Government College of Engineering, Aurangabad
(An Autonomous Institute of Government of Maharashtra)
FYMCA (CBCS) Examination
End Semester Examination July-August 2022
MC1114- Information Security

Time: 3 Hours 15 Minutes 01 AUG 2022 *Max. Marks: 60*

"Verify the Course Code and check whetheryou have got the Correct Question Paper"

N.B.
1. *Attempt all questions.*
2. *Figures to the right indicate full marks*
3. *Assume suitable data if necessary and state it clearly*
4. *Use of Non-Programmable Calculator and Data Sheet is allowed*

Q1	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Define threats and vulnerability. Describe any two attacks.	*CO3*	*K1*	*06*
	B) Compare steganography and cryptography. Explain any one steganography method in detail.	*CO2*	*K3*	*06*
	C) Classify different watermarking techniques based on the following criteria a) Watermark type b) Domain d) Perceptivity e) Host data f) Data extraction	*CO2*	*K2*	*06*
Q2	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) What is importance of auditing and reporting in IRM? How users are given access to IRM-protected data and how that leads to locking down that data so it can be distributed to allow authorized users to access it.	*CO4*	*K3*	*06*
	B) Illustrate the strengths and weaknesses of firewall.	*CO4*	*K3*	*06*
	C) Give applications of IP security. What are benefits of IP security? Which are different usages of IDS in system security.	*CO4*	*K3*	*06*
Q3	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Explain Cipher Block Chaining (CBC) and Cipher Feedback mode (CFB) of operation in cryptography. Compare CFC and CFB.	*CO3*	*K3*	*06*
	B) Illustrate the working of Data Encryption Standard (DES) algorithm.	*CO2*	*K2*	*06*
	C) i) Construct a Playfair matrix with the key 'aurangabad'. ii) Apply Transposition technique to encrypt the message "government engineering college" with a rail fence technique.	*CO2*	*K3*	*06*

Q4	Attempt any TWO	CO	B.T. Level	Marks
	A) Determine the encrypted and decrypted data of message M with RSA algorithm. p = 7, q = 11, e = 7, M = 5	CO2	K4	06
	B) Define authentication. Define message authentication code. Why MAC is used?	CO1	K1	06
	C) What are the principal elements of a public-key cryptosystem? Write down the steps in Diffie-Hellman key exchange algorithm.	CO3	K2	06
Q5	**Attempt any TWO**	CO	B.T. Level	Marks
	A) Determine the requirements of biometric security scheme? What is need of liveness detection system? Explain different biometric identification techniques.	CO2	K2	06
	B) Write Fuzzy vault algorithm for biometric template security.	CO5	K3	06
	C) Explain biometric recognition system with diagram. Which are different types of features used in fingerprint recognition system?	CO5	K2	06

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

Government College of Engineering, Aurangabad
(An Autonomous Institute of Government of Maharashtra)
FYMCA (CBCS) Examination
Re - End Semester Examination NOV – 2022
MC1114- Information Security

Time: 3 Hours 15 Minutes 11 NOV 2022 *Max. Marks: 60*

"Verify the Course Code and check whetheryou have got the Correct Question Paper"

N.B.
1. *Attempt all questions.*
2. *Figures to the right indicate full marks*
3. *Assume suitable data if necessary and state it clearly*
4. *Use of Non-Programmable Calculator and Data Sheet is allowed*

Q1	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Compare watermarking and cryptography. Explain the process of embedding watermark into the host image and extraction of watermark from the image. Explain encryption and decryption process.	*CO1*	*K3*	*06*
	B) Which are the required features of stego-medium? Explain Spatial Domain Techniques and Transform Domain Techniques from steganography techniques.	*CO2*	*K2*	*06*
	C) Explain different threats associated with user authentication over a network or Internet?	*CO1*	*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*	*K1*	*06*
	B) How packet sniffing works in network layer attack? How network layer attacks attempt to compromise network devices and protocol stacks?	*CO4*	*K3*	*06*
	C) Compare Authentication and Authorization. Which are the factors to response to the authentication challenge? Which are different types of authorization systems?	*CO3*	*K3*	*06*
Q3	**Attempt any TWO**	*CO*	*B.T. Level*	*Marks*
	A) Compare between public key cryptosystems and private key cryptosystems. Describe structure of AES algorithm with all transformations in each round.	*CO2*	*K3*	*06*
	B) Illustrate the working of DES algorithm.	*CO2*	*K2*	*06*
	C) Which are different block cipher modes of operation? Explain output feedback mode and	*CO2*	*K2*	*06*

	counter mode of operation.			
Q4	**Attempt any TWO**	***CO***	***B.T. Level***	***Marks***
	A) Determine the encrypted and decrypted data of message M with RSA algorithm. p = 3, q = 11, e = 7, M = 5	***CO5***	***K5***	***06***
	B) Define authentication. Define message authentication code. Why MAC is used?	***CO1***	***K1***	***06***
	C) Define TRNG, PRNG and PRF with example. Which block cipher mode of operations is used as PRNG? How?	***CO2***	***K2***	***06***
Q5	**Attempt any TWO**	***CO***	***B.T. Level***	***Marks***
	A) Explain biometric recognition system with diagram. Determine disadvantages of traditional authentication methods and find requirements of biometric security scheme?	***CO2***	***K2***	***06***
	B) Which are different techniques used for anti spoofing in biometric system? Write Fuzzy vault algorithm for biometric template security.	***CO5***	***K3***	***06***
	C) Which are different types of features used in fingerprint recognition system?	***CO2***	***K2***	***06***

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

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