Sri Lanka Institute of Information Technology

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

Final
~~Mid~~ Semester Examination
Year 3, Semester 2(2017)

IT349 - Cryptography

Duration: 3 Hours

October 2017

Instructions to candidate:

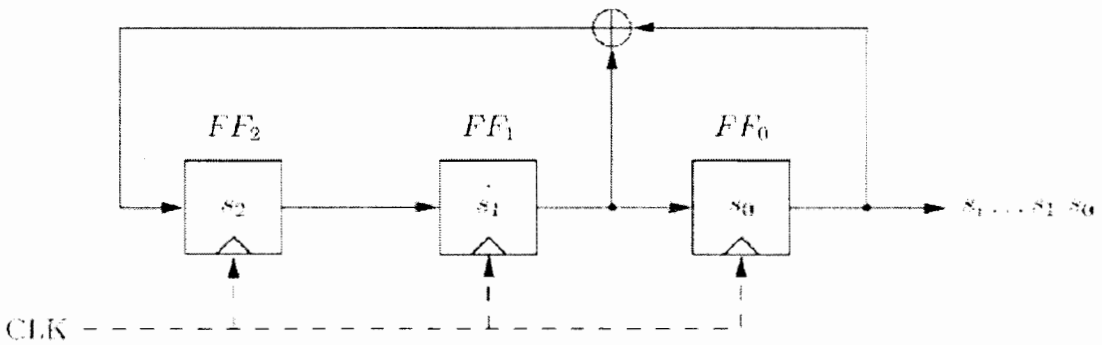
- This paper has 4 questions.
- Answer all questions.
- Marks for each question are given.
- Non programmable calculators are allowed.
- Total mark is 40.
- This paper contains 4 pages including cover page.

Question 1 (10 marks)

a) 'Trivium' is a modern stream cipher that is used in GSM communication. Briefly explain how such stream ciphers achieve non-linearity.

(3 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 maximum length of output this can produce?

(1 mark)

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

(2 marks)

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

(2 mark)

c) Affine cipher encryption can be defined using the following equation,

$$y = a*x + b \bmod p$$

x = Plain text
y = Cipher text
a,b = Key

Explain the relationship of modular/multiplicative inverse with respect to affine cipher decryption.

(2 marks)

Question 2 (10 marks)

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

(2 marks)

b) DES encryption round consists of various sub components in 'f' function. State the purpose of the given functions with respect to your answer in (a).

i. Expansion Function
ii. Round Key X-OR
iii. S-box Substitution

(3 marks)

c) Apart from brute forcing K_1 and then K_2, which better technique can be used to attack 2DES?

(1 mark)

d) State two modes of operation for block ciphers that use the encryption function as a key generator.

(2 marks)

e) Using the equation given below, calculate the complexity of finding a collision with a probability of 50% for SHA-1 hash function.

$$t \approx 2^{(n+1)/2} \sqrt{\ln\left(\frac{1}{1-\lambda}\right)}.$$

(2 marks)

Question 3 (10 marks)

a) Let the two primes p = 11 and q = 13 be given as set-up parameters for RSA.

i. Which of the parameters e1 = 3, e2 = 7 is a valid public exponent? Justify your choice.

(2 marks)

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

(3 marks)

b) Briefly explain an attack against RSA based digital signature scheme. You may use a diagram to explain.

(2 marks)

c) All public key algorithms are rarely used for data encryption due to high processing requirements. Briefly explain why Diffie Hellman based Elgamal scheme can be used for data encryption.

(2 marks)

d) State an advantage of using Elliptic Curve Digital Signature Algorithm (ECDSA).

(1 mark)

Question 4 (10 marks)

a) Briefly explain how secret prefix attack works in hash based message authentication codes (HMACs).

(3 marks)

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

(2 marks)

c) Draw a diagram of the Certificate Authority (CA) based Diffie–Hellman Key Exchange (DHKE).

(2 marks)

d) State three important fields you can find in a X.509 digital certificate.

(3 marks)

-- End of the Question Paper --