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

Enrollment No.....

Faculty of Engineering

End Sem Examination Dec-2023

IT3EL10 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. Assume suitable data if necessary. Notations and symbols have their usual meaning.

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 secrate key cryptography is- **1**

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

vi. For p = 11 & q = 17 and choose e = 7. **1**
Apply RSA Algorithm where PT message = 88 and thus find the CT.
(a) 23 (b) 64 (c) 11 (d) 54

vii. Which algorithm is message digest algorithm? **1**
(a) DES (b) MD5 (c) IDEA (d) ASA

viii. A digital signature is a mathematical technique which validates? **1**
(a) Authenticity (b) Integrity
(c) Non-repudiation (d) All of these

ix. Which authentication protocol is primarily used for network authentication, especially in a Windows environment? **1**
(a) Kerberos
(b) X.509
(c) Pretty Good Privacy
(d) S/MIME

x. S/MIME is an encryption and authentication protocol primarily used for: **1**
(a) Encrypting and digitally signing email messages
(b) Firewall configuration
(c) User authentication in Windows networks
(d) IP Security (IPsec) configuration

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. Discuss the classical encryption techniques used in information security. Compare and contrast substitution techniques with transposition techniques. **5**
OR iv. Explain the concept of a symmetric cipher model in information security. Describe the key principles of symmetric cryptography and discuss a practical application of symmetric encryption in securing data. **5**

Q.3 i. What is the difference between a block cipher and a stream cipher? **2**
ii. Discuss the concepts of differential and linear cryptanalysis. Explain how these techniques can be used to break block ciphers. **8**
OR iii. Describe the principles of elliptical curve cryptography. Discuss its importance in cryptography. **8**

Q.4 i. Explain the fundamental principles of public key cryptography and how it differs from symmetric key cryptography. **3**
ii. Describe the RSA algorithm in detail, including the key generation process, encryption, and decryption. Discuss the security considerations and applications of RSA in modern cryptography. **7**
OR iii. In the Diffie-Hellman Key Exchange, suppose two parties select prime numbers p = 23 and g = 5. Party A chooses a secret key (a) of 6, while Party B chooses a secret key and (b) of 15. Calculate the shared secret key (K) after the key exchange process. **7**

Q.5 i. Explain the concept of a Message Authentication Code (MAC) and its role in ensuring the integrity and authenticity of a message. **4**
ii. You are given a message and a secret key. Using the HMAC-SHA256 algorithm, calculate the HMAC value for the given message and key. Provide the HMAC value as the result. **6**
Message: "Hello, World!"
Secret Key: "SecretKey123"
OR iii. Describe the differences between a digital signature and a Message Authentication Code (MAC). Explain when and why you would choose one over the other for securing data in a communication system. **6**

Q.6 Attempt any two:
i. Explain the key principles and components of the Kerberos authentication system. Describe how it achieves secure authentication in a networked environment. **5**
ii. Define X.509 and its role in authentication. Discuss the components of an X.509 digital certificate and how it is used to establish trust in electronic communication. **5**
iii. Compare and contrast the authentication mechanisms provided by Pretty Good Privacy (PGP) and S/MIME for securing email communication. **5**

******