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

Sub: Network security and cryptography
Paper: IT-52(29)

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 a test that human can pass but computers can’t?

a. Firewall. b. Inference control. c. CAPTCHA. d. Multilevel security.

7. For MD5, MD stands for

a. Message digest. b. Messenger digest. c. Message dependent. d. Message decryption.

8. Which of the following is used to detect transmission errors, and not to detect intentional tampering with data?

a. CRC. b. Similar checksum. c. WEP. d. Hash function.

9. Which of the following is very similar to SHA-1?

a. MD3. b. MD4. c. MD5. d. MD1.

10. MD5 produces _______ bits-output.

a. 128. b. 64. c. 256 d. 512.

11. How many bit-output is generated by SHA-1?

a. 128. b. 180. c. 256. d. 512.

12. MD5 is the successor of

a. MD4. b. MD3. c. MD2. d. SHA.

13. ATM or Smart card is an example of

a. Something you know. b. Something you have. c. Something you are. d. Something you want

14. Which of the following is not included in hash function?

a. Authentication. b. Message integrity. c. Fingerprinting. d. Inefficiency.

15. Which of the following Ciphertext is true for RSA?

a. C=M^e mod N. b. C=e^M mod N. c. C=N mod Me. d. C=N mod eM.

GROUP B

Direction: Answer any Four **5*5=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. What is the use of A5/1 algorithm?
6. What do you mean by hash function?
7. Which algorithm is very similar to MD5?
8. List the three different methods of authentication.
9. Define firewall.
10. List three classification of firewall.
11. When are the CAPTCHA being used?
12. Which are the two methods of intrusion detection

GROUP C

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

1. Explain El-Gamal and its uses in cryptography? Also explain its algorithm with example, where prime number (P=23), G= 11 and x=6, Suppose the message is BAG& r=6 4 7 resp.

2. Solve the problem for RSA. Take p=11 and q=3 find the encryption exponent and construct a private and public key?

3. What is security policy? Write a short note on Reflection attack and Mutual Authentication?

4. Explain AES algorithm in brief given an example.

5. How cryptography played an important role in major world event? Justify the statement