ROLL NO. _____

Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT (NEW SCHEME)

Time: 3 Hours **JUNE 2012** **Max. Marks: 100**

PLEASE WRITE YOUR ROLL NO. AT THE SPACE PROVIDED ON EACH PAGE IMMEDIATELY AFTER RECEIVING THE QUESTION PAPER.

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. If a student breaks into a professor's office to obtain a copy of the next day's test then it is a _____type of security attack

(A) snooping **(B)** modification
(C) denial of service **(D)** none of the above

b. Assuming n is a non negative integer, what will be the gcd(2n+1,n)?

(A) n **(B)** n+1
(C) 1 **(D)** None of the above

c. A private club has only 100 members. How many secret keys are needed if all members of the club need to send secret message to each other?

(A) 100 **(B)** 5900
(C) 4950 **(D)** None of the above

d. What is the block size in DES?

(A) 48 **(B)** 64
(C) 56 **(D)** 72

e. How many exclusive-or operations are used in DES cipher?

(A) 48 **(B)** 64
(C) 56 **(D)** 32

f. The message digest algorithm(s) _____

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

g. In asymmetric key cryptography, _____ keys are required per communicating party.

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

h. How many Exclusive-OR operations are used in DES cipher?

(A) 40 **(B)** 32
(C) 76 **(D)** None of the above

i. Symmetric-key cryptography is based on sharing secrecy; asymmetric-key cryptography is based on_____

(A) personal secrecy **(B)** availability
(C) snooping **(D)** none of the above

j. When a session is resumed, which of the following cryptographic secrets need not to be recalculated?

(A) Pre-master secret **(B)** Authentication keys
(C) Encryption keys **(D)** IVs

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

Q.2 a. What do you understand by information security? Explain three Security goals in information security? **(8)**

b. Distinguish between Z and Z*n*. Which sets can have negative integers? How can we map an integer in Z to an integer in Z*n*? **(8)**

Q.3 a. What are monoalphabetic ciphers? List any three monoalphabetic ciphers. Are all stream ciphers monoalphabetic? Explain. **(8)**

b. Define P-box and discuss three variations of it. Which variation is invertible? **(8)**

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

b. What is triple DES? Discuss two versions of triple DES in use today. **(8)**

Q.5 a. Discuss CTR mode. List its advantages and disadvantages. **(8)**

b. Define CFB mode. State why it is useful? Also show why CFB mode creates a non synchronous stream cipher, but OFB mode creates a synchronous one? **(8)**

Q.6 a. Distinguish between the following:

(i) Message integrity and message authentication.
(ii) MDC and MAC **(8)**

b. What is the maximum and minimum number of padding bits that can be added to a message? Explain. **(8)**

Q.7 a. In the Diffie-Hellman Protocol, g=7, p=23, x=3 and y=5

(i) What is the value of symmetric key?
(ii) What is the value of R1 and R2? **(8)**

b. Define Kerberos and name its server. Briefly explain the duties of each server. **(8)**

Q.8 a. What type of message should be sent in PGP to provide the following security services:
(i) Confidentiality
(ii) Message integrity
(iii) Authentication
(iv) Non-repudiation **(8)**

b. Briefly explain E-mail architecture. **(8)**

Q.9 a. List and give purpose of four protocols. **(8)**

b. Describe how key materials are created from master secret in TLS? Also compare and contrast the handshake protocols in SSL and TLS. **(8)**