ROLL NO. _____

Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT

Time: 3 Hours **DECEMBER 2013** **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 designed to protect data from disclosure attack.

(A) data confidentially **(B)** authentication
(C) data integrity **(D)** access control

b. Symmetric-key cryptography is based on _____secrecy.

(A) personal **(B)** professional
(C) sharing **(D)** non-sharing

c. Non-feistel ciphers uses _____components.

(A) invertible **(B)** non-invertible
(C) both **(A)** & **(B)** **(D)** none of these

d. DES uses ___rounds of Feistel ciphers.

(A) 48 **(B)** 16
(C) 56 **(D)** 24

e. Which (of the following) a digital signature cannot provide directly, we still need encryption/decryption?

(A) Message authentication **(B)** Message integrity
(C) Nonrepudiation **(D)** Message confidentiality

f. A digital signature is

(A) scanned signature **(B)** signature in binary form
(C) encrypting information **(D)** handwritten signature

g. SHA-512 creates ____ 64-bit words message digest from a multiple-[illegible] message where each block is 1024 bits

(A) five **(B)** eight
(C) six **(D)** ten

h. Transposition ciphers include keyless, keyed and _____transposition ciphers.

(A) double **(B)** playfair
(C) Enigma **(D)** additive

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. To prove the integrity of the message and the data origin authentication, we need _____

(A) MDC **(B)** MAC
(C) Both **(A)** & **(B)** **(D)** None of these

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

Q.2 a. Define and explain briefly four different services of security- Confidentiality, Integrity, Authentication and Non-repudiation. **(6)**

b. Solve the equation $14x \equiv 12 (\text{mod} 18)$, through two methods. **(4)**

c. Find an integer that has a remainder of 3 when divided by 7 and 13, but is divisible by 12. Verify your answer. **(6)**

Q.3 a. Use the additive cipher with key =15 to decrypt the message "WTAAD". **(4)**

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

c. Define a S-Box and mention the necessary condition for a S-Box to be invertible. What is the difference between Linear & Non-Linear S- Boxes? **(4)**

Q.4 a. Describe briefly two desired properties of a block cipher. How do you rate DES with regard to these two properties? **(4)**

b. What is triple DES? What is triple DES with two keys? What is triple DES with three keys? Draw a diagram of TRIPLE DES with two keys. **(12)**

Q.5 a. Explain CBC mode. Also list its advantages and disadvantages. **(6)**

b. Briefly explain the idea behind the RSA cryptosystem. What is the trapdoor and one-way function in this system? **(10)**

Q.6 a. Distinguish between HMAC and CMAC. **(4)**

b. What is the minimum & maximum number of padding bits that can be added to a message? Explain. **(6)**

c. "Before processing, each message block must be expanded" Explain. **(6)**

Q.7 a. Compare and contrast existential and selective forgery. **(4)**

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

c. What is the need for a key-distribution centre (KDC)? **(4)**

Q.8 a. Explain how Bob and Alice exchange the secret key for encrypting messages in PGP. **(8)**

b. What is CMS? Name all the content types defined by CMS and their purposes. **(8)**

Q.9 a. Explain any four key-exchange methods to establish pre-master secret in SSL. **(6)**

b. Distinguish between a session and a connection. **(4)**

c. How "Records protocol" in TLS is different from that in SSL? Discuss. **(6)**