B.Tech 7th Semester Exam., 2017

CRYPTOGRAPHY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

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

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

*(iv) Question No. **1** is compulsory.*

1. Answer the following (any *seven*) : 2×7=14

   (a) Explain why modern block ciphers are designed as substitution ciphers instead of transposition ciphers.

   (b) Use a brute force attack to decipher the following message :

   XPALASXYFGFUKPXUSOGEUTKCDGFXANMGNVS

   Assume that it is an affine cipher and the plaintext 'hb' is ciphered as 'PL'.

   (c) Encrypt the message "Attack tonight" by using playfair cipher of key 'dollar'.

   (d) What is the difference between Feistel and Non-Feistel Ciphers?

   (e) A transposition block has 10 inputs and 10 outputs. What is the order of the permutation group and what is the key size?

   (f) Use the Vigenere cipher with keyword "HEALTH" to encipher the message "cryptography is fun".

   (g) Find the n-bit word that is represented by the polynomial (x^2+1) in GF (2^5).

   (h) Find out the multiplicative inverse of 23 in Z_{100}.

   (i) Explain how to invert a permutation table represented as a one-dimensional table.

   (j) Which of the four transformations defined for AES change the contents of bytes? Which one doesn't change the content of bytes?

2. *(a)* Explain the steps involved in each round of DES encryption algorithm with description of DES function.

   (b) Explain the round key generation process in DES and AES. 7+7=14

3. *(a)* Describe handshaking protocol in SSL and the process of creation of master key from premaster secret in SSL.

   (b) Draw a diagram to illustrate the Diffie-Hellman key exchange between Bob and Alice. 7+7=14

4. *(a)* Explain one-stream cipher technique used in wireless networks.

   (b) Explain different modes of operations of block ciphers. 7+7=14

5. *(a)* Explain different approaches for public key distribution in a network.

   (b) How is Kerberos used to establish authentication in distributed environment? Explain briefly. 7+7=14

6. *(a)* Find the value of x for the following sets of congruence using the Chinese remainder theorem :

   (i) $x \equiv 2 \bmod 7$ and $x \equiv 3 \bmod 9$

   (ii) $x \equiv 4 \bmod 5$ and $x \equiv 10 \bmod 11$

   (iii) $x \equiv 7 \bmod 13$ and $x \equiv 11 \bmod 12$

   (b) Explain the attacks in RSA with the description of the algorithm. 7+7=14

7. *(a)* What is the difference between MAC and Hash? Explain HMAC algorithm.

   (b) Explain what are the security services provided by a digital signature. What types of attacks can be performed on digital signatures? 7+7=14

8. *(a)* Compare the various generation of firewalls.

   (b) What are the malicious programs which try to hamper system security? 7+7=14

9. *(a)* IP Security (IPSec) is a collection of protocols to provide security at network level. Explain the protocols and modes of IPSec.

   (b) How dual signatures are created and used in Secure Electronic Transactions (SET)? 7+7=14

***

Code : 051718

B.Tech 7th Semester Exam., 2018

CRYPTOGRAPHY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) All questions carry equal marks.

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

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

(iv) Question No. 1 is compulsory.

1. Answer the following (any *seven*) :

   (a) Distinguish between cryptography and steganography.

   (b) Distinguish between a monoalphabetic cipher and a transposition cipher.

   (c) Show how a polynomial can represent an *n*-bit word.

   (d) List the parameters (block size, key size and the number of rounds) for the three AES versions.

   (e) Define Euler's theorem and explain its application.

   (f) List some family of hash functions that do not use a cipher as the compression function.

   (g) What is the padding for SHA-512 if the length of the message is 5121 bits?

   (h) Explain a logic bomb and a time bomb.

   (i) List four kinds of cryptanalysis attack.

   (j) Give one example of a field using a set of residues.

2. Use the Play Fair cipher to encipher the message "We live in an insecure world". The secret key can be made by filling the first and part of the second row with the word 'GUIDANCE' and filling the rest of the matrix with the rest of the alphabet.

3. Explain the DES encryption and decryption process in detail.

4. Compare the round keys in DES and AES. In which cipher is the size of the round key the same as the size of the block? Explain the AES encryption and decryption process in detail.

5. Alice uses Bob's RSA public key ($e = 7$, $n = 143$) to send the plain text $p = 8$ encrypted as ciphertext $c = 57$. Show how Eve can use the chosen ciphertext attack if she has access to Bob's computer to find the plain text.

6. In the elliptic curve digital signature scheme, prove the correctness of the verifying process.

7. Distinguish between two modes of IPsec. Define AH and the security services it provides. Define ESP and the security services it provides.

8. What are the various functionalities of IDS in security? What is the difference between a firewall and an IDS?

9. List and give the purpose of four protocols defined in SSL or TLS.

* * *

Code : 051718

B.Tech 7th Semester Exam., 2019

CRYPTOGRAPHY

Time : 3 hours *Full Marks* : 70

Instructions :

(i) The marks are indicated in the right-hand margin.

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

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

*(iv) Question No. **1** is compulsory.*

1. Choose the correct option of the following (any *seven*) : 2×7=14

(a) The DES algorithm cipher system consists of ____ rounds (iterations) each with a round key.

(i) 12

(ii) 18

(iii) 9

(iv) 16

(b) How many rounds does the AES-192 perform?

(i) 10

(ii) 12

(iii) 14

(iv) 16

(c) The solution of

$$x^2 \equiv 2 \bmod 11$$

is

(i) No solution

(ii) $x \equiv 9 \bmod 11$

(iii) $x \equiv 4 \bmod 11$

(iv) $x \equiv 4 \bmod 11$ and $x \equiv 7 \bmod 11$

(d) SHA-1 produces a hash value of

(i) 256 bits

(ii) 160 bits

(iii) 180 bits

(iv) 128 bits

(e) Message authentication code is also known as

(i) key code

(ii) hash code

(iii) keyed hash function

(iv) message key hash function

(f) Public key encryption/decryption is not preferred, because

(i) it is slow

(ii) it is hardware/software intensive

(iii) it has a high computational load

(iv) All of the above

(g) RSA stands for

(i) Rivest, Shamir, Adleman

(ii) Roger, Shamir, Adrian

(iii) Robert, Shamir, Anthony

(iv) Rivest, Shaw, Adleman

(h) These ciphers replace a character or characters with a different character or characters, based on some key.

(i) Polyalphabetic substitution based

(ii) Transposition-based

(iii) Substitution based

(iv) Mono-alphabetic substitution based

(i) What type of symmetric key algorithm, uses a streaming cipher to encrypt information?

(i) RC4

(ii) Blowfish

(iii) SHA

(iv) MD5

(j) Message ____ means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

(i) confidentiality

(ii) integrity

(iii) authentication

(iv) None of the above

2. *(a)* List and briefly define the categories of security mechanisms. Also list and briefly define the fundamental security design principles. 7

(b) Consider an automated cash deposit machine in which users provide a card or an account number to deposit cash. Give examples of confidentiality, integrity and availability requirements associated with the system, and, in each case, indicate the degree of importance of the requirement. 7

3. (a) Define Feistel Cipher. Which parameters and design choices determine the actual algorithm of a Feistel cipher? 7

(b) What is the output of the first round of the DES algorithm when the plaintext and the key are both all ones? 7

4. Design a security service that provides data integrity, data confidentiality and non-repudiation using public-key cryptography in a two-party communication system over an insecure channel. Give a rationale that data integrity, confidentiality and non-repudiation are achieved by your solution. (Recommendation : Consider the corresponding threats in your argumentation). 14

5. Answer the following : 7×2=14

(a) Compare the substitution in DES and AES. Why do we have only one substitution table (S-Box) in AES, but several in DES?

(b) AES defines implementations with three different numbers of rounds (10, 12 and 14); DES defines only implementation with 16 rounds. What are the advantages and disadvantages of AES over DES with respect to this difference?

6. Explain Diffie-Hellman key exchange in detail. In the Diffie-Hellman protocol, each participant selects a secret number x and sends the other participant $a^x \bmod q$ for some public number a. What would happen if then participants sent each other x^a for some public number a instead? Give at least one method Alice and Bob could use to agree on a key. Can Eve break your system without finding the secret numbers? Can Eve find the secret numbers? 14

7. (a) What services are provided by the SSL record protocol? What steps are involved in the SSL Record Protocol Transmission? 7

(b) Explain the process of Secure Electronic Transaction. 7

8. Write short notes on the following : 14

(a) S/MIME

(b) HMAC

(c) Digital signature

(d) Message authentication code

9. Write short notes on the following :

✓ *(a)* Password management

(b) Firewall

(c) Intrusion detection system

(d) Denial of service attack

★ ★ ★