VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

IBRAHIMBAGH, HYDERABAD-31

Department of Computer Science and Engineering

#### Name of the Course: Cryptography and Network Security

Quiz – III

Name of the Faculty: Dr. K.Srinivas Date: 20-11-2024

Class: B.E 4/4 Time: 10:40am – 11:40am

Section: A

Sem: VII

Academic Year: 2024-25

Note: Answer all the Questions (20 Marks)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q. No. | Description of the question | Marks | BTL  (1/2/3/4/5/6) | Mapped | |
| CO | PO |
|  | Which of the following operations is used to verify data integrity of a message sent across a network?   1. Encryption 2. Decryption 3. Hashing 4. Transposition | 1 | 1 | 3 | 1,2 |
|  | What does 512 indicate in SHA-512 algorithm? | 1 | 2 | 3 | 1,2 |
|  | What is the maximum size of a message that the SHA-512 algorithm can handle? | 1 | 3 | 3 | 1,2,3 |
|  | Which of the following keys is used by user A to provide authentication service using hashing while sending a message from user A to user B?   1. Public Key of A 2. Private Key of A 3. Public Key of B 4. Private Key of B | 1 | 2 | 3 | 1,2 |
|  | What is source repudiation? Which security service addresses this issue? | 1 | 2 | 3 | 1,2 |
|  | What is HMAC? | 1 | 2 | 3 | 1,2 |
|  | It is required to maintain users’ credentials in a database table named ‘passwords’ in a certain web application. It contains two fields namely username and password. For every user, the username is stored, as it is, chosen by the user. How to avoid storing the actual password in the 2nd field and yet facilitate the user authentication? | 3 | 3 | 3 | 1,2,3 |
|  | With the help of a block diagram, explain SHA-512 algorithm. | 3 | 2 | 1 | 1,2 |
|  | With the help of a block diagram, explain CMAC. | 4 | 2 | 1 | 1,2 |
|  | Consider the following cheating in communication from user A to user B using symmetric encryption. User A encrypts message M using a shared secret key and the resulting cipher text is sent to user B. User B ignores the received cipher text, creates his own cheating message, encrypts it using the shared secret key and claims that the resulting cipher text has come from user A. Provide a solution to address this type of cheating. | 4 | 3 | 1 | 1,2,3 |