Code : 051718

B.Tech 7th Semester Exam., 2018

CRYPTOGRAPHY

Time : 3 hours **Full Marks : 70**

Instructions :

(i) The questions are of equal value.

*(ii) There are **NINE** questions in this paper.*

*(iii) Attempt **FIVE** questions in all.*

(iv) Question No. 1 is compulsory.

1. Choose the correct answer of the following (any *seven*) :

(a) In cryptography, what is cipher?

(i) Algorithm for performing encryption and decryption

(ii) Encrypted message

(iii) Both *(i)* and *(ii)*

(iv) None of the above

(b) In cryptography, the order of the letters in a message is rearranged by

(i) transpositional ciphers

(ii) substitutional ciphers

(iii) Both *(i)* and *(ii)*

(iv) None of the above

(c) Cryptanalysis is used

(i) to find some insecurity in a cryptographic scheme

(ii) to increase the speed

(iii) to encrypt the data

(iv) None of the above

(d) Which one of the following is a cryptographic protocol used to secure HTTP connection?

(i) Stream control transmission protocol (SCTP)

(ii) Transport layer security (TLS)

(iii) Explicit congestion notification (ECN)

(iv) Resource reservation protocol

(e) What is data encryption standard (DES)?

(i) Block cipher

(ii) Stream cipher

(iii) Bit cipher

(iv) None of the above

(f) Cryptographic hash function takes an arbitrary block of data and returns

(i) fixed-size bit string

(ii) variable-size bit string

(iii) Both *(i)* and *(ii)*

(iv) None of the above

(g) Which of the following algorithms belongs to asymmetric encryption?

(i) 3-DES

(ii) RC5

(iii) IDEA

(iv) RSA

(h) Which is the largest disadvantage of the symmetric encryption?

(i) More complex and therefore more time-consuming calculations

(ii) Problem of the secure transmission of the secret key

(iii) Less secure encryption function

(iv) Is not used anymore

(i) Which of the following statements is correct?

(i) PGP uses asymmetric encryption

(ii) In the World Wide Web, primarily symmetric encryption is used

(iii) PGP uses combined encryption

(iv) None of the above

(j) In which way does the combined encryption combine symmetric encryption and asymmetric encryption?

(i) First, the message is encrypted with symmetric encryption and afterwards it is encrypted asymmetrically together with the key

(ii) The secret key is symmetrically transmitted, the message itself asymmetrically

(iii) First, the message is encrypted with asymmetric encryption and afterwards it is encrypted symmetrically together with the key

(iv) The secret key is asymmetrically transmitted, the message itself asymmetrically

2. (a) Consider the implementation of the row transposition cipher with the keyword SCRAMBLE :

(i) Encrypt the plaintext thoroughly mixed

(ii) Decrypt the ciphertext EAAERCKTNEH-RAREWGNALGINRESTXXRTE

(b) Explain Security Services (X.800).

3. Alice and Bob decide to communicate with each other using the RSA algorithm. Against the advice of cryptographers, Bob selects two small primes $p = 7$ and $q = 13$ to use for the RSA algorithm. He observes that $n = p \cdot q = 7 \cdot 13 = 91$ and chooses an encryption key of $e = 5$. He makes his selection of n and e public :

   (a) Alice wishes to send the number $m = 23$ to Bob. Compute the ciphertext that Alice will obtain.

   (b) Compute the decryption key d that Bob uses to decrypt messages. Suppose he receives the ciphertext $c = 2$. Decrypt this ciphertext to reveal the number that Alice sent.

4. (a) Briefly explain the terms 'confusion' and 'diffusion' in the context of symmetric ciphers.

   (b) Describe SSL. Sketch its architecture.

5. (a) Write the steps involved in SET transaction.

   (b) How can public-key encryption be used to overcome the key distribution problem for a symmetric encryption?

6. (a) Explain the importance of random number generation in cryptography. When are random numbers truly random?

   (b) Explain MD5. Why is padding required in MD5?

7. (a) Explain challenge response protocol.

   (b) Encrypt the following message using an affine cipher with $a = 7$ and $b = 5$:

   new jersey

8. (a) What do you think the largest problem is with the security of the Hill cipher?

   (b) Explain about triple DES and intruder-in-the-middle attack against Diffie-Hellman.

9. (a) Explain about the flaw present in Needham Schroeder protocol.

   (b) Explain about X.509 certificate and its components.

★ ★ ★