ROLL NO. _____

Code: AC76/AT76 Subject: CRYPTOGRAPHY & NETWORK SECURITY

AMIETE – CS/IT

Time: 3 Hours **JUNE 2014** **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. Guarding against improper information modification or destruction, including ensuring information nonrepudiation and authenticity is called _____.

(A) Confidentially **(B)** Availability
(C) Integrity **(D)** None of these

b. A _____is one that encrypts a digital data stream one bit or one byte at a time.

(A) block cipher **(B)** stream cipher
(C) Feistel block cipher **(D)** non-feistel block cipher

c. If (a * b) ≡ (a * c) (mod n) then b ≡ c (mod n)

(A) if a is relatively prime to n **(B)** always
(C) never **(D)** if a and b both are even

d. Which of the following is/are ingredients of public-key encryption scheme?

(A) Plaintext **(B)** Ciphertext
(C) Public and private keys **(D)** all of these

e. A possible approach to attack the RSA algorithm involves trying all possible private keys. This is known as _____.

(A) Brute force **(B)** Mathematical attack
(C) Timing attack **(D)** Chosen ciphertext attack

f. _____is similar in structure to that of CFB mode.

(A) CFM mode **(B)** OFB mode
(C) CTR mode **(D)** none of these

g. SHA-512 algorithm takes as input a message with a maximum length of less than 2128 bits and produces as output a _____message digest.

(A) 1024-bit **(B)** 256-bit
(C) 512-bit **(D)** not defined

h. Typically, PKI implementations make use of _____certificates.

(A) X.508 **(B)** X.506
(C) X.509 **(D)** X.507

i. Which of the following is not a MIME header field?

(A) Content-Type **(B)** Content-ID
(C) Content-Description **(D)** Content-decoding

j. Kerberos is a/an _____designed for use in a distributed environment.

(A) authentication service **(B)** digital signature service
(C) 512 algorithm **(D)** None of these

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

Q.2 a. Differentiate between active and passive attacks. List some passive attacks and some active attacks. **(6)**

b. Determine gcd(24140, 16762) **(4)**

c. The example used by Sun-Tsu to illustrate the CRT was
$x \equiv 2 \pmod 3$; $x \equiv 3 \pmod 5$; $x \equiv 2 \pmod 7$
Solve for x. **(6)**

Q.3 a. What are the essential ingredients of a symmetric cipher? Explain briefly. **(5)**

b. Define a P-box and list its three variations. Which variation is invertible? **(5)**

c. Explain synchronous stream cipher and one-time pad. Why one-time pad cipher is not practical? **(6)**

Q.4 a. The criteria used in the design of DES focused on the design of the S-boxes and on the P function that takes the output of the S-boxes. List and briefly explain these criterions. **(10)**

b. Explain the avalanche effect using a suitable example. **(6)**

Q.5 a. Describe CTR mode. Write the encryption algorithm for CTR. Also list its advantages. **(3+4+3)**

b. What is a one-way function? What is a trap-door one-way function? Give an example of each. **(6)**

Q.6 a. What are the motivations behind developing MACs based on hash functions? Describe design objectives and overall operation of HMAC. **(8)**

b. Explain procedure of Message Digest (MD) generation using SHA-512. **(8)**

Q.7 a. Describe briefly the kind of attacks on digital signatures. **(6)**

b. What problem was Kerberos designed to address? In the context of Kerberos, what is a realm? **(4)**

c. Describe man-in-the-middle attack. How can such vulnerabilities be overcome? **(6)**

Q.8 a. Describe briefly the five header fields defined in MIME. **(5)**

b. How does PGP use the concept of trust? Describe the operation of the trust processing. **(6)**

c. Describe one-way e-mail exchange architecture. **(5)**

Q.9 a. Briefly describe Data-expansion and Pseudorandom function in TLS. **(4)**

b. Briefly describe the list of parameters for a session state in SSL. **(6)**

c. What steps are involved in the SSL Record Protocol transmission? **(6)**