| | |
|---|---|
| **Name:**<br>**Enrolment No:** | UPES<br>UNIVERSITY WITH A PURPOSE |

**UNIVERSITY OF PETROLEUM AND ENERGY STUDIES**
**End Semester Examination, July 2020**

**Course: Cryptography and Network Security** **Semester: VI**
**Program: B TECH (CSE) LLB(CL)** **Time 03 hrs.**
**Course Code: CSEG4001** **Max. Marks:**

**Instructions:**

## 60 Multiple Choice questions

| Q. No | Question | Ans-1 | | Ans-2 | | Ans-3 | | Ans-4 | |
|---|---|---|---|---|---|---|---|---|---|
| 1 | An Algorithm used to find the greatest common divisor of two numbers. | Fermat theorem | Incorrect | Euclid | Correct | Euler theorem | Incorrect | None | Incorrect |
| 2 | For a relatively prime the gcd of two number is | Zero | Incorrect | One | Correct | Greater than one | Incorrect | Less than one | Incorrect |
| 3 | A public key cryptosystem is called assymmetric encryption because | Use single key | Incorrect | Use multiple keys | Incorrect | Use two key instead of one | Correct | None of above | Incorrect |
| 4 | The sender and receiver can confirm each other identity and the origin/destination of the information. | Confidentia lity | Incorrect | Authenti cation | Correct | Non-epudiation | Incorrect | Notorization | Incorrect |
| 5 | The requirement for public key cryptography is | Public key | Incorrect | Private key | Incorrect | Both a and b | Correct | None | Incorrect |
| 6 | Which of the following is an advantage of using conventional encryption | It is the most secure | Correct | It is very fast | Incorrect | It is economical | Incorrect | None of the above | Incorrect |
| 7 | To protect the data while in transit on a network, what is used to identify errors and omissions in the information | Record sequence checking | Incorrect | Transmis sion error correctio n | Incorrect | Retransmis sion control | Incorrect | Hash total | Correct |
| 8 | The preventing the unauthorized disclosure of sensitive information | Integrity | Incorrect | Authenti cation | Incorrect | Confidentia lity | Correct | Authorization | Incorrect |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 9 | Attempt to learn or make use of information from system but does not effect system resources | Active attack | Incorrect | Passive attack | Correct | Modification of message | Incorrect | Masquerade | Incorrect |
| 10 | A Hill cipher invented by Lester S. Hill in 1929 is a ..... substituted cipher based on linear algebra. | Simple | Incorrect | Manual | Incorrect | Polygraphic | Correct | Multiple | Incorrect |
| 11 | A transposition or permutation cipher hide the message by. | Replacement | Incorrect | Rearrangement | Correct | Removing | Incorrect | Regular substituting. | Incorrect |
| 12 | In Rail fence technique the message is written in alternate row and read cipher by | Coloumn | Incorrect | Row | Correct | Diagnol | Incorrect | Alternate. | Incorrect |
| 13 | Block cipher principles have contain methods of | Stream cipher | Incorrect | Block cipher | Incorrect | Both a and b | Correct | None | Incorrect |
| 14 | In Feistal structure the encryption and decryption operation is | Similar | Correct | Different | Incorrect | Depends | Incorrect | All of above | Incorrect |
| 15 | Shannon theory of confusion refers to making the relationship between the key and the ciphertext as | Simple | Incorrect | Divisible by 2 | Incorrect | Complex | Correct | Easy to dfferentiate | Incorrect |
| 16 | Simplified DES produce ciphertext as output of | 10 bits | Incorrect | 8 bits | Correct | Depend on key | Incorrect | None. | Incorrect |
| 17 | Simplified DES encryption also takes ..... bit block of plaintext and ..... bit key as input. | 8, 8 | Incorrect | 10, 8 | Incorrect | 8,10 | Correct | 10, 10 | Incorrect |
| 18 | DES have 16 identical stages of processing called | Blocks | Incorrect | Rounds | Correct | Trip | Incorrect | None | Incorrect |
| 19 | Triple DES is another mode of DES takes | 2 key of 64 bit | Incorrect | 3 key of 64 bit | Correct | 2 key of 128 bit | Incorrect | 3 key of 128 bit | Incorrect |
| 20 | The Feistal Function consist of | Expansion, key mixing | Incorrect | Expansion, key mixing, substitution | Incorrect | Expansion, permutation | Incorrect | Expansion, key mixing, substitution and permutation | Correct |
| 21 | The RSA Algorithm can be used for | Public key encryption | Incorrect | Symmetric encryption | Incorrect | Digital signature | Incorrect | Both a and c | Correct |
| 22 | Diffie-Hellman key exchange the first public key algorithm that allow two parties | Shared secret key | Correct | Distribute public key | Incorrect | Both a and b | Incorrect | None | Incorrect |
| 23 | The main role of cryptographic Hash function is in the provision of | Message integrity checks and | Correct | Message integrity checks only | Incorrect | Digital signature only | Incorrect | Signautre algorithm computations | Incorrect |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| | | digital signature | | | | | | | |
| 24 | A digitally signed message offers | Authentication of origin | Incorrect | Integrity of data | Incorrect | Non-repudiation | Incorrect | All of above | Correct |
| 25 | Select the protocol that is utilized for management and negotiation of SA's | MD5 | Incorrect | RC3 | Incorrect | ISA KMP | Correct | IDEL | Incorrect |
| 26 | A digital signature is used for which of the following. | Encrypting | Correct | Identifying | Incorrect | Encapsulating | Incorrect | None of the above | Incorrect |
| 27 | Which of the following does cryptography use to encrypt | Hash | Correct | Digital signature | Incorrect | Token | Incorrect | None of the above | Incorrect |
| 28 | Which of the following is an improvement over the scheme used in digital signatures | Token | Incorrect | One-way Hash function | Correct | Cryptanalysis | Incorrect | None of the above | Incorrect |
| 29 | Digital certificate can provide | Authentication | Correct | Integrity | Incorrect | Encryption | Incorrect | Token verification | Incorrect |
| 30 | Which of the following will a certificate server do. | Accepts and process certificate request | Correct | Accepts digital signature and verifies the same | Incorrect | Generates certificates for all certificates server in Public Network | Incorrect | None of the above | Incorrect |
| 31 | Kerberos provide a service developed as part of projet Athena at MIT | Unauthorised | Incorrect | Distributed | Incorrect | Distributed | Incorrect | Authentication | Correct |
| 32 | Kerberos is a solution of | Computer security | Incorrect | Information security | Incorrect | Network security | Correct | Internet security | Incorrect |
| 33 | The best way to protect message is to encrypt them using program that support. | Kerberos | Incorrect | MD4 | Incorrect | X.509 | Incorrect | S/MIME | Correct |
| 34 | A standard that provide certificate structure | Kerberos | Incorrect | X.509 | Correct | S/MIME | Incorrect | SSL | Incorrect |
| 35 | Envelope data and signed data is a function of | PGP | Incorrect | X.509 | Incorrect | S/MIME | Correct | DAS | Incorrect |
| 36 | Secure socket layer is build on top of | Application layer | Correct | TCP | Incorrect | Internet protocol | Incorrect | Network layer | Incorrect |
| 37 | SSL Handshake protocol exchange ..... using ..... algorithm | Public key, Public key encryption | Incorrect | Private key, Public key encryption | Correct | Public key, Symmetric encryption | Incorrect | Private key, Symmetric encryption | Incorrect |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 38 | TELNET and FTP is the gateway | Application -level | Correct | Packet Router | Incorrect | Circuit level | Incorrect | Bastion host | Incorrect |
| 39 | Proxy server is another name of | Application -level | Correct | Packet Router | Incorrect | Circuit level | Incorrect | Bastion host | Incorrect |
| 40 | A Gateway does not permit end to end TCP connection | Application -level | Incorrect | Packet Router | Incorrect | Circuit level | Correct | Bastion host | Incorrect |
| 41 | AES is a block cipher with block length | 256 bits | Incorrect | 128 bits | Correct | 64 bits | Incorrect | 192 bits | Incorrect |
| 42 | Advanced Encryption standard used in symmetric key is | substitutio n Permutatio n Network | Incorrect | is a fiestal network | Incorrect | not a fiestal network | Incorrect | both a and b | Correct |
| 43 | In a RSA cryptosystem a particular A uses two prime numbers p = 13 and q =17 to generate her public and private keys. If the public key of Ais 35. Then the private key of A is _____ | 11 | Correct | 13 | Incorrect | 16 | Incorrect | 17 | Incorrect |
| 44 | For p = 11 and q = 17 and choose e=7. Apply RSA algorithm where Plaintext message=88 and thus find the Ciphertext | 23 | Incorrect | 64 | Incorrect | 11 | Correct | 54 | Incorrect |
| 45 | Which is the largest disadvantage of the symmetric Encryption? | More complex and therefore more time-consuming calculations . | Incorrect | Problem of the secure transmis sion of the Secret Key. | Correct | Less secure encryption function | Incorrect | Isn't used any more. | Incorrect |
| 46 | Which of the following cipher uses the pair of key for encryption in which the first key is from Z26*and the second key is from Z26. | Vigenere Cipher | Incorrect | Hill cipher | Incorrect | Additive Cipher | Incorrect | Affine Cipher | Correct |
| 47 | Confusion hides the relationship between the ciphertext and the plaintext. | TRUE | Incorrect | False | Correct | May be | Incorrect | Can’t say | Incorrect |
| 48 | A Student gives a check for Rs 100 to buy a used text book. Later she finds that the check was cashed for Rs 1000. Which of the following type of security attack is this. | Masquerad ing | Incorrect | Repudiat ion | Incorrect | Modificatio n | Correct | Snooping | Incorrect |
| 49 | The Multiplicative inverse of 23 in Z100 and 12 in Z26 are. | 87, no Multiplicati ve inverse | Correct | No Multiplic ative inverse, 87 | Incorrect | 13, No Multiplicati ve inverse | Incorrect | No multiplicative inverse,13 | Incorrect |

| | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|
| 50 | The encryption of the message 'Life is full of surprises' through Vigenere cipher using the key as 'HEALTH' is | SMFPBZMYLWHMZYPPKPZI | Correct | SMFLWHMZYPPKPZIZMYLP | Incorrect | SMFPBZMYLWHMZYPPSMF | Incorrect | None of these | Incorrect |
| 51 | Which of the 4 operation are false for each round in AES algorithm i) Substitute Bytesii) Shift Columnsiii) Mix Rowsiv) XOR Round Key | i) only | Incorrect | ii) iii) and iv) | Correct | ii) and iii) | Incorrect | only iv) | Incorrect |
| 52 | Which of the following is not the stream cipher. | Monoalphabetic substitution cipher | Incorrect | Additive | Incorrect | Playfair | Correct | Vegenere | Incorrect |
| 53 | In Double DES cryptographic algorithm, cipher can be attacked by which of the following attack. | Man in middle | Incorrect | Brute force | Incorrect | Meet in middle | Correct | Known plaintext attack | Incorrect |
| 54 | Calculate the GCD of 8376238 and 1921023 using Euclidean algorithm. | 13 | Correct | 12 | Incorrect | 17 | Incorrect | 7 | Incorrect |
| 55 | In which of the following transformation in AES, the interbyte transformation(bits inside byte) takes place. | Sub byte transformation | Incorrect | Shift Row | Incorrect | Mix Column | Correct | Add round key | Incorrect |
| 56 | AES-128 version the how many words are there in key expansion routine. | 40 words | Incorrect | 45 words | Incorrect | 44 words | Correct | 44 words | Incorrect |
| 57 | How many total transformations are in AES-128 version? | 41 | Incorrect | 42 | Incorrect | 43 | Incorrect | 40 | Correct |
| 58 | Which one of the following algorithm is not used in asymmetric-key cryptography? | rsa algorithm | Incorrect | diffie-hellman algorithm | Incorrect | electronic code book algorithm | Correct | dsa algorithm | Incorrect |
| 59 | Another name for Message authentication codes is | cryptographic checksum | Correct | cryptographic codebreak | Incorrect | cryptographic checkbreak | Incorrect | All of above | Incorrect |
| 60 | When a hash function is used to provide message authentication, the hash function value is referred to as | Message Field | Incorrect | Message Score | Incorrect | Message Leap | Incorrect | Message Digest | Correct |