ROLL NO. ___________________

Code: AC76/AT76/AC132/AT132
Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **December - 2017** **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. The technique of decoding message from non-readable format back to readable format without knowing how they were initially converted from readable format to non-readable format is called
(A) cryptography **(B)** cryptanalysis
(C) cryptology **(D)** cryptogram

b. In the RSA digital signature scheme, ___ is private; ___ and ____ are public.
(A) n, d, e respectively **(B)** e, d, n respectively
(C) d, e, n respectively **(D)** None of these

c. _________is the most common authentication mechanism.
(A) Smart card **(B)** Password
(C) PIN **(D)** Biometrics

d. MIME stands for
(A) Multipurpose Internet Mail Extensions
(B) Multiple Internet Merge Extensions
(C) Multipurpose Internal Mail Extensions
(D) None of these

e. 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 needs to be available to an authorized entity when needed.
(D) All of these

f. How many exclusive-OR operations are used in DES cipher?
(A) 48 **(B)** 64
(C) 56 **(D)** 32

g. Because additive, multiplicative and affine ciphers have _____________ domains, they are very vulnerable to brute force attack.
(A) complex **(B)** small
(C) large **(D)** None of these

h. The residue class is
(A) the set of integers congruent modulo n
(B) the set of all integers such that x = a (mod n)
(C) Both **(A)** and **(B)**
(D) None of these

i. Kerberos is an encryption-based system that uses
(A) secret key encryption **(B)** public key encryption
(C) private key encryption **(D)** data key encryption

j. If (a * b) ≡ (a * c) (mod n) then b ≡ c (mod n)
(A) if a is relatively prime to n **(B)** always
(C) never **(D)** if a and b both are even

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

Q.2 a. Provide the Extended Euclidean Algorithm to find the multiplicative inverse of an integer. Using the algorithm, find the multiplicative inverse of 550 in Z_{1769}. **(8)**

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

Q.3 a. Draw a diagram for depicting general idea of a symmetric-key cipher. **(8)**

b. Briefly describe Affine Cipher. Please draw a diagram to elaborate. **(4+4)**

Q.4 a. What is triple DES? Discuss two versions of triple DES in use today. **(8)**

b. Write a brief overview of differential cryptanalysis. **(8)**

Q.5 a. When modern ciphers are used for encryption in real life applications, different modes of cipher operations are used. Justify the need of different modes of operation. Describe the encryption operation using any one of the modes of operation. **(8)**

b. Describe CTR mode. Write the encryption algorithm for CTR. Also list its advantages. **(2+4+2)**

Q.6 a. Explain the three categories which a cryptography hash function must satisfy. **(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. What is Public-Key Infrastructures (PKI)? List some duties of a PKI. **(8)**

b. Explain the Diffie-Hellman Protocol and its purpose. Use a diagram to further explain. **(8)**

Q.8 a. Describe the reasons for popularity and growth of PGP. **(8)**

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

Q.9 a. What is the purpose of Record Protocol? Describe the fields in Record protocol general headed. **(8)**

b. What steps are involved in the SSL Record Protocol transmission? **(8)**