|  |  |  |
| --- | --- | --- |
| 1 | A practice of -hoosing a key that is e'tremely random and the algorithm should use the full range of the key+space is called \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_  a. Cipher management  b.Key combination  c.Key management  d.none of above | c |
| 2 | Public key cryptography is also called as \_\_\_\_\_\_\_\_\_  a.Asymmetric key Cryptography  b.Symmetric Key Cryptography  c.Hash key  d.None of above | a |
| 3 | RSA algorithm is the best example of \_\_\_\_\_\_\_  a.Asymmetric key Crytography  b.Symmetric Key Cryptography  c.Hash key Cryptography  d.None of above | a |
| 4 | For RSA to work the value of P must be less then  a. p  b. q  c. n  d. r | c |
| 5 | In symmetric key cryptography, key used by sender and receiver is  a. shared  b. different  c. two keys are used  d. none | a |
| 6 | RSA stands for:  a. Rivest Shamir Aldeman  b. Rock Shane and Amozen  c. Rivest Shane and Amozen  d. Rock Shamir and Adleman | a |
| 7 | Which of the following is also known as key exchange algorithm?  a. RSA.  b. DES.  c. DH.  d. ECC. | c |
| 8 | In which of the following algorithm MiM attack occurs?  a. DES.  b. Triple DES.  c. DH.  d. RSA. | c |
| 9 | In MD5 Message Digest Algorithm takes an input of arbitrary length and \_\_\_\_\_\_\_\_ message digest is produced.  a. 64 bits  b. 128 bits  c. 160 bits  d. 256 bits | b |
| 10 | The input message in MD5 algorithm is produced in \_\_\_\_\_\_  a. 128 bit blocks  b. 256 bit blocks  c. 64 bit blocks  d. 512 bit blocks | d |
| 11 | SHA-1 produces an output of \_\_\_\_\_\_\_\_ message digest  a. 64 bits  b. 128 bits  c. 160 bits  d. 256 bits | c |
| 12 | The man-in-the-middle attack can endanger the security of the Diffie Hellman method if two parties are not  a. Authenticated  b. Joined  c. Submit  d. Separate | a |
| 13 | Function provided by key storage  a. Operational Storage  b. Backup Storage  c. Archive Storage  d. All of above | d |
| 14 | ECC stands for  a. Elliptic Curve Cryptography  b. Euler Curve Cryptography  c. Euclidean Curve Cryptography  d. Eclipse Curve Cryptography | a |
| 15 | Size of key used in ECC is  a. 256 bits  b. 128 bits  c. 512 bits  d. 160 bits | d |
| 16 | In which attack original data gets modified and new malicious code is retransmitted again and again to receiver  a. Masquerade Attack  b. Replay attack (Rewrite)  c. Non Repudiation  d. Traffic Analysis | b |
| 17 | Which of the following is not a Authentication method  a. Hash function  b. Message encryption  c. Message Authentication Code (MAC)  d. Key Generation | d |
| 18 | Which algorithm uses big-endian method to represent the message  a. SHA-1  b. MD5  c. Both a and b  d. None of above | a |
| 19 | Which algorithm uses little-endian method to represent the message  a. SHA-1  b. MD5  c. Both a and b  d. None of above | b |
| 20 | SHA has how many rounds  a. 64  b. 4  c. 20  d. 10 | c |
| 21 | What is used instead of passwords during login session and then can be used in any Kerberos services  a. Key  b. Tickets  c. Header  d. Certificate | b |
| 22 | What will be the value of n according to RSA algorithm if the two prime number a and b are given has 3 and 5  a. 8  b. 15  c. 2  d. 3 | b |
| 23 | The attack which in which Hacker tries all possible private keys is known as  a. Brute force attack  b. Mathematical attacks  c. Timing attacks  d. Chosen Cipher text attack | a |
| 24 | he attack which in which Hacker tries to attack on the properties of RSA algorithm is known as  a. Brute force attack  b. Mathematical attacks  c. Timing attacks  d. Chosen Cipher text attack | d |
| 25 | For given parameters P = 3 ,Q = 19 , e=7,d=31 using RSA algorithm encrypt message M = 6 find the value of Cipher text (C)  a. 3  b. 15  c. 9  d. 12 | c |
| 26. | In public key cryptosystem \_\_\_\_\_ keys are used for encryption and decryption. 1) Same 2) Different 3) Encryption Keys 4) None of the mentioned | 2 |
| 27. | Private key algorithm is used for \_\_\_\_\_ encryption and public key algorithm is used for \_\_\_\_\_ encryption. 1) Messages, session key 2) Session key, messages 3) Can be used for both 4) None of the mentioned | 1 |
| 28. | Which has a key length of 128 bits? 1) IDEA 2) Triple-DES 3) IDEA & Triple-DES 4) None of the mentioned | 1 |
| 29. | Which algorithm can be used to sign a message? 1) Public key algorithm 2) Private key algorithm 3) Public & Private key algorithm 4) None of the mentioned | 1 |
| 30. | Examples of hash functions are 1) MD5 2) SHA-1 3) MD5 & SHA-1 4) None of the mentioned | 3 |
| 31. | Encryption transformations are known as 1) Diffusion 2) Confusion 3) Diffusion & Confusion 4) None of the mentioned | 3 |
| 32. | In transposition, the plaintext letters are 1) Substituted 2) Rearranged 3) Removed 4) None of the mentioned | 2 |
| 33. | RSA is also a stream cipher like Merkel-Hellman. 1) True 2) False | 1 |
| 34. | In the RSA algorithm, we select 2 random large values ‘p’ and ‘q’. Which of the following is the property of ‘p’ and ‘q’? 1) p and q should be divisible by Ф(n) 2) p and q should be co-prime 3) p and q should be prime 4) p/q should give no remainder | 3 |
| 35. | For p = 11 and q = 19 and choose e=17. Apply RSA algorithm where message=5 and find the cipher text. 1) C=80 2) C=92 3) C=56 4) C=23 | 1 |
| 36. | For p = 11 and q = 19 and choose d=17. Apply RSA algorithm where Cipher message=80 and thus find the plain text. 1) 54 2) 43 3) 5 4) 24 | 3 |
| 37. | For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where PT message=88 and thus find the CT. 1) 23 2) 64 3) 11 4) 54 | 3 |
| 38. | For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Cipher message=11 and thus find the plain text. 1) 88 2) 122 3) 143 4) 111 | 1 |
| 39. | The \_\_\_\_\_\_\_\_ method provides a one-time session key for two parties.  1) Diffie-Hellman  2) RSA  3) DES  4) AES | 1 |
| 40. | Which one of the following algorithm is not used in asymmetric-key cryptography?  1.) RSA algorithm  2.) diffie-hellman algorithm  3.) electronic code book algorithm  4.) none of these | 3 |
| 41. | When a hash function is used to provide message authentication, the hash function value is referred to as 1) Message Field 2) Message Digest 3) Message Score 4) Message Leap | 2 |
|  |  |  |
|  |  |  |
| 42. | Message authentication code is also known as 1) key code 2) hash code 3) keyed hash function 4) message key hash function | 3 |
| 43. | What is the number of round computation steps in the SHA-256 algorithm? 1) 80 2) 76 3) 64 4) 70 | 3 |
| 44. | In SHA-512, the message is divided into blocks of size \_\_\_ bits for the hash computation. a) 1024 b) 512 c) 256 d) 1248 | 1 |
| 45. | The message in SHA-512 is padded so that it’s length is 1) 832 mod 1024 2) 768 mod 1024 3) 960 mod 1024 4) 896 mod 1024 | 4 |
| 46. | Which one of the following is not an application hash functions? 1) One-way password file 2) Key wrapping 3) Virus Detection 4) Intrusion detection | 2 |
| 47. | The main difference in MACs and digital signatures is that, in digital signatures the hash value of the message is encrypted with a user’s public key. 1) True 2) False | 2 |
| 48. | Hashed message is signed by sender using  1) His public Key  2) His private Key  3) Receivers public Key  4)Receivers private key | 1 |
| 49. | The responsibility of certification authority for digital signature is to authenticate the  1) hash function used  2) private key of subscribers  3) public key of subscribers  4) key used in DES | 3 |
| 50. | Encryption can be done  1) On any textual data  2) only on ASCII coded data  3) on any bit of string  4) only on mnemonic data | 3 |