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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2009

Course Title : CSS322 Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 21 December 2009, 13:30 to 16:30

Instructions:

- This examination paper has 14 pages (including this page).
- Condition 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.
- Turn off all communication devices (mobile phone etc.) and leave them under your seat.
- Write your name, student ID, section, and seat number clearly on the answer sheet.
- The space on the back of each page can be used if necessary.

Questions [100 marks]

Question 1 [11 marks]

a) Given the ciphertext and key below, find the plaintext if the Playfair cipher was used. *x* is the special character used for padding and *i* and *j* are treated as the same character. [4 marks]

C = eiioqoyldc

K = security

P = ______________________ (write your final answer here; show your calculations below)

b) The following ciphertext was obtained by encrypting the original plaintext *P* with a Rows/Column Transposition cipher using a key K. No padding was necessary. What is the original plaintext and key K? (Hint: the 5th character of the plaintext is *y*; Note: this question may take you a long time – complete other questions before attempting a brute force attack) [7 marks]

C = r a a y e m x n p w y a a e r e m d p y r s h n a

K = ____________________

P = ____

(write your final answers above; show calculations below and on back of sheet)

Question 2 [14 marks]

Consider a modified Vigenere cipher where the set of characters are the hexadecimal digits (instead of letters from the English alphabet).

a) If P_i is the ith digit of the plaintext, C_i is the ith digit of the ciphertext, and K_i is the ith digit of the key, write equations for the encryption and decryption operations: [4 marks]

E(P_i,K_i) = C_i = ____

D(C_i,K_i) = P_i = ____

b) For P = 3AE60A3 and keyword = 17E, what is C? [3 marks]

C = ___ ___ ___ ___ ___ ___ ___ (write final answer here; show calculations below)

c) A polyalphabetic cipher such as the above Vigenere is stronger against letter frequency analysis when compared to a monoalphabetic cipher like Caesar. Explain why (hint: the answer in part (b) may help). [2 marks]

d) Despite being stronger than monoalphabetic ciphers, the Vigenere cipher is still subject to letter frequency attacks. Explain why (hint: the answer in part (b) may help). [2 marks]

e) Can the modified Vigenere cipher in this question be used as a one-time pad. If yes, then explain how. If no, then explain why not. [3 marks]

Question 3 [10 marks]

Consider a block cipher, called *A*, shown in the table below. The table gives the ciphertext *C* produced when encrypting the plaintext *P* with one of the four keys.

	C			
P **K**	**00**	**01**	**10**	**11**
0000	1111	0000	0101	0001
0001	0001	0010	1001	0111
0010	1010	0101	0111	1000
0011	0111	1010	0010	1111
0100	1000	1001	1100	0101
0101	1100	1110	1011	1010
0110	1011	0111	1110	0100
0111	0000	1111	0001	1110
1000	1110	0001	1101	0110
1001	1001	0011	1000	1011
1010	0100	1100	0000	1101
1011	0110	1101	0100	1001
1100	0101	0100	0110	0010
1101	1101	0110	1111	0000
1110	0010	1000	0011	1100
1111	0011	1011	1010	0011

Using cipher *A* and one of the following modes of operation, decrypt the ciphertext *C* with key *K*:

C	1101 0100 1100 0100
K	00

In all cases assume any initial values are 0. Write your answers below and show the calculations in the space provided on the next page:

a) Counter: ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

b) CBC: ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___ ___

a) Counter Mode (calculations) [5 marks]

b) CBC, Cipher Block Chaining (calculations) [5 marks]

Question 4 [12 marks]

In all parts of this question assume an attacker can identify the correct plaintext when performing attacks.

Consider a block cipher *B* with *n*-bit plaintext input and a *k*-bit key. Assume an encrypt operation takes 1µs and a decrypt operation takes 1µs.

a) In the worst case, how many microseconds (µs) will it take an attacker to find the plaintext/key if a brute force attack is applied on cipher *B*? [2 marks]

Consider a block cipher, *Double-B*, which involves applying the block cipher *B* 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 *k*-bit key.

b) In the worst case, how many microseconds (µs) will it take an attacker to find the plaintext/key if a brute force attack is applied on cipher *Double-B*? [2 marks]

c) If the attacker applied a meet-in-the-middle attack on *Double-B*, what is the *approximate* time it takes to find the plaintext/key? [2 marks]

d) Show how the meet-in-the-middle attack works by applying it against *Double-A*, where cipher *A* is given in Question 3. Use the attack to find the key used if the attacker already knows the (plaintext, ciphertext) pairs:

(1110, 0111)

(0100, 1101)

Explain clearly the steps applied by the attacker and how the key is identified. (Use the back of the sheet if necessary)[6 marks]

Question 5 [9 marks]

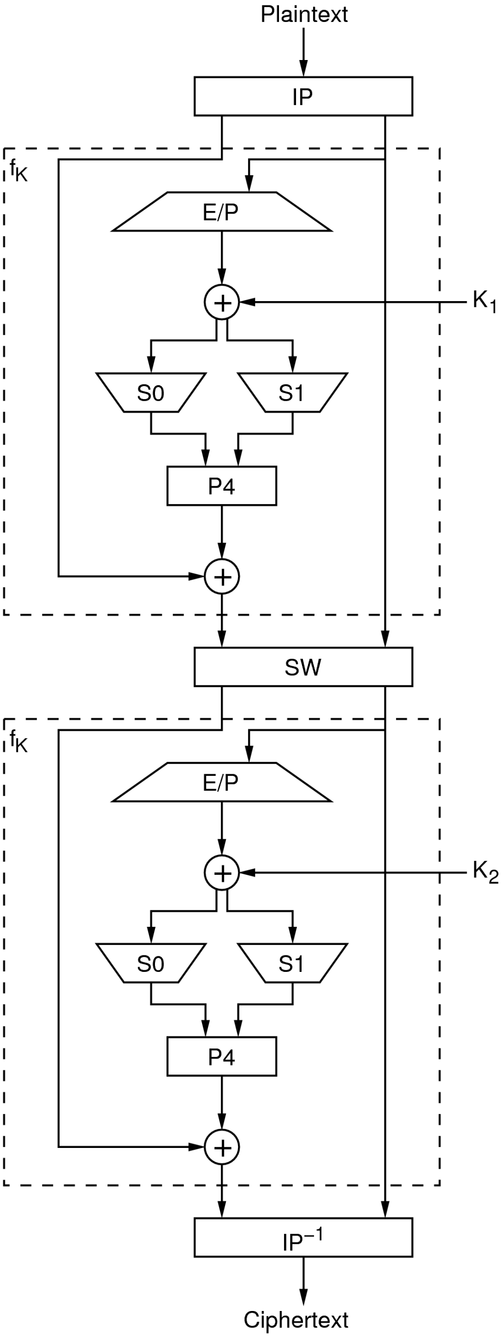
Assuming the output of the first application (round) of f_K of S-DES is 00101011 and K_2 is 10111001, what is the output ciphertext? You may use the information below (note: you need to determine IP^{-1} yourself).

C = ___ ___ ___ ___ ___ ___ ___ ___

(write your final answer above; show calculations on next page)

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

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



(calculations for S-DES)

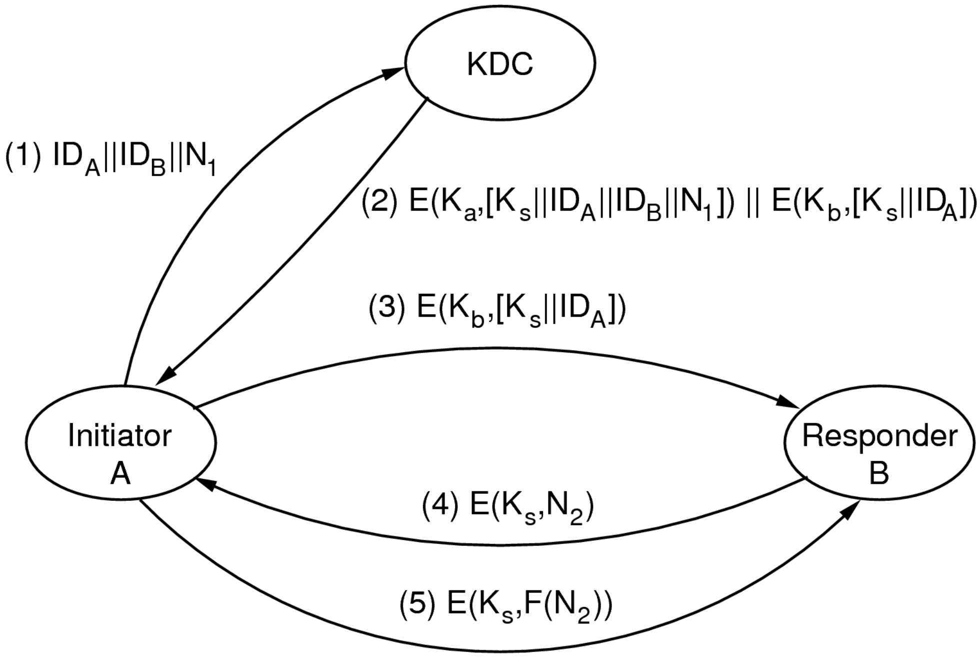
Question 6 [16 marks]

Consider a network containing 100 hosts. Each host runs 3 network applications (a file sharing application, voice call application, and instant messaging application), and each application should be able to communicate with the corresponding application on any other host (e.g. voice on host 1 with voice on host 2; but not voice on host 1 with file sharing on host 2).

a) If host-level symmetric key security is required in the network, what is the maximum number of session keys needed? [2 marks]

b) If application-level symmetric key security is required in the network (for the 3 applications), what is the maximum number of session keys needed? [2 marks]

The figure below shows a typical key distribution protocol when using a Key Distribution Centre (KDC). Assume the nonce values, N_1 and N_2, are chosen randomly by the sender.



c) Considering only host-level symmetric key security, how many master keys are needed for the network of 100 hosts? [2 marks]

d) In the key distribution protocol, what information must be known by the KDC *before* step 1 can occur? [2 marks]

e) Explain why an attacker, after intercepting message (2), does not know the value of K_s. [2 marks]

f) Explain the purposes of messages (4) and (5), including what type of attack they can prevent, how they can be used to prevent an attack (e.g. how the attack is detected), and what is an appropriate function F. [4 marks]

g) Explain an advantage of using the KDC based approach for key distribution. [1 mark]

h) Explain a disadvantage of using the KDC based approach for key distribution. [1 mark]

Question 7 [10 marks]

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

Fermat's theorem: $a^p \equiv a \pmod{p}$ if p is prime

Euler's theorem: $a^{\Phi(n)+1} \equiv a \pmod{n}$

First 20 prime numbers: 2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71

a) Find the answer of 54^{3433} mod 3551. Show your calculations (e.g. explain which theorem(s) can be used and why; do not use a calculator). [5 marks]

b) Show that $7^{60} \equiv 34 \pmod{47}$. Show your calculations (do not use a calculator). [5 marks]

Question 8 [8 marks]

a) List the names of five security services desired in computer networks. For each service, explain what the service means. [5 marks]

b) Describe one passive and one active attack that can occur in computer networks. [3 marks]

Active attack

Passive attack

Question 9 [10 marks]

Suppose A and B want to confirm that they are both in possession of the same secret key. Consider this scheme to provide such confirmation: A creates a random sequence of bits the length of the key, XORs the random bits with the key, and sends the result over the network to B. B XORs the received bits with B's key (which is supposed to be the same as A's key) and sends back the result. A compares the received result with the original random bits to determine if the keys held by A and B are the same. In this scheme, neither A nor B transmit the key over the network.

a) Prove that the scheme works. (that is, if the keys held by A and B are the same, then A can confirm this; and if they are different, A will detect this). [6 marks]

b) Show how an attacker can take advantage of this scheme to discover the secret key. [4 marks]