Q. Code:444620

Reg. No. | | | | | | | | | | | | | |

B.E./ B.TECH. DEGREE EXAMINATIONS, MAY 2024

Sixth-Semester

IT18603 – INFORMATION SECURITY

(Information Technology)

(Regulation 2018 / 2018A)

TIME:3 HOURS **MAX. MARKS: 100**

COURSE OUTCOMES	STATEMENT	RBT LEVEL
CO 1	Practice secure coding principles.	**3**
CO 2	Implement security controls.	**3**
CO 3	Examine the techniques specific to mitigating the occurrence of common software vulnerabilities.	**4**
CO 4	Test and evaluate secure software	**5**
CO 5	Formulate policies and procedures to manage enterprise security risks.	**6**

PART- A(10x2=20Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	Mention any two categories of threat and attacks that are possible under those threat.	**1**	**2**
2.	List the measures to protect the confidentiality of information.	**1**	**1**
3.	Illustrate the essence of Digital Millennium Copyright Act.	**5**	**3**
4.	Summarize the key areas addressed by Payment Card Industry Data Security Standards.	**5**	**2**
5.	Interpret the information that are typically included in a digital certificate.	**2**	**2**
6.	Articulate the assurances provided by digital signature.	**2**	**3**
7.	Analyze the benefits of implementing a padded cell system in computer security.	**3**	**4**
8.	Correlate two applications where implementing access control are very crucial.	**3**	**4**
9.	The blockchain network is experiencing growth in the number of nodes and transactions. To ensure the integrity and reliability of the network, a robust consensus protocol is necessary. Recommend the essential Requirements for the consensus Protocols.	**4**	**3**
10.	Cryptocurrencies are designed to work as a medium of exchange through a computer network that is not reliant on any central authority, such as a government or bank, to uphold or maintain it. Justify this statement.	**4**	**3**

PART- B (5x 14=70Marks)

		Marks	CO	RBT LEVEL
11. (a)	Apply knowledge of SDLC phases to illustrate how security can be integrated into each stage of the development process.	**(14)**	**1**	**3**

(OR)

(b)	Encrypt "This is the final exam" with Playfair cipher using key "Guidance". Explain the steps involved.	**(14)**	**1**	**3**
12. (a)	Evaluate the implications of non-compliance with key laws on information security, including potential legal consequences and reputational damage.	**(14)**	**5**	**5**
	(OR)			
(b)	Assess the effectiveness of existing policies, procedures, and controls in preventing software license violations and misuse of corporate resources.	**(14)**	**5**	**5**
13. (a)	Demonstrate how plaintext is encrypted into ciphertext using the Data Encryption standard.	**(14)**	**2**	**3**
	(OR)			
(b)	Dexter wants to set up his own public and private keys. He chooses p = 23 and q = 19 with e =283.He encrypts the message "NO" using the RSA algorithm and sends it to Carol. Deduce the encrypted message that is sent to Carol.	**(14)**	**2**	**3**
14. (a)	Demonstrate how each type of firewall filters network traffic based on source/destination IP addresses, port numbers, and protocol types.	**(14)**	**3**	**3**
	(OR)			
(b)	Demonstrate how a honeypot differ from traditional security measures like firewalls and intrusion detection systems.	**(14)**	**3**	**3**
15. (a)	Assess how MD5 operates as a cryptographic hash function, converting arbitrary-length input messages into fixed-length hash values.	**(14)**	**4**	**5**
	(OR)			
(b)	Evaluate the potential impact of blockchain on industries beyond finance and cryptocurrency, highlighting key challenges and considerations for widespread adoption.	**(14)**	**4**	**5**

PART- C (1x 10=10Marks)

(Q.No.16 is compulsory)

		Marks	CO	RBT LEVEL
16.	Suppose Alice and Bob wish to do Diffie-Hellman key exchange. Alice and Bob have agreed upon a prime p = 13, and a generator g = 2. Alice has chosen her private exponent to be a = 5, while Bob has chosen his private exponent to be b = 4. Show the intermediate quantities that both Alice and Bob calculate, as well as the final (shared) secret that Diffie-Hellman produces.	**(10)**	**2**	**3**

****