Sri Lanka Institute of Information Technology

B.Sc. Special Honours Degree
in
Information Technology
(Cyber Security)

Final Examination
Year 3, Semester 2 (2018)

IT349 - Cryptography

Duration: 3 Hours

October 2018

Instructions to candidate:

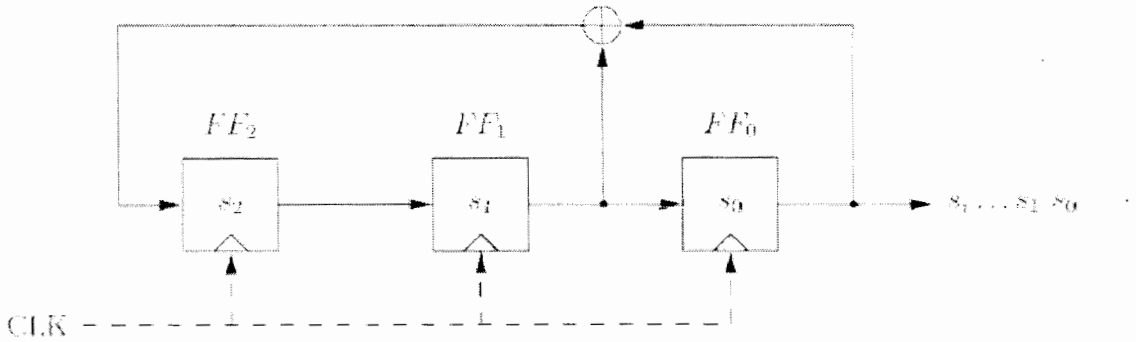
- This paper has 4 questions and answer all questions.
- Non programmable calculators are allowed.
- Marks for each question are given.
- Total mark is 100.
- This paper contains 5 pages including cover page.

Question 1 (25 marks)

a) Briefly explain the perfect secrecy of a one-time pad (OTP).

(4 marks)

b) Refer the Linear Feedback Shift Register (LFSR) circuit diagram given below which can be used for random number generation.



i) What is the degree (m) of this LFSR?

(2 marks)

ii) What is the maximum length of output this can produce?

(2 marks)

iii) Compose the first 8 sequence of states of LFSR, given the initial vector(IV) $s_2 = 1$ $s_1 = 0$ $s_0 = 0$

(5 marks)

iv) What is distinctive about this IV?

(2 marks)

c) A simple Linear Feedback Shift Registers (LFSR) construct can be compromised using Gaussian elimination. Explain how modern LFSR based random number generators such as GSM (A5/1) avoids this.

(5 marks)

d) Briefly describe how the inventors of DES algorithm made sure it was resistant to 'differential cryptanalysis'.

(5 marks)

Question 2 (25 marks)

a) S-Box component defined in the Data Encryption Standard (DES) is a crucial element for its overall operation. Refer the table S1 given below and answer the question.

S_1	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
0	14	04	13	01	02	15	11	08	03	10	06	12	05	09	00	07
1	00	15	07	04	14	02	13	01	10	06	12	11	09	05	03	08
2	04	01	14	08	13	06	02	11	15	12	09	07	03	10	05	00
3	15	12	08	02	04	09	01	07	05	11	03	14	10	00	06	13

Compose the binary outputs from S1 given the inputs:

i. 001010

ii. 100101

(4 marks)

b) DES algorithm's 56bit key length is not secure against modern computing power. Explain why it is not possible to achieve 112bit key length by doing double encryption using two different keys. You may use a diagram to explain.

(8 Marks)

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

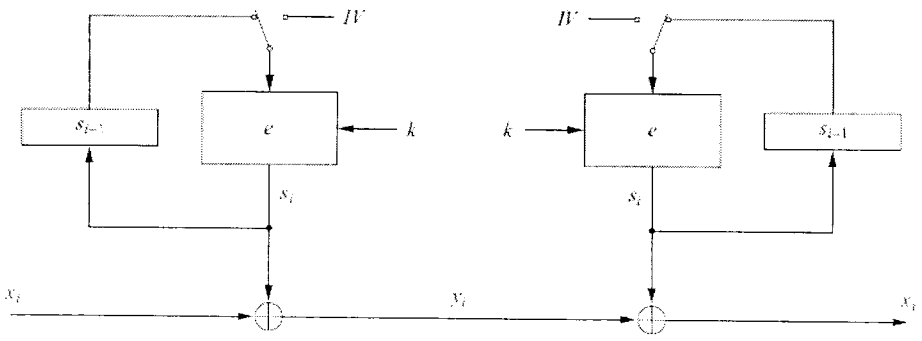
i. Briefly describe how a brute-force attack can produce false positive results.

(4 marks)

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

(2 mark)

d) Output Feedback Mode (OFB) is a commonly used block encryption mode. Refer to the diagram below and answer the questions.



iii. What is the encryption/decryption function in this mode?

(3 marks)

iv. Explain why there is no involvement of a block cipher decryption function (e^{-1}) in OFB mode.

(4 marks)

Question 3 (25 marks)

a) Let the two primes p = 17 and q = 11 be given as set-up parameters for RSA.

i. Which one of these parameters $e_1 = 8$, $e_2 = 7$ is a valid RSA exponent? Justify your choice.

(4 Marks)

ii. Public key can be defined as Kpub = (p,q,e).

Using 'e' from your answer from question 'i' compute the corresponding private key Kpr = (p,q,d). Use the extended Euclidean algorithm for the inversion and point out every calculation step.

(6 Marks)

iii. For Oscar (attacker) to determine the private key d, he needs to calculate $d \equiv e{-}1 \bmod \Phi(n)$. There is an efficient expression for calculating $\Phi(n)$. What prevents him from using this formulae to derive the private key d?

(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, $\alpha = 2$ (generator)
- Alice private key (a) = 3
- Bob private key (b) = 5

(8 Marks)

c) Briefly explain the relationship between El-gammal encryption scheme and Diffie-Hellman Key Exchange.

(3 Marks)

Question 4 (25 marks)

a) Given an RSA signature scheme with the following parameters (n=33, public exponent (e) = 3, private exponent (d) = 7), state if the following signatures are valid for a given message 'x'.

i. (x = 5, sig(x) = 22)
ii. (x = 4, sig(x) = 16)

(4 marks)

b) Compare the following security properties with respect to 'Hash Functions'.

- Pre-image Resistance
- 2nd Pre-image Resistance

(4 Marks)

c) Briefly describe the purpose of a rainbow table and explain how to prevent rainbow table based attacks.

(3 Marks)

d) 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)

e) Write down the main components of an X.509 certificate.

(5 marks)

f) Briefly explain the purpose of Certificate Revocation Lists (CRLs) with respect to public key infrastructure (PKI).

(3 marks)

-- End of the Question Paper --