Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination

Year 3, Semester 2 (2019)

IE3082 – Cryptography

Duration: 3 Hours

October 2019

Instructions to Candidates:

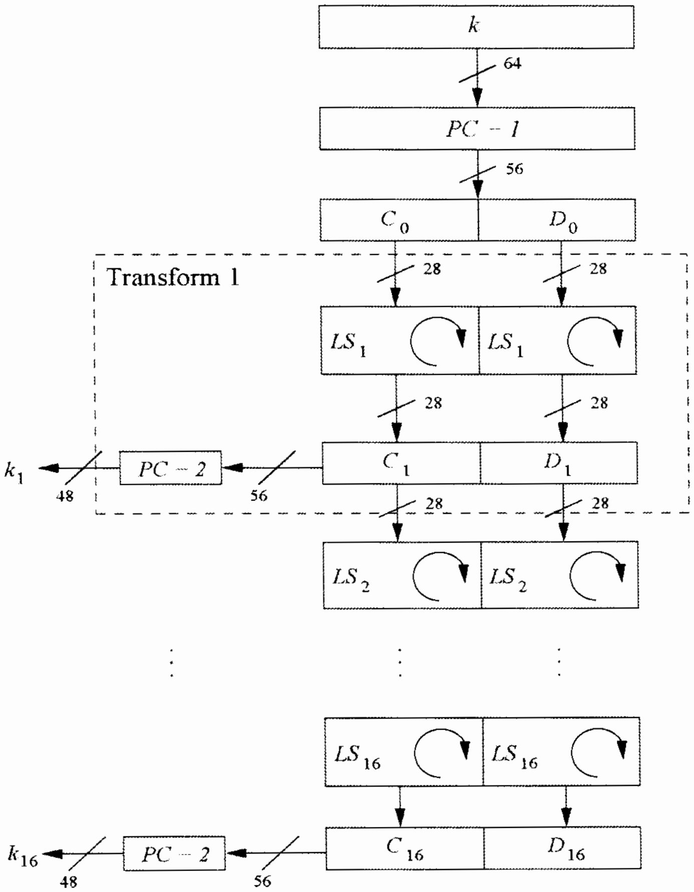
- ♦ This paper has 4 questions on 5 pages (including the cover page).
- ♦ Answer all questions in the booklet given.
- ♦ The total marks for the paper is 100.
- ♦ University approved calculators are allowed.

Question 1 (25 marks)

a. Construct mathematical equations for Encryption and Decryption for a generalized 'Shift Cipher' with a key of 6. Assume that the English alphabet is mapped to numbers.

(8 marks)

b. Following diagram depicts the reverse key schedule of Data Encryption Standard. With the use of the diagram below explain how **k₀ = k₁₆** after 16 rounds.



(8 marks)

c. Consider the storage of data in encrypted form in a large database using AES. One record has a size of 16 bytes. Assume that the records are not related to one another. Which mode of operation would you recommend to encrypt the database? Justify your answer.

(5 marks)

d. Compare 'XOR' and 'AND' logical operations with respect to stream ciphers.

(4 marks)

Question 2 (25 marks)

a. AES-256 has an input size of 128bits. Hence the plain-text and cipher-text space is limited to 2^{128} possibilities.

i. Briefly describe how a brute-force attack can produce false positive results.

(4 marks)

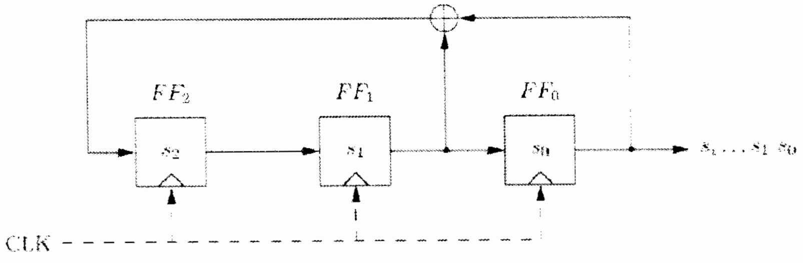
ii. How can the attacker verify whether it is a false positive?

(2 marks)

b. Block ciphers have a limited input size. Hence they have to be used in a suitable mode to achieve optimum results. Compare Electronic Codebook Mode (ECB), Cipher Block Chaining (CBC), and Counter Modes considering the following three factors when comparing: Security, Speed and Ease of Implementation.

(9 marks)

c. The Linear Feedback Shift Register (LFSR) circuit diagram given below which can be used for random number generation in stream ciphers.



i. Calculate the maximum number of random output bits this LFSR can generate.

(2 marks)

ii. Compose first 8 sequences of states, given the initial vector (IV) $s_2 = 1$ $s_1 = 0$ $s_0 = 0$

(4 marks)

iii. Briefly explain the relationship of primitive polynomials and LFSRs.

(2 marks)

d. According to Claude Shannon, what are the two most desirable properties in block ciphers?

(2 marks)

Question 3 (25 marks)

a. Let the two primes be p = 13 and q = 17 be given as set-up parameters for RSA.

i. Which of the following public exponents are valid parameters? Justify your choice.

$e_1 = 19$
$e_2 = 27$

(3 marks)

ii. Public Key can be defined as $K_{pub} = (n,e)$. Using the valid parameter from previous question, Compute the corresponding private key $K_{pr} = (d)$. Use the extended Euclidean algorithm for the inversion and point out every calculation step.

(5 marks)

iii. Explain, why an attacker cannot derive the private key $K_{pr} = (d)$.

(2 marks)

b. Compute the two public keys and the shared secret key for the Diffie-Hellman (DHKE) scheme with the following parameters:

Domain parameters: $p = 373$, $\alpha = 5$ (generator/primitive root).

Alice private key (a) = 7

Bob private key (b) = 4

(5 marks)

c. Given an RSA signature scheme with following parameters n=33, public exponent (e) = 3, private exponent (d) = 7,

i. State if the following signatures are valid for a given message 'x'.

- (x = 4, sig(x) = 15)
- (x = 6, sig(x) = 30)
- (x = 2, sig(x) = 29)

(6 marks)

ii. Generate the signatures for the following messages 'x'.

- x = 8
- x = 13

(4 marks)

Question 4 (25 marks)

a. Hash functions play an important role in computer security. Commonly used hash functions have a number of functional and security requirements. Write a single sentence to explain the following requirements of a hash function.

- Arbitrary length input size
- Diffusion
- Pre-image resistance
- Collision resistance

(8 marks)

b. What is the purpose of a rainbow table? How can we protect against rainbow table attacks?

(3 marks)

c. In cryptography, an HMAC (hash based message authentication codes) is a specific type of message authentication code involving cryptographic hash function and a secret key.

i. Using a diagram illustrate how an attacker can carry out the secret prefix attack against an HMAC.

(4 marks)

ii. Recommend a mechanism to prevent the above mentioned attack.

(3 marks)

d. Briefly describe the n^2 key distribution problem with respect to symmetric cryptography.

(3 marks)

e. In Public Key Infrastructure (PKI) Certificates play an important role to validate the authenticity of a given user. Write a single sentence to explain the purpose of the following components in a certificate.

- Subject
- Issuer
- Public Key
- Signature algorithm

(4 marks)

-- End of the Question Paper --