ROLL NO. _____

**Code: AC76/AT76/AC132/AT132**

**Subject: CRYPTOGRAPHY & NETWORK SECURITY**

## AMIETE – CS/IT (Current & New Scheme)

**Time: 3 Hours** **JUNE 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. Inserting some bogus data into the data traffic to thwart the adversary's Attempt to use the traffic analysis.
**(A)** Authentication Exchange **(B)** Routing Protocol
**(C)** Notarization **(D)** Traffic Padding

b. The result of the following operation -18 mod 14 is:
**(A)** -4 **(B)** 14
**(C)** 10 **(D)** 12

c. The size of the key-domain of Hill Ciphers is:
**(A)** $26^{mxm}$ **(B)** 36
**(C)** mxm matrix **(D)** 0-25

d. The round – key generator in the DES creates following 48-bit keys out of 56-bit cipher keys
**(A)** Sixteen **(B)** Twelve
**(C)** Four **(D)** Eight

e. Which of the following is not a Hash Algorithms for message integrity?
**(A)** Null **(B)** MD5
**(C)** SHA-1 **(D)** Diffie- Helman Algorithm

f. The result of $6^{10}$ mod 11
**(A)** 1 **(B)** 2
**(C)** 3 **(D)** 4

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

h. Which one of the following is a cryptographic protocol used to secure HTTP connection?
**(A)** stream control transmission protocol (SCTP)
**(B)** transport layer security (TSL)
**(C)** explicit congestion notification (ECN)
**(D)** RSA

i. ElGamal encryption system is
**(A)** symmetric key encryption algorithm
**(B)** asymmetric key encryption algorithm
**(C)** not an encryption algorithm
**(D)** none of these

j. The key size of IDEA block cipher is:
**(A)** 64 **(B)** 128
**(C)** 256 **(D)** 512

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

**Q.2** a. Find an integer that has remainder of 3 when divided by 7 and 13 but is divisible by 12 using Chinese remainder theorem. **(6)**

b. Discuss the security services as ITU – T (X.800). Also discuss the various security mechanisms and the relationship between the two. **(10)**

**Q.3** a. Alice and Bob can agree on the number of columns and the use of the method of the text in written into the table of row by row and transmitted column by column from this. **(3+3+2)**
(i) Identify the type of cipher.
(ii) If the plain text is as given below: (row by row, in table of four columns), write the ciphertext.

BOBL
ETSP
LANT
OEAT

(iii) Discuss the relation between the plaintext and the ciphertext.

b. Explain Hill Cipher with example. **(8)**

**Q.4** a. With reference to DES algorithm, explain the following:
(i) Block Size in DES
(ii) Cipher Key-Size
(iii) Round- Key size
(iv) No. of Rounds
(v) No. of Mixes and Swappers used in the first approach of making
(vi) encryption and decryption inverses of each other.
(vii) No. of Mixes and Swappers used in the second approach
(viii) Permutations used in DES algorithm
(ix) Exclusive –OR operations are used in DES. **(8)**

b. Discuss the weaknesses of DES algorithm and security challenges. **(8)**

**Q.5** a. Enlist five modes of operation designed to be used with modern block ciphers. Explain with the help of block diagram Cipher Feedback Mode (CFB). Also write its algorithm for encryption. **(8)**

b. Discuss the mechanism for secret communication with Knapsack Cryptosystem with the help of suitable diagram. **(8)**

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

b. Briefly explain how modification detection code and message authentication code is used to generate the integrity of a message. **(8)**

**Q.7** a. Explain various types of Attacks on Digital Signature. **(8)**

b. Enlist and explain in brief the differences between conventional and digital signatures. **(8)**

**Q.8** a. Discuss the general structure of an e-mail application program. **(8)**

b. Discuss how PGP protocol is used to secure e-mail message and store the file securely for future retrieval. Support your answer through suitable diagram. **(8)**

**Q.9** a. Discuss in brief four SSL protocols. **(8)**

b. Discuss the general architecture of TLS. **(8)**