Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT (Current Scheme)

Time: 3 Hours **DECEMBER 2015** **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. _____ is the science and art of transforming messages to make them secure and immune to attacks.
(A) Cryptography **(B)** Cryptoanalysis
(C) Security **(D)** Cryptosystem

b. A combination of an encryption algorithm and a decryption algorithm is called a _____.
(A) Cipher **(B)** Secret
(C) Key **(D)** None of these

c. A _____ is a keyless transposition cipher with N inputs and M outputs that uses a table to define the relationship between the input stream and the output stream.
(A) S-box **(B)** P-box
(C) T-box **(D)** None of these

d. DES has an initial and final permutation block and _____ rounds.
(A) 14 **(B)** 15
(C) 16 **(D)** 32

e. The _____ method provides a one-time session key for two parties.
(A) Diffie-Hellman **(B)** RSA
(C) DES **(D)** AES

f. In asymmetric key cryptography, the private key is kept by
(A) Sender
(B) Receiver
(C) Sender and receiver
(D) All the connected devices to the network

g. Which one of the following is a cryptographic protocol used to secure HTTP connection?
(A) Stream Control Transmission Protocol (SCTP)
(B) Transport Layer Security (TSL)
(C) Explicit Congestion Notification (ECN)
(D) Resource Reservation Protocol

h. Cryptographic hash function takes an arbitrary block of data and returns
(A) Fixed size bit string **(B)** Variable size bit string
(C) Both **(A)** and **(B)** **(D)** None of these

i. _____ is both an authentication protocol and KDC
(A) Hellman key agreement **(B)** Station-to-station key agreement
(C) Kerberos **(D)** Public-key infrastructure

j. The _____ attack can endanger the security of the security of the Diffie-Hellman method if two parties are not authenticated to each other.
(A) Man-in-the middle **(B)** Ciphertext attack
(C) Plaintext attack **(D)** Encrypted text attack

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

Q.2 a. Discuss the security mechanisms recommended by ITU-T (X.800) to provide the security services. **(8)**

b. Define Euclidean algorithm. Write the pseudo code of the algorithm. Use this algorithm to find the greatest common divisor of 2740 and 1760. **(8)**

Q.3 a. What is the pattern in the cipher text of a one-time pad cipher in each of the following cases?
(i) The plaintext is made of n 0's.
(ii) The plaintext is made of n 1's.
(iii) The plaintext is made of alternating 0's and 1's.
(iv) The plaintext is a random string of bits. **(2×4)**

b. Define D-box and briefly describe its three variations. Which variation is invertible? Also define S-box. **(8)**

Q.4 a. Draw the figure of general structure of DES. **(4)**

b. What is difference between a weak key, a semi-weak key and a possible weak key? What is the disadvantage of using a weak key? **(8)**

c. What is the number of rounds in DES? Explain. **(4)**

Q.5 a. Explain Electronic Codebook (ECB) mode? What are the security issues in ECB mode? **(6)**

b. How initialization is done for each frame of encryption in A5/1? **(4)**

c. Write the algorithm inv_knapsackSum for a superincreasing k-tuple. Assume that a = [17, 25, 46, 94, 201, 400] and s = 272 are given. Use the algorithm to show how tuple x is found. **(6)**

Q.6 a. What are the different criterion for a cryptographic hash function? **(8)**

b. What kind of compression function is used in SHA-512? Differentiate it with WHIRLPOOL Cipher Method. **(8)**

Q.7 a. Compare and contrast a conventional signature and a digital signature. **(6)**

b. Define Kerberos and name its server. Briefly explain the duties of each server. **(6)**

c. List the different ways using the public keys can be distributed. **(4)**

Q.8 a. Name the seven types of packets used in PGP and explain the purpose of any four. **(8)**

b. Describe each of the five headers of MIME, with the help of figure that can be added to the original e-mail header section to define the transformation parameters. **(8)**

Q.9 a. Explain the procedure using which cryptographic parameters are generated. **(8)**

b. Draw the format of Record protocol general header that is added to each message coming from the sources and discuss each fields of the header. **(8)**