

Time: 3 Hours

DECEMBER 2012

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 goals of security are

- (A) confidentiality and availability
- (B) integrity and availability
- (C) integrity and confidentiality
- (D) integrity, confidentiality and confidentiality

b. What will be the value of $36 \bmod 12 =$

- (A) 3
- (B) 0
- (C) 1
- (D) none of these

c. Because additive, multiplicative and affine ciphers have _____ domains, they are very vulnerable to brute force attack.

- (A) complex
- (B) small
- (C) large
- (D) none of these

d. The round-key generator creates sixteen _____ bit keys out of a _____ bit cipher key

- (A) 24, 56 respectively
- (B) 56, 48 respectively
- (C) 48, 56 respectively
- (D) none of these

e. If x and y want to communicate seemly with each other y must know.

- (A) X's private key
- (B) X's public key
- (C) Y's private key
- (D) Y's public key

Code: AC76/AT76

Subject: CRYPTOGRAPHY & NETWORK SECURITY

- f. Expansion for CFB is:
- (A) Cryptography Feed Back (B) Cryptic Face Book
(C) Cipher Feed Book (D) none of these
- g. Alice encrypts two plaintexts, P1 and P2, and encrypts them with $e = 3$ and sends C1 and C2 to Bob. If P1 is related to P2 by linear function, then Eve can recover P1 and P2 in a feasible computation time. This is an example of _____
- (A) Related Message Attack (B) Broadcast Attack
(C) Coppersmith Theorem Attack (D) Short Pad Attack
- h. When two different message digest have the same value, it is called as:
- (A) RSA (B) Encryption
(C) Hash (D) Digital signature
- i. In SHA-512, do we need padding if the length of the original message is already a multiple of 1024 bits?
- (A) Yes (B) No
- j. In the RSA digital signature scheme, ____ is private; ____ and ____ are public.
- (A) n, d, e respectively (B) e, d, n respectively
(C) d, e, n respectively (D) none of these

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

- Q.2** a. Internetwork security is both fascinating and complex. Please specify some of the reasons. (8)
- b. Write the pseudocode for Millar-Rabin test. (4)
- c. What is meant by Quadratic Residues (QR) and Quadratic Non Residues (QNR)? (4)
- Q.3** a. Describe the procedure for encrypting and decrypting a message through Enigma machine. (8)
- b. What is block cipher? (4)
- c. Draw the diagram for a modern block cipher. (4)

- Q.4** a. How key size and nature of algorithm affect the security provided by DES? Explain. (10)
- b. Write a brief overview of differential cryptanalysis. (6)
- Q.5** a. Draw a diagram depicting a Cipher Block Chaining (CBC) mode. (8)
- b. What are the advantages of using Asymmetric Encryption? (8)
- Q.6** a. How do we check the integrity of a message? Explain by using a diagram. (5)
- b. What are the three criteria which needs to be satisfied by a cryptographic hash function? (3)
- c. What is SHA? (4)
- d. In SHA-512, what is the minimum and maximum number of padding bits that can be added to a message? (4)
- Q.7** a. What is the need for Digital Signatures? What are the properties and requirements for a digital signature? (12)
- b. Draw a diagram depicting the concept of CA. (4)
- Q.8** a. Describe the reasons for popularity and growth of PGP. (8)
- b. What are the data types and subtypes in MIME? (8)
- Q.9** a. Draw a diagram depicting the processing done by the record protocol. (7)
- b. What are the differences between the cipher suites available under SSLv3 and under TLS? (9)