Q. Code:843559

B. E / B. TECH.DEGREE EXAMINATIONS, MAY 2023

Sixth Semester

IT18603 – INFORMATION SECURITY

(Information Technology)

(Regulation 2018 /Regulation2018A)

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

CO1	Practice secure coding principles.	**3**
CO2	Implement security controls.	**3**
CO3	Examine the techniques specific to mitigating the occurrence of common software vulnerabilities.	**4**
CO4	Test and evaluate secure software.	**5**
CO5	Formulate policies and procedures to manage enterprise security risks.	**6**

PART- A(10x2=20Marks)

(Answer all Questions)

		CO	RBT LEVEL
1.	List down the deliberate acts of Espionage or tresspass.	**1**	**2**
2.	Decode by Ceasar cipher using frequency analysis with shift +6 "KGYEZUHXKGQ"	**1**	**3**
3.	List out the different types of Laws.	**2**	**2**
4.	How is due diligence different from due care?	**2**	**2**
5.	In DES,the statement "if a single bit changed in either plaintext or key produces enormous changes in the ciphertext". Is it True?.If so, Justify with example and name the effect.	**3**	**4**
6.	Is Steganaography is same as Cryptography? Criticize.	**3**	**4**
7.	What common security system is an IDPS most like? In what ways are these systems similar?	**4**	**4**
8.	What is Metasploit Framework? Why is it considered riskier to use than other vulnerability scanning tools?	**4**	**4**
9.	What is the purpose of distributed ledgers?	**5**	**1**
10.	What do you mean by Crypto currency?	**5**	**2**

PART- B (5x 14=70Marks)

		Marks	CO	RBT LEVEL
11. (a)	Consider that an individual threat agent, like a hacker, can be a factor in more than one threat category. If a hacker breaks into a network, copies a few files, defaces a Web page, and steals credit card numbers, how many different threat categories does the attack fall into?.Illustrate each type of threat with a neat sketch.	**(14)**	**1**	**3**

(OR)

(b)	**(i)**	Construct a playfair matrix with the key "occurrence". Make assumption about how to treat the redundant letters in the key. Encrypt the plaintext "balloons"	**(7)**	**1**	**3**
	(ii)	Perform Single columnar and Double columnar Transposition technique on the plaintext "Information Security plays crucial role" with the key (4,3,2,1,6,5,7).	**(7)**		
12. (a)		Illustrate how General computer crime laws will take action on people against computer thefts or information disclosure. Also, discuss about Digital millennium copyright act.	**(14)**	**2**	**3**
		(OR)			
(b)		How does code of Ethics followed in Organizations? Interpret different types of codes of ethics followed by Major IT and InfoSec Professional Organizations.	**(14)**	**2**	**3**
13.(a)	**(i)**	Perform Encryption and Decryption for the string "SECURE" suing RSA Algorithm by considering the values p=17,q=11 and e=3.	**(7)**	**3**	**3**
	(ii)	Users A and B use the Diffie Hellman Key exchange technique, a common prime q=71 and a primitive root α=7.If user A has a private key XA=3,what is A's public key YA? If user B has a private key XB=10,what is B's public key YB? What is the shared secret key?	**(7)**		
		(OR)			
(b)	**(i)**	Illustrate with a neat sketch about the Elliptic curve cryptography.	**(10)**	**3**	**3**
	(ii)	Draw the structure of x.509 v3 certificate.	**(4)**		
14. (a)		Explain with a neat sketch about Host Based IDPS.	**(14)**	**4**	**2**
		(OR)			
(b)		Explain in detail about Scanning and Analysis Tools.	**(14)**	**4**	**2**
15. (a)		Assess the functionality of Secure Hash Algorithm with a neat sketch and differentiate between the different types of SHA.	**(14)**	**5**	**5**
		(OR)			
(b)		Evaluate how Block chain works and explain the concept of Hash chain to Block chain.	**(14)**	**5**	**5**

PART- C (1x 10=10Marks)

(Q.No.16 is compulsory)

		Marks	CO	RBT LEVEL
16.	Demonstrate with a neat sketch about the different states of Encryption and Decryption process of Advanced Encryption Standard (AES).	**(10)**	**3**	**3**

****