DR. SHYAMA PRASAD MUKHERJEE UNIVERSITY, RANCHI
MASTER OF COMPUTER APPLICATIONS
MODEL QUESTIONS FOR SEMESTER –III

Sub: Network security and cryptography
Paper: CCMCA302

GROUP A

1. Stream ciphers are like_______, except that we trade provable security for a relatively small key.

A. Simple substitution cipher
B. Codebook cipher
C. Double transposition cipher
D. One-time pad

2. A stream cipher takes a key K of n bits in length and stretches it into along ___________.

A. Key stream
B. Search key
C. Key Length
D. Public Key

3. Message ________ means that the sender and the receiver expect privacy

A. confidentiality
B. integrity
C. authentication
D. none of the above

4. Message_____ means that the data must arrive at the receiver exactly as sent
A. confidentiality
B. integrity
C. authentication
D. none of the above

5. Message _______ means that the receiver is ensured that the message is coming from the intended sender, not an imposter

A. confidentiality
B. integrity
C. authentication

D. none of the above

6. Which of the following is the art and science of making and breaking “secret codes”?

A. Cryptology.
B. Cryptography
C. Cryptanalysis
D. Crypto.

7. Which of the following is the making of “secret codes”?

A. Cryptography
B. Cryptology
C. Cryptanalysis
D. Crypto

8. Which of the following is the breaking of “secret codes”?

A. Cryptography.
B. Cryptology
C. Cryptanalysis
D. Crypto.

9. Which of the following is used to encrypt data?

A. Cipher
B. Cryptosystem
C. Plaintext
D. Crypto

10. 16. DES stands for.

a. Default Encryption System.

b. Default Encryption Standard

c. Data Encryption Standard.

d. Data Encryption System.

11. Which of the following’s has the innovative feature of the use of mixed mode arithmetic?

a. Stream cipher.

b. Block cipher.

c. IDEA.

d. DES.

12. The initialization vector in block cipher mode is

a. Secret.

b. Non-secret.

c. Public key.

d. Private Key.

13. Which of the following is also known as key exchange algorithm?

a. RSA. b. DES. c. DH. d. ECC.

14. Which of the following is not a block cipher modes?

a. CBC.

b. ECB.

c. MCB.

d. Electronic codebook.

15. In which of the following the encryption and decryption key are same?

a. Symmetric key cryptography.

b. Asymmetric key cryptography.

c. Public key cryptography.

d. Non secret key.

GROUP B

Direction: Answer any Four **5*4=20**

1. What do you mean by Arithmetic modular with suitable example?
2. Discuss the concept of IDEA in detail with their processing?
3. What do you mean by services of security? How does it relate with Integrity check?
4. Discuss about AES, its structure and their basic operations?
5. List the three different methods of authentication.
6. Explain Block Cipher and their all modes in detail with suitable diagram?
7. Write the algorithm for stream cipher with example?
8. In which technique of cryptography same key is used to encryption and decryption?
9. What are the two major advantages of public key cryptography over symmetric key crypto?
10. Explain the need of passwords?
11. Define firewall?
12. List three classification of firewall?

GROUP C

Direction: Answer any Two **15*2=30**

1. Distinguish between DES and AES.
2. What is security policy? Write a short note on Reflection attack and Mutual Authentication?
3. Explain biometrics and fingerprints in brief?
4. Write algorithm for Diffie- Hellman key generation?
5. Write a short note on Kerberos. What are the various types of Kerberos?