(6 pages) **Reg. No. :** .....

Code No. : 8573 **Sub. Code : HCSE 22**

M.Sc. (CBCS) DEGREE EXAMINATION, APRIL 2013.

Second Semester

Computer Science

Elective — NETWORK SECURITY AND CRYPTOGRAPHY

(For those who joined in July 2012 onwards)

Time : Three hours Maximum : 75 marks

PART A — (10 × 1 = 10 marks)

Answer ALL questions.

Choose the correct answer :

1. Which is the most common aspect of information security?

   (a) confidentiality

   (b) integrity

   (c) cryptography

   (d) availability

2. Symmetric key is also called as

   (a) public key (b) secret key

   (c) private key (d) primary key

3. DES stands for

   (a) Data Entry System

   (b) Dynamic Encryption System

   (c) Data Encryption Standard

   (d) Double Entry System

4. RC4 is ———— oriented stream cipher.

   (a) data oriented (b) object oriented

   (c) key oriented (d) byte oriented

5. How many possible attacks on RSA algorithm?

   (a) 3 (b) 2

   (c) 7 (d) 1

6. RSA stands for

   (a) Reverse Search Algorithm

   (b) Rivest, Shanmir, Adleman

   (c) Random Search algorithm

   (d) Reverse Security Algorithm

7. The Digital Signature may be formed by _____ with encrypting message.

(a) public key (b) secret key

(c) private key (d) primary key

8. One time passwords are majorly employed in

(a) Security (b) Industry

(c) Business (d) Banking applications

9. Kerberos protocols are used for

(a) authentication (b) authorization

(c) security (d) communication

10. SSL is mainly used for

(a) online transactions (b) industry

(c) business (d) security

PART B — (5 × 5 = 25 marks)

Answer ALL questions choosing either (a) or (b).

11. (a) Explain various security mechanisms.

Or

(b) Define cipher and list down its categories.

12. (a) Explain DES Structure.

Or

(b) What is the use of Stream Ciphers?

13. (a) Explain RABIN cryptosystem.

Or

(b) Explain the concept of message integrity.

14. (a) What are the various services on Digital Signatures?

Or

(b) Explain the concept of Biometrics.

15. (a) Distinguish between symmetric key and public key.

Or

(b) Explain SSL message formats.

PART C — (5 × 8 = 40 marks)

Answer ALL questions choosing either (a) or (b).

16. (a) Explain the various security attacks.

Or

(b) Write short notes on Substitution ciphers.

17. (a) Distinguish between DES and AES.

Or

(b) What is the use of modern block ciphers?

18. (a) Compare and contrast RSA and RABIN cryptosystem.

Or

(b) Explain Message integrity and authentication.

19. (a) Explain various Digital Signature schemes.

Or

(b) Explain in detail about Zero Knowledge.

20. (a) Explain in detail about symmetric key distribution.

Or

(b) Describe SSL Architecture.

———————