BRAINWARE UNIVERSITY

Term End Examination 2022
Programme – MCA-2020/MCA-2021
Course Name – Cryptography & Network Security
Course Code - MCA304A
(Semester III)

Full Marks : 60 Time : 2:30 Hours

[The figure in the margin indicates full marks. Candidates are required to give their answers in their own words as far as practicable.]

Group-A
(Multiple Choice Type Question) 1 x 15=15

1. *Choose the correct alternative from the following :*

(i) Identify the Caesar cipher is an example of

a) Substitution cipher b) Transposition cipher
c) Both d) None of these

(ii) Conversion of Cipher text into Plain text is called as

a) Encryption b) Decryption
c) Cryptography d) Cryptanalysis

(iii) Identify the mode of operation being used in DES.

a) Cipher Feedback Mode (CFM) b) Cipher Block Chaining (CBC)
c) Electronic Code Book (ECB) d) Output Feedback Mode (OFM)

(iv) Identify the passive attack from the following:

a) Masquerade b) Modification of message
c) Denial of service d) Traffic analysis

(v) Public key cryptosystem is a ____________ cryptosystem. Choose from the following:

a) Symmetric b) Asymmetric
c) Both d) None of these

(vi) Identify the block cipher.

a) Caesar cipher b) Hill cipher
c) Playfair cipher d) None of these

(vii) Select which one is used to verify the integrity of a message.

a) message digest b) decryption algorithm
c) digital envelope d) None of these

(viii) When two different message digests have the same value, it is called as ____________.

a) attack b) collision
c) hash d) None of these

(ix) To decrypt a message encrypted using RSA, we need the ________________.

a) sender's private key b) sender's public key
c) receiver's private key d) receiver's public key

(x) The cryptographic algorithm used in CMAC is

a) Triple DES and AES b) DES
c) RC4 d) AES

(xi) Hashing followed by encryption (H->E) is used by which algorithm?

a) IPSec b) SSH
c) WEP d) SSL/TLS

(xii) Select how many entries are present in each of the S-boxes present in the blowfish algorithm?

a) 256 b) 512
c) 1024 d) 64

(xiii) On Encrypting "cryptography" using Vignere Cipher System using the keyword "LUCKY" we get cipher text

a) nlazeiibljji b) nlazeiibljii
c) olaaeiibljki d) mlaaeiibljki

(xiv) AES has __________ different configurations.

a) two b) three
c) four d) five

(xv) ECB and CBC are ______________ ciphers.

a) block b) stream
c) field d) None of these

Group-B

(Short Answer Type Questions) 3 x 5=15

2. State the disadvantages of Symmetric key cryptography. (3)
3. Write the requirements for Message Authentication. (3)
4. Distinguish between active attack and passive attack with suitable examples. (3)
5. Define cipher text & plain text. (3)

OR

Discuss the concept of Caesar Cipher. (3)

6. Briefly explain virus and worms. (3)

OR

Discuss the algorithm of Rail Fence Technique. (3)

Group-C

(Long Answer Type Questions) 5 x 6=30

7. Write down RSA algorithm. (5)
8. Evaluate the transformation of a message 'We the people of India' using Rail Fence technique. (5)
9. Briefly explain PGP. (5)
10. Illustrate the four main stages in AES operation. (5)
11. State the four principles of security and explain each of them. (5)

OR

Distinguish between Symmetric and Asymmetric Key Cryptography. (5)

12. Write short notes on SSL. (5)

OR

Compare the MD5 and SHA-1 algorithms. (5)