

Time: 3 Hours

**JUNE 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. The residue class is

- (A) the set of integers congruent modulo  $n$
- (B) the set of all integers such that  $x = a \pmod{n}$ .
- (C) both (A) and (B)
- (D) none of these

b. What will be the value of  $-18 \pmod{14}$ ?

- (A) -4
- (B) 10
- (C) 4
- (D) None of these

c. What is the value of  $\phi(240)$ ?

- (A) 4
- (B) 64
- (C) 6
- (D) 16

d. Viruses and \_\_\_\_\_ are two examples of software attacks

- (A) Bacteria
- (B) Worms
- (C) Bugs
- (D) Germs

e. Which of the following is not a security goal?

- (A) Confidentiality
- (B) Integrity
- (C) Availability
- (D) Accessibility

**Code: AC76/AT76      Subject: CRYPTOGRAPHY & NETWORK SECURITY**

- f. Expansion for SKEME is:
- (A) Software Key Exchange Mechanism
  - (B) Secure Kernal Exchange Mechanism
  - (C) Secure Key Extended Mechanism
  - (D) none of these
- g. \_\_\_\_\_ is the simplest and least efficient algorithm to find the factors of a positive integer in which all positive integers, starting with 2, are tried to find one that divides n
- (A) Trial division factorization method
  - (B) Bruteforce
  - (C) 3DES
  - (D) SHA
- h. MIME stands for
- (A) Multipurpose Internet Mail Extensions
  - (B) Multiple Internet Merge Extensions
  - (C) Multipurpose Internal Mail Extensions
  - (D) None of these
- i. SSL provides services such as
- (A) fragmentation and compression
  - (B) message integrity and confidentiality
  - (C) framing
  - (D) all of these
- j. Needham-Schroeder protocol is an example of
- (A) Public-key distribution
  - (B) Symmetric key distribution
  - (C) KERBEROS
  - (D) none of these

---

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

---

- Q.2** a. What are Passive Attacks? Why are they difficult to detect? Name some passive attacks. (8)
- b. Distinguish between cryptography and steganography. (4)
- c. Is 97 a prime? How do you check for primeness of a number? (4)
- Q.3** a. Draw a diagram for depicting general idea of a symmetric-key cipher. (5)

- b. Write a note on Multiplicative Ciphers. What is the key domain for a multiplicative cipher? (5)
- c. 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? (6)
  - (i) The cipher is designed as a substitution cipher.
  - (ii) The cipher is designed as a transposition cipher.

**Q.4** a. The input to S-box 1 (the table below) is 100011. What is the output? (4)

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	10	03	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

- b. Mention any eight properties of S-boxes. (8)
- c. What is the probability of randomly selecting a weak, a semi-weak or a possible weak key in DES? (4)

**Q.5** a. What are the different modes of operation designed to be used with modern block ciphers? Describe any four. (8)

b. Draw a diagram to depict encryption, decryption and key generation in RSA, cryptosystem. Describe the security of this system. (8)

**Q.6** a. Explain the meaning of “Document & Finger print” and “Message & Message Digest”. What’s the difference between the 2 pairs? (6)

b. Explain Davies Meyer scheme with diagram. (5)

c. What kind of compression function is used in SHA-512? Explain. (5)

**Q.7** a. What are the differences between conventional signatures and digital signatures? Write a note on “Attacks on digital signature”. (8)

b. What is Public-Key Infrastructures (PKI)? List some duties of a PKI. (8)

**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. Let us assume that Alice has only two user IDs, alice@some.com and alice@anet.net. We also assume that Alice has two sets of private/public keys, one for each user ID. Please draw the private key ring table for Alice. (4)

- c. Explain the need for Key Revocation. How it is done? (4)
- Q.9** a. "SSL differentiates a connection from a session". Elaborate through a diagram. (8)
- b. What are the four phases in a handshake protocol? Draw a diagram to elaborate four cases in phase II. (8)