ROLL NO. _____

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

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **December 2016** **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 not provided by encipherment.
(A) Confidentiality **(B)** Data Integrity
(C) Non-repudiation **(D)** Authentication

b. (-19 mod 14) is _____.
(A) -5 **(B)** 9
(C) 11 **(D)** 5

c. _____ attack is based on the inherent characteristics of plaintext language
(A) Brute-force **(B)** Frequency analysis
(C) Known plaintext **(D)** Kasiski test

d. Rotor cipher is a _____
(A) Substitution cipher **(B)** Transposition cipher
(C) Block cipher **(D)** Stream cipher

e. The major attack on double DES is _____.
(A) Brute force attack
(B) Known-Plain text attack
(C) Differential Cryptanalysis
(D) Meet in-the-middle attack

f. Plain text and cipher text are treated as _____ in asymmetric key cryptography.
(A) Character **(B)** Integer
(C) Alphabet **(D)** Alpha-numeric

g. _____ works on block mode.
(A) CFB **(B)** OFB
(C) CCB **(D)** CBC

h. Through public key infrastructure, the sender and receiver of an electronic communication are authenticated through the exchange of ____.
(A) Private keys **(B)** Symmetric keys
(C) Digital certificates **(D)** Hash values

i. Which of the following is a valid server-role in a Kerberos authentication system?
(A) Ticket granting server **(B)** Security assertion server
(C) Authentication agent **(D)** Token issuing system

j. For session key encryption in S/MIME, the sender and receiver must support _____.
(A) Triple DES **(B)** RSA
(C) SHA-1 **(D)** HMAC

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

Q.2 a. Define Euler's Totient function (φ). **(2)**

b. Find φ(26), φ(200) **(4)**

c. Explain any 5 security services provided by ITU-T and mechanisms to implement these services. **(10)**

Q.3 a. Which category of encryption does Playfair cipher belongs to? **(1)**

b. Consider the key used by Playfair cipher as "KEYWORD". Find the matrix formed by the cipher. Encrypt the following messages and provide the cipher text. Use Q as bogus character, if needed.
(i) Why dont you
(ii) Come to the window
(iii) the big wheel **(10)**

c. With the appropriate diagram of Fiestel cipher, prove that encryption and decryption of the cipher are inverses of each other. **(5)**

Q.4 a. Briefly explain how diffusion and confusion are provided in DES using the S-boxes and P-boxes. Why does DES require 16 Rounds? **(10)**

b. What is a weak key used in DES? What is the disadvantage of using a weak key? Briefly explain. **(6)**

Q.5 a. Describe the encryption operation using CFB mode of operation. If a bit error occurs in cipher text during transmission, how far does the error propagate in CFB mode? What type of applications use CFB? **(10)**

b. Explain Timing Attack on RSA and any one method to thwart the attack. **(6)**

Q.6 a. How many criteria are to be satisfied by a cryptographic hash function to be used for checking the integrity of a message? Explain each and demonstrate the same using appropriate diagrams. **(10)**

b. Briefly explain the outline of compression function of SHA-512. **(6)**

Q.7 a. Can we use a secret (symmetric) key to both sign and verify the signature? Why? Give justification. **(4)**

b. In Kerberos V4, the password of Alice is not transmitted in clear or encrypted form to the Ticket Granting server. Then, how can the user authentication be done by the system? **(4)**

c. What is the deficiency of distributing the public key certificates by a Certification Authority? How does X.509 overcome this deficiency? Explain the format of X.509 certificate. **(8)**

Q.8 a. How does PGP provide the following security services to Email?
1. Message Integrity
2. Confidentiality
3. Code Conversion
4. Non-repudiation.

With a diagram provide the details. **(11)**

b. Explain the Authenticated-Data content type used in S/MIME with appropriate diagram. **(5)**

Q.9 a. Suppose an attacker records the entire SSL session between a bank and its customer. Can the attacker replay the session to the bank and potentially cause the customer to pay the bill twice? If yes, explain why? If not, what prevents this form of replay in SSL? **(6)**

b. Explain any six differences between SSL and TLS. **(6)**

c. Why does a session get separated from a connection inside a session in SSL with different state information? **(4)**