**Assignment-2**

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Set –A | | | | |
| S. no | Question | Marks | Cos | BT Level |
|  | Delineate the principle of RSA Algorithm by taking an example. | 5marks | CO4 | Level 5 |
| 2. | Analyse the structure of CMAC. Compare CMAC and HMAC techniques. | 5 marks | CO5 | Level 6 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Set –B | | | | |
| S. no | Question | Marks | Cos | BT Level |
| 1. | Examine the role of Hash functions in Information Security. | 5 marks | CO5 | Level 5 |
| 2. | Delineate the principle of RSA Algorithm by taking an example | 5 marks | CO4 | Level 5 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Set –C | | | | |
| S. no | Question | Marks | COs | BT Level |
| 1. | Throw light on Digital Signature. Elaborate any one Digital Signature Algorithm. | 5 marks | CO4 | Level 5 |
| 2. | Elaborate the various attacks on Diffie Hellman Key Exchange scheme. | 5 marks | CO5 | Level 6 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Set –D | | | | |
| S. no | Question | Marks | COs | BT Level |
| 1. | Delineate SHA-512 hash algorithms along with its features. | 5 marks | CO4 | Level 5 |
| 2. | Depict MD5 Algorithm in detail and compare its performance with SHA-512 | 5 marks | CO5 | Level 6 |

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Set –E | | | | |
| S. no | Question | Marks | COs | BT Level |
| 1. | Comprehend EIGamal Public Key Cryptosystem. | 5 marks | CO4 | Level 4 |
| 2. | Convert <MEET= using Hill cipher with the key matrix  Convert the cipher text back to plaintext. Key= HILL  Convert <MEET= using Hill cipher with the key matrix  Convert the cipher text back to plaintext. Key= HILL  Convert <MEET= using Hill cipher with the key matrix  Convert the cipher text back to plaintext. Key= HILL  Convert <MEET= using Hill cipher with the key matrix  Convert the cipher text back to plaintext. Key= HILL  Delineate Optical Asymmetric Encryption Padding in detail with Encryption and Decryption Process? | 5 marks | CO5 | Level 5 |