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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Exam Answers: 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]

Answer. *Access Control: Prevent unauthorised use of a resource. Data Integrity: Assure data received are exactly as sent by authorised entity. Nonrepudiation: Protect against denial of one entity involved in communications of having participated in communications. Availability: System is accessible and usable on demand by authorised users according to intended goal.*

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

Answer. *A passive attack does not modify the system or network resources (when compared to normal operation without an attack), whereas an active attack does.*

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

Answer. *Modification: attacker modifies a message before it reaches the intended recipient. Masequerade: attacker sends a message, pretending to be someone else. Replay: attacker re-sends an identical copy of a previously sent message. Denial of servce: attacker performs operations such that normal service cannot be used.*

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]

Answer. $2^4!$

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

Answer. $4 \times 2^4 = 64$ *bits*

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

Answer. *If small blocks are used, it is easy to use statistical analysis to break the cipher. With large blocks, the key length will be too long.*

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 = _____`

Answer. *Considering the first pair, encrypt the plaintext with all possible values of K_1, and also decrypt the corresponding ciphertext with all possible values of K_2.*

$$P = 1101$$

$$K_{1,1} = 00 : X_{1,1} = 1000$$
$$K_{1,2} = 01 : X_{1,2} = 1010$$
$$K_{1,3} = 10 : X_{1,3} = 0100$$
$$K_{1,4} = 11 : X_{1,4} = 1110$$

$$C = 1100$$

$$K_{2,1} = 00 : X_{2,1} = 0100$$
$$K_{2,2} = 01 : X_{2,2} = 0000$$
$$K_{2,3} = 10 : X_{2,3} = 1110$$
$$K_{2,4} = 11 : X_{2,4} = 1010$$

The values of X that match are: $(X_{1,2}, X_{2,4})$, $(X_{1,3}, X_{2,1})$ and $(X_{1,4}, X_{2,3})$. This indicates the keys are either: $(K_{1,2} = 01, K_{2,4} = 11)$, $(K_{1,3} = 10, K_{2,1} = 00)$ or $(K_{1,4} = 11, K_{2,3} = 10)$. To know which keys, then try with the second plaintext/ciphertext pair.

$$P = 1001$$

$$K_{1,2} = 01 : X_{1,2} = 0000$$

$$X_{1,2} = 0000$$

$$K_{2,4} = 11 : C_{2,4} = 0010$$

The ciphertext obtained (`0010`) does not match the expected value (`1101`). Hence this set of keys is incorrect. Now try the next set:

$$P = 1001$$

$$K_{1,3} = 10 : X_{1,3} = 1110$$

$$X_{1,3} = 1110$$

$$K_{2,1} = 00 : C_{2,1} = 0011$$

Again, no match. That implies the third set should be correct. Lets try:

$$P = 1001$$

$$K_{1,4} = 11 : X_{1,4} = 0111$$

$$X_{1,4} = 0111$$

$$K_{2,3} = 10 : C_{2,3} = 1101$$

As expected, the ciphertext matches. Hence the keys are `11` *and* `10` *or together* `1110`*.*

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]

`___ ___ ___ ___`

Answer. *23, 7, 19, 10*

(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]

Answer. *m; it should be prime and as large as possible for computer*

(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]

`__ __ __ __ __ __ __ __ __ __ __ __ __ __ __ __`

Answer. *`1100010000011101`. This is obtained by encrypting plaintext `0000` with key `01`, then encrypting `0001`, `0010` and `0011`.*

(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]

Answer. *With LCG, once an attacker know several values in the sequence it is easy to determine the parameters, and then predict subsequent values. With the block cipher, knowing several values does not make it possible to predict the key, and hence hard to predict upcoming values.*

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 = _____

Answer. *answernine*

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

P = _____

Answer. *answerfive*

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

Answer. *Even with unlimited resource/time, the cipher is unbreakable, i.e. attacker cannot determine correct plaintext given a ciphertext.*

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

Answer. *For long plaintexts, repetition of the key leads to structure in the ciphertext that the attacker can take advantage of to determine the plaintext.*

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]

Answer. *A one-to-one mapping means each input plaintext letter produces a unique ciphertext letter.*

(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]

Answer. *Any value relatively prime with 26 and greater than 3. E.g. 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.*

(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]

Answer. *Any value greater than 3 and less than 26 that is not relatively prime with 26, e.g. 4, 6, 8, 10, 13, 14, 16, 19, 20, 22, 24.*

(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]

Answer.

$$D = \mathrm{D}([a, b], p) = \mathrm{MI}(a)(p - b) \bmod 26$$

(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]

Answer. *For a one-to-one mapping a must have a multiplicative inverse in* mod *n. That is true of a and n are relatively prime. The number of numbers relatively prime with n (and less than n) is* $\phi(n)$.

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, 23×46).

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

Answer. *First recognise that 53 is a prime number, therefore taking advantage of one of the theorems would be beneficial. However the expression does not directly match either of the theorems. However consider an expansion based upon properties of multiplication in modular arithmetic (and then using Fermat's theorem):*

$$\begin{aligned} 49^{55} \bmod 53 &= 49^{53+2} \bmod 53 \\ &= (49^2 \times 49^{53}) \bmod 53 \\ &= [(49^2 \bmod 53) \times (49^{53} \bmod 53)] \bmod 53 \\ &= [(2401 \bmod 53) \times (49 \bmod 53)] \bmod 53 \\ &= [16 \times 49] \bmod 53 \\ &= 784 \bmod 53 \\ &= 42 \end{aligned} \tag{1}$$

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

Answer. *Here we will try to use Euler's theorem. If we assume* $n = 2867$*, then to use Euler's theorem, then* $\phi(2867)$ *must equal* 2760*. Does it? If we recognise that the two prime factors of* 2867 *are* 47 *and* 61*, then* $\phi(2867)$ *can be calculated as* $(47-1) \times (61-1)$ *which is* 2760*. Hence Euler's theorem can be applied, giving the answer of* 1930*.*

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]

Answer. PU_a, PR_a, PU_b, PU_c

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

Answer. PR_a

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

Answer. *User A encrypts M using key PU_b, and then sends the ciphertext to B*

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

Answer. *User C receives the ciphertext but cannot decrypt because they do not know the key PR_b.*

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

Answer. *User C encrypts M using key PR_c, and then sends the ciphertext to B*

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

Answer. ***There is a mistake in this part. It should be "Explain how C . . . ". This part was not marked.*** *The message only successfully decrypts with the corresponding key that it was encrypted with. If it decrypts with PU_b then it means it must have been encrypted with PR_b, which C knows only B has (A does not know PR_b).*

Question 8 [6 marks]

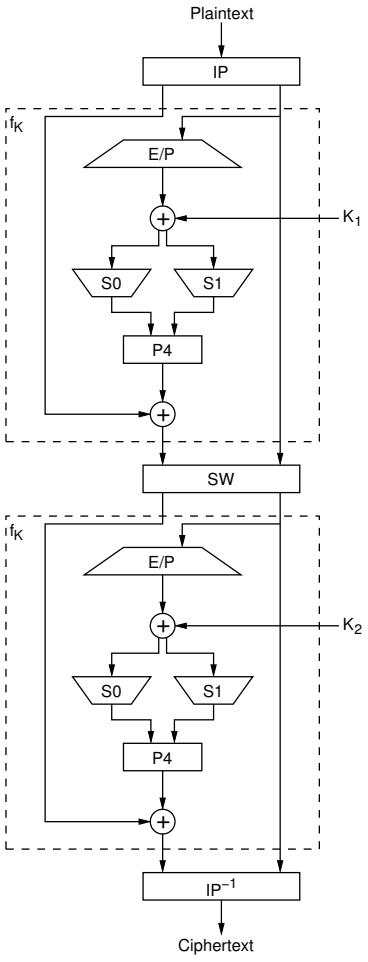
Assuming the output of the first application (round) of f_K of S-DES is `11010111` and K_2 is `10111001`, what is the output ciphertext? You may use the information below (note: you need to determine IP^{-1} yourself).

`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`

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



Answer. *Output of* f_K*:* `1101 0111`
Swap halves: `0111 1101`
E/P right half: `1110 1011`
XOR with K_2*:* `0101 0010`
SBox S0: `01`
SBox S1: `01`
Output of SBox: `0101`
P4: `1100`
XOR with left half: `1011`
Combined with right half: `1011 1101`
IP^{-1}*: 4 1 3 5 7 2 8 6*
Answer: `11110011`

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)

Answer. ***There is a mistake in this question. The given ciphertext doesn't produce any meaningful plaintext. When creating the question I made a mistake, reading the rows instead of the column. The ciphertext should be: FHNAOEAERUSNPYOAPWTXADYEY. Then the answer below is correct. This question was not marked.*** *There are 25 characters. With a 5 digit key there must be 5 columns, and hence the ciphertext can be written as:*

```
f e s a a
h a n p d
n e p w y
a r y t e
o u o x y
```

Now we need to determine the ordering of the columns such that an English phrase is constructed. Lets try different variations of the first row. We'd expect the word to start with a consonant (f or s) following by vowel or vice versa: `fe? fa? se? sa? af? as? ef? es?`*. Exploring the subsequent letters, some words that can be made with the first 5 letters are:* `safe` *and* `as`*. Consider* `safe`*, the two possible arrangements are:*

```
s a f e a
n p h a d
p w n e y
y t a r e
o x o u y
```

and

```
s a f e a
n d h a p
p y n e w
y e a r t
o y o u x
```

The second arrangement produces: safe and happy new year to you *(assuming the last character x is for padding). With this message the key is: 35124.*