VASAVI COLLEGE OF ENGINEERING (AUTONOMOUS)

IBRAHIMBAGH, HYDERABAD-31

Department of Computer Science and Engineering

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

Assignment – 2

Name of the Faculty: Dr. K. Srinivas Date of submission:15/10/2024

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 an insecure network channel. How do you provide secrecy and authentication on this channel given that you have an access to DES block cipher crypto system and RSA public key crypto system? Describe your solution with the help of block diagrams. | 3 | Apply | 3 | 1,2 |
|  | Write a Python program for implementing a client server application. 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. Given that the existing network infrastructure is insecure, how do you use the security features provided by your application for the following;   * 1. Send the text file from client to server with confidentiality.   2. Ensure that the server received the file from the original sender but not from an attacker. | 2 | Apply | 3 | 1,2 |

Set-2 (001, 003 to 009)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Encrypt the message M=3 using RSA algorithm given P=3, Q=5 and the public key of receiver is e=7. Also compute private key for the receiver and decrypt the cipher text and verify with the original message. | 3 | Apply | 3 | 1,2 |
|  | Consider the following keys.  PRA: Private Key of A  PUA: Public Key of A  PRB: Private Key of B  PUB: Public Key of B  Which of the following combinations is/are NOT used in network security algorithms?   1. User A encrypts with PRA and user B decrypts with PUA 2. User A encrypts with PUA and user B decrypts with PRA 3. User A encrypts with PRB and user B decrypts with PUB 4. User A encrypts with PUB and user B decrypts with PRB   Which of the above combinations are used in network security algorithms? And what is the security service provided by each legal combination? | 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 |
|  | Explain Elgamal crypto system with the help of the following components;   1. Global public elements 2. Key generation by sender 3. Encryption by public key of receiver   Decryption by private key of receiver | 3 | Apply | 3 | 1,2 |
|  | With the help of neat diagrams, describe Cipher Block Chaining (CBC) mode of Block Cipher Operation. | 2 | Apply | 3 | 1,2 |

Set-4 (22 to 028, 030)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No. | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Explain, with the help of a block diagram, the steps at sender and receiver sides for exchanging a key using Diffie Hellman key exchange algorithm. | 3 | Apply | 3 | 1,2 |
| 2 | With the help of neat diagrams, describe Electronic Code Book. | 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 |
|  | Show that the key computed by both the sender and the receiver produce the same value in Diffie Hellman key exchange algorithm. | 3 | Apply | 3 | 1,2 |
|  | Consider the following keys.  PRA: Private Key of A  PUA: Public Key of A  PRB: Private Key of B  PUB: Public Key of B  Which of the following combinations is/are NOT used in network security algorithms?   1. User A encrypts with PRA and user B decrypts with PUA 2. User A encrypts with PUA and user B decrypts with PRA 3. User A encrypts with PRB and user B decrypts with PUB 4. User A encrypts with PUB and user B decrypts with PRB   Which of the above combinations are used in network security algorithms? And what is the security service provided by each legal combination? | 2 | Apply | 2 | 1,2 |

Set-6 (042 to 050)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Encrypt the message M=3 using RSA algorithm given P=3, Q=5 and the public key of receiver is e=7. Also compute private key for the receiver and decrypt the cipher text and verify with the original message. | 3 | Apply | 2 | 1,2 |
|  | With the help of neat diagrams, describe Cipher Feedback (CFB) mode of Block Cipher Operation. | 2 | Apply | 2 | 1,2 |

Set-7 (051 to 058)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Explain Elgamal crypto system with the help of the following components;   1. Global public elements 2. Key generation by sender 3. Encryption by public key of receiver   Decryption by private key of receiver | 3 | Apply | 2 | 1,2 |
|  | With the help of neat diagrams, describe Cipher Block Chaining (CBC) mode of Block Cipher Operation. | 2 | Apply | 4 | 1,2 |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Describe AES algorithm. | 3 | Apply | 4 | 1,2 |
|  | Consider the following keys.  PRA: Private Key of A  PUA: Public Key of A  PRB: Private Key of B  PUB: Public Key of B  User A wants to send a message M with confidentiality to user B. Which keys are used and for what purpose? | 2 | Apply | 4 | 1,2 |

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

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Explain, with the help of a block diagram, the steps at sender and receiver sides for exchanging a key using Diffie Hellman key exchange algorithm. | 2 | Understanding | 2 | 1,2 |
|  | With the help of neat diagrams, describe Output Feedback (OFB) mode of Block Cipher Operation. | 3 | Apply | 4 | 1,2 |

Set-10 (302 to 307)

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Q.No | Description of the question | Marks | BTL | Mapped | |
| CO | PO |
|  | Show that the key computed by both the sender and the receiver produce the same value in Diffie Hellman key exchange algorithm. | 2 | Apply | 4 | 1,2 |
|  | Explain the traditional block cipher structure. | 3 | Apply | 4 | 1,2 |