VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

IBRAHIMBAGH, HYDERABAD-31

Department of Computer Science and Engineering

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

Assignment – 3

Name of the Faculty: Dr. K. Srinivas Date of submission:26/11/2024

Semester: VII Time: 4.20PM

Section: A Academic Year: 2024-25

Set-1(013, 036, 032, 037,012, 020, 063, 002, 015, 029)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q. No. | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | It is required to send a text file over a network channel. Assume that the network channel lacks the facility to ensure data integrity at the receiving end. Provide a solution to implement this facility. | 3 | Apply | 3 | 1,2 |
|  | Write a Python program for implementing a client server application for sending a text file from client to server. Also incorporate the security features. The security features should reflect the solution provided by you for question 1 above.  It is required to send a text file from a client to a server. How do you use the security features provided by your application for the following;   * 1. Send the text file from client to server.   2. Ensure that the server received the file from the original sender but not from an attacker.   3. Ensure that no attacker has changed the file content in the transit. | 2 | Apply | 3 | 1,2 |

Set-2 (001, 003 to 009)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | It is required to send a text file over a network channel. The network channel lacks the facility to ensure data integrity at the receiving end. The user application uses hashing to address the data integrity verification issue as depicted in the following figure.    Discuss man-in-the–middle attack in the above solution. | 3 | Apply | 3 | 1,2 |
|  | With the help of a block diagram, explain CMAC. | 2 | Apply | 3 | 1,2 |

Set-3 (010, 011, 014, 016 to 019, 021)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | 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 | Apply | 3 | 1,2,3 |
|  | Explain how Secure Socket Layer (SSL) is designed to make use of TCP to provide a reliable end-to-end secure service. | 2 | Apply | 4 | 1,2,3 |

Set-4 (22 to 028, 030)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No. | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | What are source repudiation and destination repudiation issues in network communication? How is source repudiation addressed by digital signatures? | 3 | Apply | 3 | 1,2 |
| 2 | With the help of a block diagram, explain SHA-512 algorithm. | 2 | Apply | 3 | 1,2 |

Set-5 (031, 033 to 035, 038, 039 to 041)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | In most of the network security related issues, the third person, with respect to sender and receiver, is an attacker (or cheater). But it is also possible that a sender can cheat the receiver and receiver can cheat the sender. Elaborate on these issues and provide the solutions. | 3 | Apply | 3 | 1,2 |
|  | Explain Machine learning approaches to intrusion detection. | 2 | Apply | 5 | 1,2,3 |

Set-6 (042 to 050)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | 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. | 3 | Apply | 2 | 1,2 |
|  | Explain various e-mail threats. | 2 | Apply | 2 | 1,2 |

Set-7 (051 to 058)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | 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 | Apply | 2 | 1,2 |
|  | With the help of a block diagram, explain CMAC. | 2 | Apply | 4 | 1,2 |

Set-8 (059 to 062, 064, 065)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | In most of the network security related issues, the third person, with respect to sender and receiver, is an attacker (or cheater). But it is also possible that a sender can cheat the receiver and receiver can cheat the sender. Elaborate on these issues and provide the solutions. | 3 | Apply | 4 | 1,2 |
|  | Explain how Secure Socket Layer (SSL) is designed to make use of TCP to provide a reliable end-to-end secure service. | 2 | Apply | 4 | 1,2,3 |

Set-9 (066 to 068, 135, 136, 301)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | What are source repudiation and destination repudiation issues in network communication? How is source repudiation addressed by digital signatures? | 2 | Apply | 3 | 1,2 |
|  | With the help of a block diagram, explain SHA-512 algorithm. | 3 | Apply | 4 | 1,2 |

Set-10(302 to 307)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | 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. | 2 | Apply | 4 | 1,2 |
|  | With the help of a diagram, explain TLS Function P\_hash(secret, seed). | 3 | Apply | 4 | 1,2 |