ROLL NO. _____

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

AMIETE – CS/IT (Current & New Scheme)

Time: 3 Hours **DECEMBER 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 major attack on double DES is
(A) Brute force attack **(B)** Known-Plain text attack
(C) Meet in-the-middle attack **(D)** Differential Cryptanalysis

b. The model to create, distribute and revoke certificates based on X.509 is defined as
(A) Ticket-Granting Server **(B)** kerberos
(C) station-to-station protocol **(D)** Public Key Infrastructure

c. _____ is the science and art of transforming messages to make them secure and immune to attacks.
(A) Cryptoanalysis **(B)** Cryptography
(C) Security **(D)** Cryptosystem

d. _____ is both an authentication protocol and KDC
(A) Kerberos **(B)** Station-to-station key agreement
(C) Hellman key agreement **(D)** Public-key infrastructure

e. Which of the following statement(s) is correct. Pretty good privacy is used
(A) for personal email.
(B) to provide conversion to radix 64 code.
(C) to provide email with privacy, integrity and authentication.
(D) to send only unencrypted messages.

f. Which encryption method uses a pair of digital keys?
(A) S-HTTP **(B)** Public key encryption
(C) SSL **(D)** Active-X

g. If $(a*b)\equiv(a*c)(\text{mod}\,n)$ then $b\equiv c\,(\text{mod}\,n)$
(A) if a and b both are even **(B)** always
(C) never **(D)** if a is relative prime to n

h. Which (of the following) a digital signature cannot provide directly? We still need encryption/decryption.
(A) Message confidentiality **(B)** Message integrity
(C) Nonrepudiation **(D)** Message authentication

i. What is the value of $\phi(240)$?
(A) 4 **(B)** 64
(C) 6 **(D)** 16

j. The message digest algorithm(s) is/are
(A) MD5 **(B)** SHA-1
(C) Both **(A)** and **(B)** **(D)** None of these

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

Q.2 a. Briefly explain different security goals and the different types of attacks which threatens these goals. **(10)**

b. What is meant by Quadratic Residues (QR) and Quadratic Non Residues (QNR)? **(6)**

Q.3 a. Suppose that we have a block cipher where n = 64. If there are 10 1's in the ciphertext, how many trial-and-error tests does Eve need to do to recover the plaintext from the intercepted ciphertext in each of the following cases? **(8)**
(i) The cipher is designed as a substitution cipher.
(ii) The cipher is designed as a transposition cipher.

b. Explain the components of modern block cipher. **(8)**

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. Describe briefly two desired properties of a block cipher. How do you rate DES with regard to these two properties? **(6)**

Q.5 a. Discuss CTR mode. List its advantages and disadvantages. **(8)**

b. Describe the advantages and disadvantages of symmetric and asymmetric key cryptography. **(8)**

Q.6 a. Discuss the algorithm of SHA-512. Support your answer with suitable diagram. **(8)**

b. What are the motivations behind developing MACs based on hash functions? Describe design objectives and overall operation of HMAC. **(8)**

Q.7 a. Compare and contrast a conventional signature and a digital signature. **(6)**

b. Define Kerberos and name its server. Briefly explain the duties of each server. **(6)**

c. Draw a diagram depicting the concept of CA. **(4)**

Q.8 a. If e-mail is one-time activity, how can the sender and receiver agree on a cryptographic algorithm to use for e-mail security? If there is no session and no handshaking to negotiate the algorithms for encryption/decryption and hashing, how can the receiver know which algorithm the sender has chosen for each purpose? **(8)**

b. Compare and contrast key management of PGP and S/MIME. **(8)**

Q.9 a. Why is the SSL layer positioned between the application layer and the transport layer? **(8)**

b. How "Records protocol" in TLS is different from that in SSL? Discuss. **(8)**