ROLL NO. ___________________

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

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **June 2019** **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. What type of security mechanisms are provided by data confidentiality?
(A) Encipherment and routing protocol
(B) Encipherment, digital signature, data integrity
(C) Encipherment, digital signature, authentication exchange
(D) Access control mechanisms

b. Given *a* = 161 and *b* = 28, then the *gcd* (*a*, *b*) is
(A) 7 **(B)** 14
(C) 9 **(D)** 21

c. What is the value of $\phi(240)$?
(A) 12 **(B)** 42
(C) 36 **(D)** 64

d. The expected security of Triple DES is
(A) 112 bits **(B)** 168 bits
(C) 156 bits **(D)** 192 bits

e. Which of the following is not a Block Cipher?
(A) DES **(B)** Blowfish
(C) IDEA **(D)** RC_4

f. The DES suffers from
(A) Meet in-the-middle attack **(B)** Known-Plain text attack
(C) Linear cryptanalysis **(D)** Differential cryptanalysis

g. MD5 is a strengthened version of MD4 that divides the message into blocks of ___________ bits and creates ___________ bit digest.
(A) 256, 128 **(B)** 512, 128
(C) 128, 128 **(D)** 512, 512

h. Which of the following is not directly provided by digital signature?
(A) Message authentication **(B)** Message integrity
(C) Nonrepudiation **(D)** Message confidentiality

i. In SSL, the data is divided into the blocks of ____________ bytes or less.
(A) 2^{10} **(B)** 2^{12}
(C) 2^{14} **(D)** 2^{16}

j. Which of the following SSL version supports TLS 1.0 version?
(A) SSL 1.0 **(B)** SSL 2.0
(C) SSL 3.0 **(D)** None of these

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

Q.2 a. Discuss the five security services (defined by ITU-T) related to the security goals and attacks. **(8)**

b. What is fast exponentiation? Explain Square-and-Multiply method of fast exponentiation with its pseudocode. **(8)**

Q.3 a. What is Playfair Cipher? Apply Playfair Cipher to encrypt the message “THE INDIA IS A GREAT COUNTRY” using a key “MONARCHY”. **(8)**

b. What do you understand by Diffusion and Confusion? How do we achieve them in product ciphers? **(8)**

Q.4 a. What is Avalanche Effect and Completeness Effect in DES? Also, briefly discuss the design criteria of DES. **(8)**

b. Explain the working of triple DES. How does it overcome the problem of Meet-in-the-Middle attack? **(8)**

Q.5 a. Explain the working of Cipher Block Chaining (CBC) Mode. Also, discuss the primary security issues of CBC Mode. **(8)**

b. What is Asymmetric key cryptosystem? Explain the process of key generation, encryption and decryption in RSA. Also explain, why RSA is secure? **(8)**

Q.6 a. State the basic difference between message integrity and message authentication. Discuss the criteria of a cryptographic hash function. **(8)**

b. What do you understand by Secure Hash Algorithm? Briefly explain the working of SHA-512. **(8)**

Q.7 a. What is Digital Signature? Discuss various types of possible attacks on digital signature. **(8)**

b. List the duties of a KDC. Also, define a session key and show how a KDC can create a session key between two parties? **(8)**

Q.8 a. Explain, how PGP establishes Introducer Trust Levels, Certificate Trust Levels and Key Legitimacy. **(8)**

b. State the differences between MIME and S/MIME. List the cryptographic algorithms which receiver must support in S/MIME. **(8)**

Q.9 a. Discuss the need for security services at the transport layer of Internet Protocol. **(8)**

b. Define the general structure of TSL and highlight the differences between TSL and SSL protocol. **(8)**