00234

Sri Lanka Institute of Information Technology

B.Sc. Honours Degree in Information Technology

Specialized in Cyber Security

Final Examination
Year 3, Semester 2 (2022)

IE3082 – Cryptography

Duration: 2 Hours

November 2022

Instructions to Candidates:

- This paper has FOUR questions.
- Answer all questions in the booklet given.
- This paper is preceded by a 10-minute reading period. The supervisor will indicate when answering may commence.
- The total mark for the paper is 100.
- This paper contains FIVE pages, including the cover page.
- Faculty approved calculators are allowed.

Question 1 (25 Marks)

a. Study the following cipher text extract of a substitution cipher-based communication between two parties. Answer the given questions based on the cipher text.

"gsrh urmzo vczn rh vzhb, r xzm tvg z tllw tizwv uli gsrh nlwfov."

i. What is the complexity of a systematic brute-force approach to cryptanalyze this cipher text?

(4 Marks)

ii. Propose a less complex and a computationally feasible cryptanalysis approach for the above scenario.

(3 Marks)

iii. Compare brute-forcing simple shift-cipher and a substitution cipher with respect to complexity.

(3 Marks)

b. In cryptography linear-feedback shift registers (LFSRs) play an important role in stream cipher construction. Based on the given primitive polynomial below, answer the given questions.

Primitive Polynomial: $x^4 + x + 1$

i. Create a maximum length LFSR circuit using the above primitive polynomial (Diagram should indicate register settings and CPU clock cycle input).

(6 Marks)

ii. What is the maximum number of random bits that could be generated by this LFSR?

(3 Marks)

iii. If an LFSR is utilized as it is, known plain text attacks can be launched against it due to its linear nature. Propose a mechanism to avoid this problem so that LFSRs can be used for cryptographically secure stream communication.

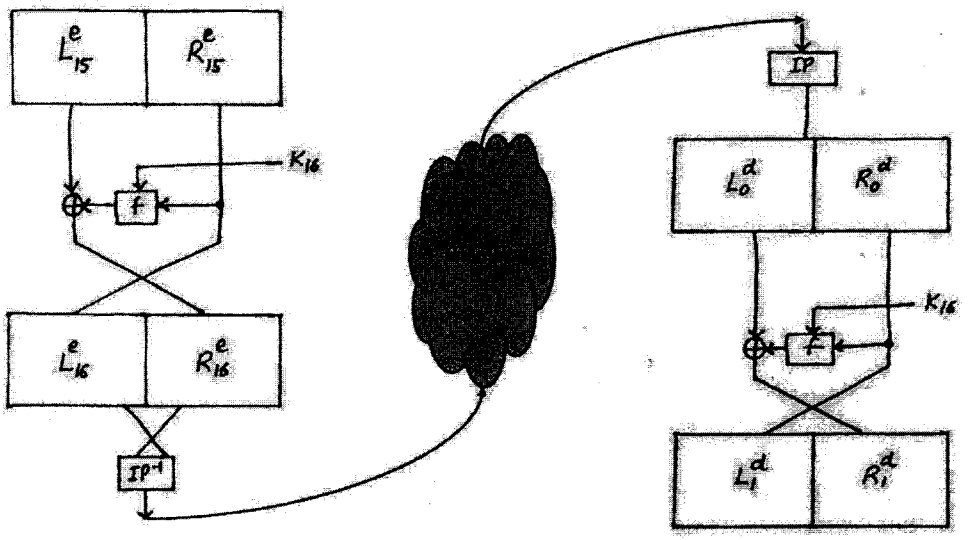
(3 Marks)

c. Briefly explain the main reason why true random number generation methods are impractical to be used in stream ciphers.

(3 Marks)

Question 2 (25 Marks)

a. Diagram given below illustrates the last round of Data Encryption Standard (DES) decryption and first round of DES encryption. Answer the questions given based on the given diagram.



i. Using the diagram as an aid prove that: $L_1^d = R_{15}^e \cap R_1^d = L_{15}^e$

(6 Marks)

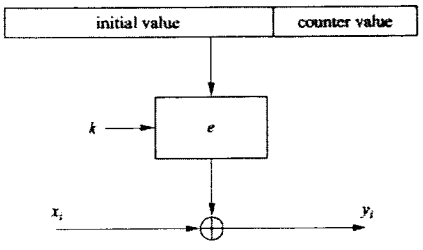
ii. Briefly explain the relationship of DES decryption process and the reversed key schedule.

(4 Marks)

iii. Propose a mechanism which could allow a legacy ATM in a bank to use DES as its encryption algorithm in 2022.

(2 Marks)

b. Alice and Bob are using Advanced Encryption Standard (AES) 128 encryption for their data communication. They are using the AES algorithm (ϕ) as given below.



i. What is mode of operation used by Alice and Bob?

(2 Marks)

ii. Compare the performance of the above mode and cipher block chaining mode with respect to speed and security.

(6 Marks)

c. Modern public key algorithms are built based on mathematically hard problems. They are also known as one-way functions.

i. Mention two mathematically hard problems used in modern public key algorithms.

(2 Marks)

ii. Briefly explain the mathematically hard problem used by the Diffie-Hellman Key Exchange.

(3 Marks)

Question 3 (25 Marks)

a. Let the two primes p = 17 & q = 11 be given as Alice's set-up parameters for RSA algorithm.

i. Which one of these parameters e1 = 16, e2 = 13 is a valid RSA exponent? Justify your choice.

(4 Marks)

ii. Using 'e' from your answer to question 'i' compute the corresponding private key K_{pr} = (d). Use the extended Euclidean algorithm for the inversion and point out every calculation step.

(6 Marks)

iii. Alice now wants to decrypt a received cipher text (y = 21) using the private key (d). Using the square & multiplication algorithm show how the decryption can be optimized to a minimum number of calculation steps.

(4 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 = 467, α = 2 (generator)
- Alice private key (a) = 3
- Bob private key (b) = 5

(7 Marks)

c. Given an RSA signature scheme with the following parameters; n=187, public exponent (e) = 7, private exponent (d) = 23, state if the following signatures are valid for a given message 'x'.

i. (x = 5, sig(x) = 180)
ii. (x = 7, sig(x) = 161)

(4 marks)

Question 4 (25 Marks)

a. Hash function is function that can be used to map data of arbitrary size to fixed-size values.

i. Compare the following security properties with respect to 'Hash Functions'.
- Pre-image Resistance
- 2nd Pre-image Resistance

(6 Marks)

ii. "Collision resistance is the most difficult security property to achieve when creating a hash function." Justify this statement using birthday-paradox.

(4 Marks)

b. Message Authentication Codes (MAC) are also known as cryptographic checksum. MACs can be designed by prefixing the secret key to the message. Construct an attack against a secret-prefix based MAC scheme.

(6 Marks)

c. Compare the security services achieved by public key based digital signatures and symmetric key based message authentication codes (MACs).

(3 Marks)

d. Certificates play an important role in modern day public key infrastructure.

i. Write down three main components of an X.509 certificate.

(3 Marks)

ii. "A single Certificate Authority (CA) for certificate issuing is not a scalable solution. Therefore, a hierarchical certificate issuing authorities are needed." Do you agree with this statement? Justify your answer.

(3 Marks)

--End-of-Question-Paper--