

AMIETE – CS/IT (Current Scheme)

Time: 3 Hours

JUNE 2015

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. Cryptanalysis is
- (A) The science and art of creating secret codes.
 - (B) Creating a fixed length digest out of a variable length message.
 - (C) Concealing the message itself covering it with something else.
 - (D) The science and art of breaking secret codes.
- b. Positive integers can be divided into three groups: number 1 , primes and composites. The composites have exactly
- (A) One divisor
 - (B) Two divisors.
 - (C) Three divisors
 - (D) More than two divisors
- c. To encrypt a message using public-key cryptography scheme, which of the following must be done
- (A) Encrypt the message using the receiver's private key
 - (B) Encrypt the message using the sender's private key
 - (C) Encrypt the message using the sender's public key
 - (D) Encrypt the message using the receiver's public key
- d. Which of the following statement(s) is correct. Pretty good privacy is used
- (A) to provide email with privacy, integrity and authentication.
 - (B) to provide conversion to radix 64 code.
 - (C) for personal email.
 - (D) to send only unencrypted messages.

- e. Which of the following procedures must be done for private encryption scheme?
- (A) Encrypt the message with the senders private key and decrypt the message with receivers public key.
 - (B) Encrypt the message with senders public key and decrypt the message with receivers private key.
 - (C) Encrypt and decrypt the message by the public keys of sender and receiver.
 - (D) Encrypt the message with senders private key and decrypt the message with (shared) receivers private key.
- f. The value of $11^7 \bmod (187)$ is
- (A) 121
 - (B) 55
 - (C) 88
 - (D) 33
- g. In the Data Encryption Standard (DES) algorithm, the number of bits of key in each round and the number of rounds are
- (A) 48 and 16
 - (B) 16 and 48
 - (C) 64 and 18
 - (D) 18 and 64
- h. A digital signature is verified by using the following documents:
- (A) Public key of sender and private key of receiver
 - (B) Public key of sender and public key of receiver
 - (C) Private key of both sender and receiver
 - (D) Private and public key of sender
- i. The number of rounds used in SHA-512 algorithm to create message digest is:
- (A) 80
 - (B) 64
 - (C) 32
 - (D) 512
- j. The role of an authentication server is:
- (A) to verify the user and to issue a session key
 - (B) to issue a ticket to the server and provide a session key
 - (C) to provide service to the user(s)
 - (D) to help the Kerberos to its proper functioning

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

- Q.2** a. Find the multiplicative inverse of 7 in Z_{180} using the extended Euclidean algorithm. **(6)**
- b. Briefly explain different security goals and the different types of attacks which threatens these goals. **(10)**

- Q.3** a. Explain, what do you understand by substitution ciphers? Explain one mono alphabetic cipher with suitable examples. **(8)**
- b. Explain stream and block ciphers. **(8)**
- Q.4** a. Draw the general structure of Data Encryption Standard (DES) algorithm and briefly explain its operation. **(8)**
- b. Explain the principle behind initial and final permutation steps of Data Encryption Standard algorithm. **(8)**
- Q.5** a. Draw the block diagram of Cipher Block Chaining (CBC) mode to encipher text of any size. Explain the details of the operation. **(8)**
- b. Explain RSA Algorithm. **(8)**
- Q.6** a. Distinguish between message integrity and message authentication. **(8)**
- b. Define the criteria for cryptographic hash function. **(8)**
- Q.7** a. Distinguish between conventional signature and digital signature. **(5)**
- b. What are the attacks on digital signatures? Explain briefly. **(5)**
- c. Describe the possible attacks on Diffie Hellman key exchange mechanism. **(6)**
- Q.8** a. Explain the details of private key ring table and public key ring table maintained by each user. **(10)**
- b. How does information needed for sending and receiving messages is extracted from the set of key rings maintained? **(6)**
- Q.9** a. What are the protocols defined in secure socket layer? **(8)**
- b. Compare and contrast the handshake protocols in secure socket layer (SSL) and transport layer security (TLS). **(8)**