ROLL NO. _____

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

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **June 2018** **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 art of hiding the code in images is called
(A) Cryptology **(B)** Steganography
(C) Cryptography **(D)** Cryptanalysis

b. (12 – 43) mod 13 = ?
(A) 8 **(B)** 9
(C) -5 **(D)** 5

c. _____is a type of passive attack.
(A) Replay **(B)** Traffic analysis
(C) Masquerade **(D)** Denial of Service

d. Number of possible weak keys in DES.
(A) 32 **(B)** 48
(C) 12 **(D)** 56

e. Input message in cryptography is called
(A) Plaintext **(B)** ciphertext
(C) Special message **(D)** cipher message

f. Man-in-the-middle attack can endanger the security of Diffie-Hellman method if two parties are not.
(A) Authenticated **(B)** Separate
(C) Joined **(D)** None of these

g. Which of the following is not a public-key algorithms
(A) ECC **(B)** RSA
(C) ElGamal **(D)** Diffie-Hellman

h. What is the name of the network attack that floods it with useless traffic?
(A) Trojan horse **(B)** DOS attack
(C) Hijacking **(D)** Spoofing

i. What are MD4 and MD5?
(A) Symmetric Encryption Algorithms
(B) Hashing algorithms
(C) Asymmetric encryption Algorithms
(D) Digital certificates

j. Kerberos is an authentication scheme that can used to implement?
(A) Public key cryptography **(B)** Hash function
(C) Digital signature **(D)** Single sign on

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

Q.2 a. Discuss the role of security services and mechanism. Also define the relation between services and mechanisms. **(8)**

b. Define the Chinese remainder theorem. Write an algorithm in pseudocode for the Chinese remainder theorem. **(8)**

Q.3 a. Distinguish between a stream cipher and a block cipher. Are all stream ciphers monoalphabetic? Explain. **(8)**

b. Explain why modern block ciphers are designed as substitution ciphers instead of transposition ciphers. **(8)**

Q.4 a. Explain the process of key generation in DES with a suitable diagram. **(8)**

b. Discuss the weaknesses of DES in the view of its design principles and cipher keys. **(8)**

Q.5 a. Describe the working of Cipher Feedback (CFB) mode with a suitable diagram. Also, discuss the security issues, error propagation and applications of CFB mode. **(8)**

b. Briefly explain the idea behind the RSA cryptosystem in the context of the following points: **(8)**
(i) What is the one-way function in this system?
(ii) What is the trapdoor in this system?
(iii) Define the public and private keys in this system
(iv) Describe the security of this system.

Q.6 a. Distinguish the following: **(4×2)**
(i) Message integrity v/s Message authentication
(ii) MDC v/s MAC

b. List the main features of the SHA-512 cryptographic hash function. What kind of compression function is used in SHA-512? **(8)**

Q.7 a. Compare and contrast a conventional signature and a digital signature. Discuss the possible types of forgery in digital signatures. **(8)**

b. Write short notes on the following: **(4×2)**
(i) X.509
(ii) Hijacking

Q.8 a. Describe the architecture of an E-mail. How does a PGP can be used to create a secure e-mail message? **(8)**

b. Name seven types of packets used in PGP and explain their purpose. **(8)**

Q.9 a. Illustrate the general architecture of SSL in detail. **(8)**

b. List the services provided by TLS. Describe the purpose of four protocols defined in TLS? **(8)**