmetric key cryptography
(b) Asymmetric key cryptography
(c) Private key cryptography
(d) Quantum cryptography

iv. The block size in 56-bit DES and 128-bit DES are respectively - **1**

(a) 64 and 64 bits
(b) 64 and 128 bits
(c) 128 and 128 bits
(d) 128 and 256 bits

v. The principle advantage of public key cryptography over secret key cryptography is- **1**

(a) Simplified key management (b) Lower chip area
(c) Improved speed (d) Higher security

P.T.O.

vi. The small sub-group attacks can be prevented by- **1**
(a) Authenticating each message in Diffie-Hellman protocol
(b) Use of a safe prime
(c) Use of an appropriate generator
(d) Encryption of each key exchange message

vii. The digital signature provides- **1**
(a) Message confidentiality
(b) Message authentication
(c) Non-repudiation
(d) All of the above

viii. Entity authentication is used to protect against- **1**
(a) Session hijacking
(b) Man-in-the-middle attacks
(c) Dictionary attacks
(d) Reflection attacks

ix. The Kerberos protocol protects against which of the following attacks- **1**
(a) Dictionary attacks
(b) Man-in-the-middle attacks
(c) DDoS attack
(d) DoS attack

x. Task performed by firewall includes- **1**
(a) Access control
(b) Packet integrity checking
(c) IP address spoofing detection
(d) Webpage caching

Q.2 i. Explain the difference between an attack surface and an attack tree. **2**

ii. Briefly define the fundamental security design principles. **3**

iii. Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and a card for account access. Give examples of confidentiality, integrity, and availability requirements associated with the system and, in each case, indicate the degree of importance of the requirement. **5**

OR iv. What is the OSI security architecture? Briefly define categories of security services and security mechanisms. **5**

Q.3 i. What is the difference between a block cipher and a stream cipher? **4**

ii. Which parameters and design choices determine the actual algorithm of a Feistel cipher? What is the purpose of the S-boxes in DES? **6**

OR iii. What is the difference between differential and linear cryptanalysis? Explain the avalanche effect. **6**

Q.4 i. Briefly describe RSA algorithm. **4**

ii. User A and B use Diffie-Hellman key exchange technique a common prime q = 71 and a primitive root $\alpha = 7$. **6**
(a) If user A has private key $X_A = 5$, What is A's Public key Y_A?
(b) If user B has private key $X_B = 12$, What is A's Public key Y_B?

OR iii. Give the main differences between RSA algorithm and Elliptic Curve Cryptography (ECC). **6**

Q.5 i. Explain Digital Signature standards in brief. **4**

ii. What characteristics are needed in a secure hash function? What is the role of a compression function in a hash function? **6**

OR iii. What are some approaches to producing message authentication? What types of attacks are addressed by message authentication? **6**

Q.6 Attempt any two:

i. What is the difference between Kerberos 4 and Kerberos 5? **5**

ii. What is the purpose of the X.509 standard? How is an X.509 certificate revoked? **5**

iii. What is the difference between a packet filtering firewall and a stateful inspection firewall? **5**

******

Marking Scheme - IT3EI08 Information Security

Q.1	i.	The buffer overflow attack is caused by- (d) A vulnerability in software		**1**
	ii.	A counter measure to eavesdropping on the communication link is the use of- (b) Encryption		**1**
	iii.	Secret key cryptography is synonymous with- (a) Symmetric key cryptography		**1**
	iv.	The block size in 56-bit DES and 128-bit DES are respectively - (a) 64 and 64 bits		**1**
	v.	The principle advantage of public key cryptography over secret key cryptography is- (a) Simplified key management		**1**
	vi.	The small sub-group attacks can be prevented by- (b) Use of a safe prime		**1**
	vii.	The digital signature provides- (d) All of these		**1**
	viii.	Entity authentication is used to protect against- (d) Reflection attacks		**1**
	ix.	The Kerberos protocol protects against which of the following attacks- (b) Man-in-the-middle attacks		**1**
	x.	Task performed by firewall includes- (a) Access control		**1**
Q.2	i.	For each difference	(0.5*4) marks	**2**
	ii.	Definition		**3**
		As per explanation	3 marks	
	iii.	Consider an automated teller machine (ATM) in which users provide a personal identification number (PIN) and		**5**
		As per explanation	(2+3) marks	
OR	iv.	OSI security architecture	3 marks	**5**
		Define categories of security services	2 marks	
Q.3	i.	For each difference	(1*4) marks	**4**
	ii.	Parameters and design choices	3 marks	**6**
		Purpose of the S-boxes in DES	3 marks	
OR	iii.	For each difference	3 marks	**6**
		Explain the avalanche effect	3 marks	
Q.4	i.	Briefly describe RSA algorithm	(2+2) marks	**4**
	ii.	User A and B use Diffie-Hellman key exchange technique a common prime q = 71 and a primitive root $\alpha = 7$.		**6**
		(a) If user A has private key X_A	3 marks	
		(b) If user B has private key X_B	3 marks	
OR	iii.	For each difference	(1*6) marks	**6**
Q.5	i.	Explain Digital Signature standards in brief	(2+2) marks	**4**
	ii.	Characteristics are needed in a secure	3 marks	**6**
		Role of a compression function	3 marks	
OR	iii.	Approaches to producing message	3 marks	**6**
		Types of attacks are addressed	3 marks	
Q.6		Attempt any two:		
	i.	For each difference between	(1*5) marks	**5**
	ii.	The purpose of the X.509 standard	2 marks	**5**
		An X.509 certificate revoked	3 marks	
	iii.	For each difference	(1*5) marks	**5**

******