ROLL NO. ___________________

Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT

Time: 3 Hours **DECEMBER 2014** **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. A certificate authority associates a specific _____ with the entity requesting the certificate.

(A) password **(B)** private key
(C) public key **(D)** digital signature

b. Encryption is used to

(A) protect privacy by encoding data **(B)** store data files in a vault
(C) save storage space **(D)** archive system files

c. With respect to security on the Internet, what is the purpose of digital signatures?

(A) To post anonymous messages to bulletin boards
(B) To request receipts for all sent messages
(C) To verify the identity of a message sender
(D) To encrypt mail messages

d. To encrypt a message using public-key encryption scheme, which of the following must be done?

(A) Encrypt the message using the receiver's private key
(B) Encrypt the message using the sender's private key
(C) Encrypt the message using the sender's public key
(D) Encrypt the message using the receiver's public key

e. How does the secure socket layer (SSL) verify the identity of the Web server requesting confidential data?

(A) It uses the server's password **(B)** It uses the server's digital signature
(C) It uses the server's public key **(D)** It uses the server's private key

f. Which of the following must be included on a digital certificate?
(i) The name of the entity and the expiration date
(ii) The number of times the certificate has been viewed
(iii) The digital signature of the certificate authority

(A) I and II only	**(B)** II and III only
(C) I, II and III	**(D)** I and III

g. Which encryption method uses a pair of digital keys?

(A) S-HTTP	**(B)** Active-X
(C) SSL	**(D)** Public key encryption

h. Which of the following is true about private-key encryption schemes?

(A) The sender and the receiver have two private keys, one for encryption and one for decryption.
(B) The sender and the receiver have different private keys.
(C) The sender must notify the receiver before sending a message.
(D) The sender and the receiver use the same private key

i. Of the following processes, which best characterizes the authentication process?

(A) Authorizing use of some resource by a particular user
(B) Logging into a secure site
(C) Establishing a user identity
(D) Verifying that software that is in use is not a pirated copy

j. Which of the following is correct with respect to customers providing highly personal information across the Internet through electronic commerce transactions?

(A) Transactions are relatively secure between the consumer and a company's Web site if the data is encrypted.
(B) It is impossible for anybody to see the transaction on the Internet except for the intended Web site conducting the transaction.
(C) If a transaction is encrypted, any unauthorized parties intercepting the transaction will take ten or more years to decrypt the information.
(D) Customers should never provide charge card information when asked to complete an electronic commerce transaction.

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

Q.2 a. Define Virus. What are the four phases of Viruses? In addition, list out the types of Viruses. **(8)**

b. What are the key principles of security? **(4)**

c. Find the order of all elements in $G = <Z_{10}*, x>$ **(4)**

Q.3 a. Explain following Feistel cipher, polyalphabetic cipher. **(8)**

b. What is affine cipher? Use an affine cipher to encrypt the message “hello” with the key-pair (7, 2). **(8)**

Q.4 a. Explain DES with neat diagram. What is the purpose of the S-boxes in DES? How is the S-box constructed? **(8)**

b. Write about linear profile and round characteristics of DES. **(8)**

Q.5 a. Explain RSA Algorithm. Given the two prime numbers p=61 and q=53, find N, e, and d. **(8)**

b. Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. **(8)**

Q.6 a. What is message digest (HD)? What are two important properties of good HD algorithm? **(8)**

b. Explain length field and padding in SHA_{512}. What is the number of padding bits if the length of the original message is 2590 bits? **(8)**

Q.7 a. Explain concept of digital signature. What is the important aspect that establishes trust in digital signatures? **(8)**

b. The Diffie-Hellman key exchange is susceptible to two attacks. Give an overview of both attacks. **(8)**

Q.8 a. What is MIME? MIME allows seven different types of data. Briefly explain each and its subtypes. **(8)**

b. Explain the concept of key rings in PGP. **(8)**

Q.9 a. Why is the SSL layer positioned between the application layer and the transport layer? **(8)**

b. Differentiate between TLS and SSL. **(8)**