Name .............................. ID ............... Section ...... Seat No ......

# Sirindhorn International Institute of Technology
# Thammasat University

**Midterm Exam: Semester 2, 2010**

**Course Title:** CSS322 Security and Cryptography

**Instructor:** Steven Gordon

**Date/Time:** Wednesday 29 December 2010; 9:00–12:00

---

**Instructions:**

- This examination paper has 11 pages (including this page).
- Conditions of Examination: Closed book; No dictionary; Non-programmable calculator is allowed
- Students are not allowed to be out of the exam room during examination. Going to the restroom may result in score deduction.
- Students are not allowed to have communication devices (e.g. mobile phone) in their possession.
- Write your name, student ID, section, and seat number clearly on the front page of the exam, and on any separate sheets (if they exist).
- The space on the back of each page can be used if necessary.

## Question 1 [7 marks]

(a) Two security services are *confidentiality* and *authentication*. List and describe the other four security services. [4 marks]

(b) Describe the difference between a *passive* and *active* attack on security. [1 mark]

(c) Describe two types of passive attacks. [2 marks]

# Question 2 [8 marks]

Consider a 4-bit block cipher, called *Steve's Simple Cipher* or SSC for short, shown in the table below. The table gives the ciphertext $C$ produced when encrypting the plaintext $P$ with one of the four keys.

| P | C (K=00) | C (K=01) | C (K=10) | C (K=11) |
|---|---|---|---|---|
| 0000 | 0110 | 1100 | 0001 | 0010 |
| 0001 | 1101 | 0100 | 1010 | 0000 |
| 0010 | 0010 | 0001 | 1111 | 1011 |
| 0011 | 0100 | 1101 | 0011 | 1001 |
| 0100 | 1100 | 0111 | 1001 | 0011 |
| 0101 | 1111 | 0101 | 0010 | 1000 |
| 0110 | 0000 | 0011 | 0111 | 1111 |
| 0111 | 0111 | 1011 | 1101 | 0001 |
| 1000 | 1010 | 1001 | 1000 | 0100 |
| 1001 | 0001 | 0000 | 1110 | 0111 |
| 1010 | 1001 | 0110 | 0110 | 1100 |
| 1011 | 1110 | 0010 | 1011 | 1101 |
| 1100 | 1011 | 1111 | 0000 | 0101 |
| 1101 | 1000 | 1010 | 0100 | 1110 |
| 1110 | 0011 | 1110 | 1100 | 0110 |
| 1111 | 0101 | 1000 | 0101 | 1010 |

(a) SSC is *not* an ideal block cipher. If SSC was to be extended to an ideal 4-bit block cipher, how many possible keys would it have? [1 mark]

(b) If SSC was extended to be an ideal 4-bit block cipher, how long would each key be? [1 mark]

(c) Give a reason why ideal block ciphers are not suitable in practice. [1 mark]

Consider a block cipher, *Double-SSC*, which involves applying the block cipher SSC two times (e.g. encrypt the plaintext to obtain a temporary value, then encrypt the temporary value to obtain the ciphertext), each time using a potentially different 2-bit key.

(d) Show how the meet-in-the-middle attack works by applying it against Double-SSC. Use the attack to find the key used if the attacker already knows the (plaintext, ciphertext) pairs: (1101, 1100) and (1001, 1101). Explain clearly the steps applied by the attacker and how the key is identified. Write your answer below, and show calculations on next page. [5 marks]

`Key = ______________________`

# Question 3 [9 marks]

(a) Consider the Linear Congruential Generator as a PRNG:

$$X_{n+1} = (aX_n + c) \bmod m$$

For the values of $a = 7$, $c = 1$, $m = 31$ and a seed of 12, what are the next 4 numbers in the pseudo-random sequence? [3 marks]

--- --- --- ---

(b) Which of the parameters of the above LCG should be changed to produce a sequence with a larger period? What is a suggested value? [1 mark]

(c) Assume the block cipher *SSC* is used in counter mode as a PRNG, where the initial counter value is 0, and the seed is 01. What are the first 16 bits of the pseudo-random sequence? [3 marks]

-- -- -- -- -- -- -- -- -- -- -- -- -- -- -- --

(d) Comparing LCG and using a block cipher in counter mode, what is the disadvantage of LCG as a PRNG? (This questions is about the general approach of using LCG and block ciphers when "good" parameter values and block/key sizes are chosen; it is not about the specific instances above, where the parameter values and key/block ciphers are inappropriate for practical usage). [2 marks]

# Question 4 [8 marks]

For reference, you may use the following mapping of English characters to numbers:

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 | 25 |

(a) The ciphertext *SGWRIJGMII* was obtained by encrypting using the Vigenère cipher with keyword *steve*. What was the plaintext? [3 marks]

P = ____________________________________

(b) The ciphertext *XNTPUXNJNE* was obtained by encrypting using the one-time pad with keyword *xabtqgibsa*. What was the plaintext? [3 marks]

P = ____________________________________

(c) The one-time pad is considered to be *unconditionally secure*. What does unconditionally secure mean? [1 mark]

(d) Explain the weakness of the Vigenère cipher. [1 mark]

# Question 5 [9 marks]

A generalisation of the Caesar cipher is known as the *Affine Caesar cipher*. For each plaintext letter $p$, the ciphertext letter $C$ is:

$$C = \mathrm{E}([a, b], p) = (ap + b) \bmod 26$$

For the Affine Caesar cipher to have a one-to-one mapping, the multiplicative inverse of $a$, or $\mathrm{MI}(a)$, in mod 26 must exist.

(a) Explain what is meant by a *one-to-one mapping* for a cipher. [1 mark]

(b) For $b = 4$ and $a > 3$, what is a value of $a$ for which the Affine Caesar cipher has a one-to-one mapping? [1 mark]

(c) For $b = 4$ and $a > 3$, what is a value of $a$ for which the Affine Caesar cipher does *not* have a one-to-one mapping? [1 mark]

(d) Using the syntax $\mathrm{MI}(a)$ for the multiplicative inverse of $a$, write an equation for the decryption operation of the Affine Caesar cipher. [3 marks]

(e) Assume the Affine Caesar cipher is extended for an $n$-character alphabet, i.e. instead of mod 26 it is mod $n$. Write an expression that gives the number of values of $a$ for which a one-to-one mapping exists. Explain your reasoning, i.e. why the expression is valid. [3 marks]

# Question 6 [8 marks]

The following information may (or may not) be useful in this question:

- Fermat's theorem: if $p$ is prime and $a$ is a positive integer, then $a^p \equiv a \pmod{p}$
- Euler's theorem: For positive integers $a$ and $n$, $a^{\phi(n)+1} \equiv a \pmod{n}$
- First 20 prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71.

For the following questions, you must show your steps that simplify the calculation, explaining which theorems can be used and why. You cannot simply use a calculator to find the answer directly. However you can use a calculator to check your answer, as well as to perform basic multiplication and division calculations (that is, you do not need to show calculations for, for example, $23 \times 46$).

(a) Find the answer of $49^{55} \bmod 53$. [4 marks]

(b) Find the answer of $1930^{2761} \bmod 2867$. [4 marks]

# Question 7 [8 marks]

Consider a public-key crytposystem with three users: $A$, $B$, and $C$. Assume all necessary keys have been created and distributed to the relevant users.

(a) List the set of keys that user $A$ knows (or can easily discover). [1 mark]

(b) List the set of keys that user $A$ knows, but users $B$ and $C$ do not. [1 mark]

(c) If user $A$ wants to send a confidential message $M$ to user $B$, then explain what user $A$ does. [1.5 marks]

(d) Explain why the message $M$ is confidential, i.e. user $C$ cannot read it. [1.5 marks]

(e) If user $C$ wants to send an authenticated message $M$ to user $B$, then explain what user $C$ does. [1.5 marks]

(f) Explain how $B$ is certain the message comes from $B$, and not $A$ pretending to be $B$. [1.5 marks]

# Question 8 [6 marks]

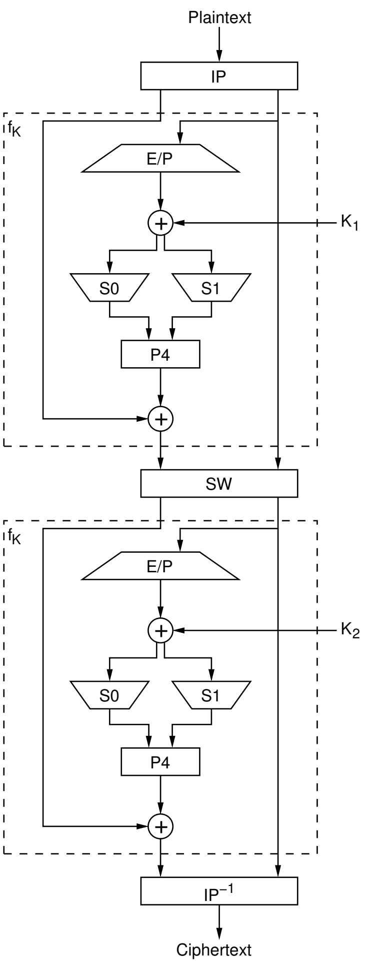
Assuming the output of the first application (round) of $f_K$ of S-DES is `11010111` and $K_2$ is `10111001`, what is the output ciphertext? You may use the information below (note: you need to determine $IP^{-1}$ yourself).

`C = ___ ___ ___ ___ ___ ___ ___ ___`

(write your final answer above; show calculations below)

`IP: 2 6 3 1 4 8 5 7  E/P: 4 1 2 3 2 3 4 1  P4: 2 4 3 1`

$$S0 = \begin{bmatrix} 01 & 00 & 11 & 10 \\ 11 & 10 & 01 & 00 \\ 00 & 10 & 01 & 11 \\ 11 & 01 & 11 & 10 \end{bmatrix} \quad S1 = \begin{bmatrix} 00 & 01 & 10 & 11 \\ 10 & 00 & 01 & 11 \\ 11 & 00 & 01 & 00 \\ 10 & 01 & 00 & 11 \end{bmatrix}$$



# Question 9 [7 marks]

The following ciphertext $C$ was obtained by encrypting the original plaintext $P$ with a Rows/Column Transposition cipher using a 5 digit key $K$. What is the original plaintext $P$ and key $K$?

`C = EFSAAAHNPDENPWYRAYTEUOOXY`

`P = _____________________________________________________ K = ___________`

(Write your answer above; perform calculations below)