ROLL NO. _____

Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT (NEW SCHEME)

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

NOTE: There are 9 Questions in all.

- **Please write your Roll No. at the space provided on each page immediately after receiving the Question Paper.**
- **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. Integrity in the context of information security implies that:

(A) The information needs to be hidden from unauthorized access.
(B) The information needs to be protected from unauthorized change.
(C) The information need to be available to an authorized entity when needed.
(D) All of the above.

b. Which cipher changes the location of the symbols?

(A) Transposition Cipher **(B)** Monoalphabetic Cipher
(C) Shift Cipher **(D)** Stream Cipher

c. Reverse cipher is used:

(A) At the encryption site.
(B) At the decryption site.
(C) Both at encryption and decryption sites
(D) At the transposition site

d. The situation in which two or more different keys can create the same ciphertext from the same plaintext is called:

(A) Weak keys **(B)** Semi-weak keys
(C) Key Clustering **(D)** Key complement.

e. DES encrypts and decrypts a block of:

(A) 48 bits. **(B)** 128 bits.
(C) 66 bits. **(D)** 64 bits

f. Which of these is a stream cipher?

(A) CTR **(B)** CFB
(C) OFB **(D)** All of the above

g. A message digest:

(A) Guarantees that the message has not been changed.
(B) Authenticates the sender of the message
(C) Cannot detect any modification to the message
(D) Provides a proof that the message has been sent by the sender and not by the imposter

h. Digital signature:

(A) Provides message integrity. **(B)** Provide confidentiality for the message
(C) Needs symmetric-key system **(D)** All of the above

i. Pretty good policy (PGP)_____

(A) Is used to provide e-mail with privacy, integrity, and authentication
(B) is used to create a secure e-mail message
(C) is used to store a file for future retrieval
(D) All of the above

j. Alert protocol is used_____

(A) to authenticate the server to the client and the client to the server
(B) to define the process of moving values between the pending and active states.
(C) for reporting errors and abnormal conditions.
(D) to carry message from the upper layer

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

Q.2 a. Explain eight security mechanisms recommended by ITU-T to provide security. **(10)**

b. Explain Passive and Active attacks to information security. Give two examples of these attacks. **(6)**

Q.3 a. Explain two categories of symmetric ciphers. **(8)**

b. Explain the components of modern block cipher. **(8)**

Q.4 a. Explain the four sections of DES function. **(10)**

b. Explain the weaknesses in DES. **(6)**

Q.5 a. Define the ECB mode of operation to encipher text of any size. What are the security issues in ECB mode? **(8)**

b. A person **A** creates a pair of keys and chooses p=397 and q=401. He calculates n=397×401=159197. He then calculates $\phi(n)$= 396×400 =158400. He then chooses e =343 and d = 12007. Show how his friend **B** can send a message to **A** if he knows e and n. **(8)**

Q.6 a. Explain the three categories which a cryptography hash function must satisfy. **(8)**

b. Describe the Merkle-Damgard scheme. Explain the steps used in the scheme. **(8)**

Q.7 a. Describe three kinds of attacks on digital signature. **(8)**

b. Explain public-key infrastructure. List the duties of a PKI. **(8)**

Q.8 a. What is Pretty Good Privacy? Describe the format of public key ring table. **(8)**

b. What is MIME? Describe seven different types of data that MIME allows. **(8)**

Q.9 a. What is the purpose of Secure Socket Layer (SSL) protocol? Describe the services provided by SSL. **(8)**

b. What is the purpose of Record Protocol? Describe the fields in Record protocol general headed. **(8)**