Government College of Engineering, Aurangabad

(An Autonomous Institute of Government of Maharashtra)

FYMCA (Sem-II) Class Test

MC1114- Information Security

Max. Marks: 20 Time: 1 Hour

Solve any five questions. 5 marks for each question.

1. Describe image steganography using LSB algorithm.
2. Compare steganography, cryptography and watermarking.
3. i) Construct a Playfair matrix with the key *occurrences*.
   ii) Apply Transposition technique to encrypt the message "this is online exam" with a rail fence technique.
4. Design an output feedback mode operation.
5. Write an algorithm for key expansion of AES algorithm.
6. Describe in brief AddRoundKey transformation of AES cryptosystem. Apply ShiftRows transformation of AES algorithm for the following data.

87	F2	4D	97
EC	6E	4C	90
4A	C3	46	E7
8C	D8	95	A6

prop

Government College of Engineering, Aurangabad

(An Autonomous Institute of Government of Maharashtra)

FYMCA (CBCS) Examination

End Semester Examination July 2023

MC1114- Information Security

Time: 3 Hours 18 JUL 2023 *Max. Marks: 60*

Q1	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Define threats and vulnerability. What is CIA (Confidentiality, Integrity and Availability)?	*CO1*	*K1*	*06*
	B) Compare between stream cipher and block cipher. Why is it important to study Feistel cipher?	*CO2*	*K3*	*06*
	C) Explain spatial domain technique and transfer domain technique of steganography.	*CO2*	*K2*	*06*
Q2	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Which are the five principal services provided by PGP? Explain in brief the authentication and confidentiality operations of PGP.	*CO4*	*K2*	*06*
	B) How packet sniffing works in network layer attack?	*CO5*	*K3*	*06*
	C) What is role of a) cost of security b) performance c) Availability d) security in designing an appropriate network.	*CO5*	*K4*	*06*
Q3	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Which are different block cipher modes of operation? Explain output feedback mode operation. Give application of it.	*CO2*	*K3*	*06*
	B) Compare AES and DES. Which one is bit oriented? Which one is byte oriented?	*CO1*	*K3*	*06*
	C) Which are different block cipher modes of operation? Give application of each. Explain output feedback mode operation.	*CO1*	*K2*	*06*
Q4	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Show AES encryption process with diagram. Which are different AES transformation functions?	*CO2*	*K2*	*06*
	B) Compare MD5 and SHA Hash functions.	*CO2*	*K3*	*06*
	C) What is the need for message authentication? List various techniques used for message authentication. Explain anyone.	*CO2*	*K4*	*06*

Q5	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Compare biometrics authentication method with other authentication methods. Explain different biometric identification techniques.	*CO2*	*K3*	*06*
	B) Which are different techniques used for anti spoofing in biometric system? Write Fuzzy vault algorithm for biometric template security.	*CO5*	*K2*	*06*
	C) Design a fingerprint recognition system using minutiae points.	*CO5*	*K5*	*06*

Note: CO: Course Outcome; B.T. Level: Bloom's Taxonomy Level