ROLL NO. _____

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

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **JUNE 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. -7 mod 19 = ?
(A) 26 **(B)** -7
(C) 12 **(D)** 19

b. The _____is the original message before transformation.
(A) Ciphertext **(B)** Plaintext
(C) Secret-text **(D)** Secret Key

c. Which of the following is a transposition ciper?
(A) Caeser cipher **(B)** Vinere cipher
(C) One time pad **(D)** Playfair cipher

d. DES uses a key generator to generate sixteen _____ round keys.
(A) 32 bit **(B)** 48 bit
(C) 54 bit **(D)** 92 bit

e. What is data encryption standard (DES)?
(A) Stream Cipher **(B)** Bit Cipher
(C) Block Cipher **(D)** Product Cipher

f. ECB and CBC are _____ ciphers.
(A) Stream **(B)** Field
(C) Block **(D)** Product

g. One of the most widely used public-key algorithms today is called
(A) ECC **(B)** RSA
(C) ElGamal **(D)** PKI

h. An encoding algorithm that converts an input string into a numerical signature for that string is called
(A) RSA **(B)** A hash code
(C) PKI **(D)** PGP

i. A way of verifying both the sender of information and the integrity of a message is through the use of
(A) Private key encryption **(B)** Public key encryption
(C) Digital certificates **(D)** Digital signatures

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

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

Q.2 a. Illustrate with the help of neat diagram, passive and active security attacks. Discuss the various types of passive and active attacks in brief. **(8)**

b. Discuss Extended Euclidean Algorithm. Find the gcd (a, b) and the values of s and t when a=161 and b=28. **(8)**

Q.3 a. Distinguish between monoalphabetic cipher and polyalphabetic cipher? Which one is more secure and why? List three monoalphabetic ciphers and three polyalphabetic ciphers. **(8)**

b. Explain the working of Ceaser Cipher with a suitable example. **(4)**

c. Differentiate between a block cipher and a stream cipher? Give an example of each one. **(4)**

Q.4 a. Discuss the DES algorithm in context of the following points: **(6×2)**
(i) General structure of DES (ii) DES function

b. Discuss the following: **(2×2)**
(i) Confusion and Diffusion (ii) Avalanche and Completeness Effect

Q.5 a. Describe the working of Cipher Block Chaining (CBC) mode with a suitable diagram. Also, discuss the security issues and error propagation involved in CBC mode. **(8)**

b. Explain the process of key generation, encryption and decryption in RSA. In RSA, if $p = 7, q = 11$ and $e = 13$ then find $n, \phi(n)$ and d. **(8)**

Q.6 a. Discuss the need for message authentication? Explain the concept of MDC and MAC with suitable diagrams. **(8)**

b. Discuss Secure Hash Algorithm (SHA)? List the various versions of SHA. Briefly describe the working of SHA-512. **(8)**

Q.7 a. Define Digital Signature? Discuss the possible types of attacks on Digital Signature. **(8)**

b. Explain Kerberos authentication protocol with a suitable diagram in detail. **(8)**

Q.8 a. Define PGP. List the five services provided by PGP. Explain authentication and confidentiality operational services of PGP with a suitable example. **(8)**

b. Differentiate between MIME and S/MIME. Discuss the role of Cryptographic Message Syntax (CMS) in S/MIME. Briefly define the syntax of encoding schemes of various content type. **(8)**

Q.9 a. How many layers are there in SSL? Explain briefly the four protocols used by SSL to accomplish its tasks. **(8)**

b. Define TLS. How it is different from SSL? How does it generate cryptographic secrets using data-expansion function and pseudorandom function? **(8)**