Subject: CRYPTOGRAPHY & NETWORK SECURITY

Time: 3 Hours **JUNE 2011** **Max. Marks: 100**

NOTE: There are 9 Questions in all.

- **Question 1 is compulsory and carries 20 marks. Answer to Q.1 must be written in the space provided for it in the answer book supplied and nowhere else.**
- **The answer sheet for the Q.1 will be collected by the invigilator after 45 Minutes of the commencement of the examination.**
- **Out of the remaining EIGHT Questions answer any FIVE Questions. Each question carries 16 marks.**
- **Any required data not explicitly given, may be suitably assumed and stated.**

Q.1 Choose the correct or the best alternative in the following: (2×10)

a. _________ is designed to protect data from modification, insertion, deletion and replaying by an adversary.

(A) Confidentiality **(B)** Authentication
(C) Data integrity **(D)** Access control

b. The language that we commonly use can be termed as

(A) Pure text **(B)** Simple text
(C) Normal text **(D)** Plain text

c. What will be the value of 27 mod 5?

(A) 2 **(B)** 0
(C) 1 **(D)** 3

d. At the encryption site, DES takes a 64-bit plaintext and creates _______bit cipher text

(A) 56 **(B)** 64
(C) 48 **(D)** 128

e. ________can issue digital certificates

(A) Government **(B)** Bank
(C) CA **(D)** Shopkeeper

f. _________is the most common authentication mechanism.

(A) Smart card **(B)** Password
(C) PIN **(D)** Biometrics

g. The final solution to the problem of key exchange is the use of _______

(A) passport **(B)** digital envelope
(C) digital certificate **(D)** message digest

h. In asymmetric key cryptography, _________ keys are required per communicating party.

(A) 2 **(B)** 3
(C) 4 **(D)** 5

i. The message digest algorithm(s) _______

(A) MD5 **(B)** SHA-1
(C) Both **(A)** and **(B)** **(D)** None of the above

j. __________ increases the redundancy of plain text.

(A) Confusion **(B)** Diffusion
(C) Both **(A)** and **(B)** **(D)** Neither **(A)** nor **(B)**

Answer any FIVE Questions out of EIGHT Questions.
Each question carries 16 marks.

Q.2 a. What do you understand by security services? List and define five security services. **(8)**

b. Define Chinese Remainder Theorem and its application? Using Chinese Remainder Theorem solve:
x== 2 mod 3,
x== 3 mod 5,
x== 4 mod 11,
x==5 mod 16. **(8)**

Q.3 a. Distinguish between monoalphabetic and polyalphabetic cipher. Are all stream ciphers monoalphabetic? Explain. **(10)**

b. A message has 2000 characters. If it is supposed to be encrypted using a block cipher of 64 bits, find the size of the padding and number of blocks. **(6)**

Q.4 a. What is double DES? What is kind of attack on double DES makes it useless? **(8)**

b. Why does the round key generator need a parity drop permutation? **(4)**

c. Describe the three attempted attacks on DES. **(4)**

Q.5 a. Define CFB and list its advantages and disadvantages. **(8)**

b. Write the Encryption algorithm pseudocode for CFB mode. **(8)**

Q.6 a. Define MDC and MAC. Also distinguish between MDC and MAC. **(8)**

b. Compare the compression function of SHA-512 without the last operation of final adding with a Feistel cipher of 80 rounds. Show the similarities and differences. **(8)**

Q.7 a. Compare and contrast attacks on digital signatures with attacks on cryptosystems. **(5)**

b. What is KDC? List the duties of a KDC. **(6)**

c. There are two nonces (R_A, R_B) in Needham- Schroeder protocol, and only three nonces (R_A, R_B, R) in the Otway-Ress protocol. Explain why there is need for extra nonce, R, in the second protocol? **(5)**

Q.8 a. Write short notes on the following: **(5×2 = 10)**

(i) PGP
(ii) S/MIME

b. Compare and contrast key management in PGP and S/MIME. **(6)**

Q.9 a. Define and explain SSL. Also state the purpose of four protocols defined in SSL. **(10)**

b. Show how SSL or TLS reacts to brute-force attack can an intruder use an exhaustive computer search to find encryption key in SSL or TLS? Which protocol is more secure in this respect SSL or TLS? **(6)**