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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination Answers: 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 16 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)

Answer

With K = security the Playfair matrix is:

s	e	c	u	r
i/j	t	y	a	b
d	f	g	h	k
l	m	n	o	p
q	v	w	x	z

Considering the ciphertext C, find the pairs of input plaintext:

C =	ei	io	qo	yl	dc
P =	st	al	xl	in	gs

P = stalxlings

As there are two *l*'s separated by an *x*, remove the special padding character *x* to get the original plaintext:

P = stallings

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)

Answer

There are 25 characters. Since no padding is used that means the 25 characters must evenly be divided across the columns. The practical option is only: 5 rows by 5 columns. Hence write every 5 characters in a column.

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

Now we need to choose the correct ordering of columns. Consider the first 5 letters: rmyer. How can they be arranged? The hint says the 5th character is an *y*. The possible arrangements are

rmery	rmrey	rremy	rrmey	remry	rermy
mrery	mrrey	merry			
emrry	ermry	errmy			

Of these, *merry* is the only word that makes sense, so lets try it. Possible ordering of columns are:

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

or

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

The second ordering gives a readable plaintext message: merry xmas and a happy new year. The key is: 24153.

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 = ____

Answer

E(P_i,K_i) = C_i = (P_i + K_i) mod 16

D(C_i,K_i) = P_i = (C_i - K_i) mod 16

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

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

Answer

P	3	A	E	6	0	A	3
K	1	7	E	1	7	E	1
C	4	1	C	7	7	8	4

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]

Answer

With a monoalphabetic cipher the same input plaintext character will always encrypt to the same ciphertext letter. Hence it is easy to count the frequencies of letters in the ciphertext and determine the mapping from the expected frequency of letters in the plaintext. With a polyalphabetic cipher the same input plaintext letter often will not encrypt to the same ciphertext letter. For example, above A encrypts to 1 and 8, because the key changes.

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]

Answer

With long plaintext and short keys, repetitions in the key may lead to occurrences of the same input plaintext character encrypting to the same ciphertext letter. For example, above 3 maps to 4 and because the the short, repeated key, 3 maps to 4 again at the end. This pattern can be exploited for letter/diagram frequency analysis.

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]

Answer

Yes.

The key must be the same length as the input plaintext.

The key must be random.

The key must be changed for each encryption.

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:

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

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

a) Counter Mode (calculations) [5 marks]

Answer

Block 1: E(0000,00) = 1111

P1 = C1 XOR 1111

= 1101 XOR 1111

= 0010

Block 2: E(0001,00) = 0001

P2 = C2 XOR 0001

= 0101

Block 3: E(0010,00) = 1010

P3 = C3 XOR 1010

= 0110

Block 4: E(0011,00) = 0111

P4 = C4 XOR 0111

= 0011

P = 0010 0101 0110 0011

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

Answer

IV: 0000

Block 1: D(1101,00) = 1101

1101 XOR 0000

P1 = 1101

Block 2: D(0100,00) = 1010

1010 XOR 1101

P2 = 0111

Block 3: D(1100,00) = 0101

0101 XOR 0100

P3 = 0001

Block 4: D(0100,00) = 1010

1010 XOR 1100

P4 = 0110

P = 1101 0111 0001 0110

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]

Answer

2^{k} µs

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]

Answer

2^{2k} µs

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]

Answer

2^{k+1} µs

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. [6 marks]

Answer

Using the first known (plaintext, ciphertext) pair, the attacker attempts a brute force on the input plaintext:

1110	K=00	=> X1p =0010
1110	K=01	=> X2p =1000
1110	K=10	=> X3p =0011
1110	K=11	=> X4p =1100

Then using the output ciphertext the attacker decrypts:

1101	K=00	=> X1c = 0011

1101	K=01	=> X2c = 0110
1101	K=10	=> X3c = 0010
1101	K=11	=> X4c = 0001

There are two values of X that match: X1p and X3c (K = 0010); and X3p and X1c (K = 1000). The attacker can try again with the second (plaintext, ciphertext) pair, considering those possible keys:

0100	K=00	=> X =1000	1101	K=10	=> X = 1000
0100	K=10	=> X =1100	1101	K=00	=> X = 1101

Only K = 0010 produces a correct value of X and hence this is the key.

Question 5 [9 marks]

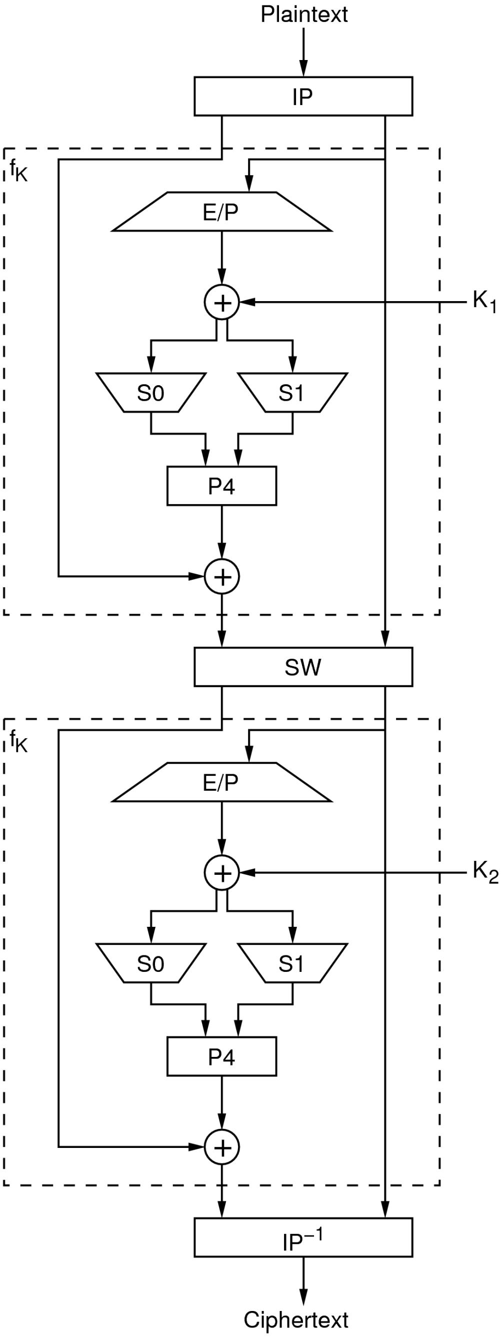
Assuming the output of the first application (round) of f_K of S-DES is 00101011 and K_2 is 10111001, what is the output ciphertext? You may use the information below (note: you need to determine IP^{-1} yourself).

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

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



Answer

00101011 K2: 10111001

Swap halves:	10110010
E/P on right half:	00010100
XOR with K2:	10101101
Output of S0:	10
Output of S1:	00
P4:	0001
XOR with left half:	1010
IP-1 [4 1 3 5 7 2 8 6]:	01101000
Ciphertext:	01101000

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]

Answer

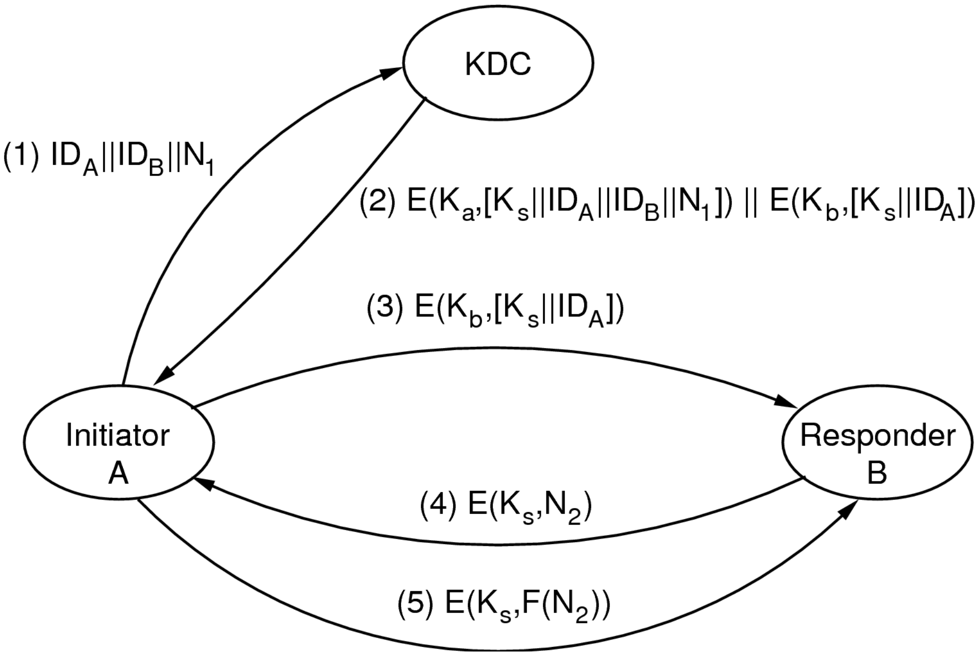
Each host must have a session key with every other host. Total session keys = 100 x 99 / 2 = 4950 keys.

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]

Answer

Each application must have a session key with the corresponding application on other host. Total session keys = 3 x (100 x 99 /2) = 14850 keys

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]

Answer

Each host must exchange a master key with the KDC. Therefore 100 master keys.

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

Answer

KDC must know the IDs and master keys of A and B: ID_A, ID_B, K_a, K_b.

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

Answer

The first instance of K_s is encrypted with K_a and the second instance is encrypted with K_b. The attacker does not know either K_a or K_b and therefore cannot determine K_s.

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]

Answer

The messages are used to prevent an attacker replaying message (3), masquerading as A. If the attacker replays (3) then B will respond with a nonce value encrypted with Ks. B expects a reply containing the function F of the nonce value, where the function may be incrementing the value by 1. Since the attacker cannot determine the nonce value, it cannot send back the valid response.

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

Answer

Automates the distribution of session keys, so that only Master keys need to exchanged manually.

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

Answer

Requires the KDC to be trusted. If the KDC is compromised then the security of the system fails. The KDC can be a performance bottleneck in the system.

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]

Answer

Using Euler's theorem, if n is 3551, then find $\Phi(3551)$. It is difficult to find this manually, but if we notice that 3551 is in fact 53x67 (multiplication of 2 prime numbers) then $\Phi(3551)$. = 52x66 = 3432. Therefore the statement is in the form of Euler's theorem which says the answer is 54.

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

Answer

7^{60} mod 47 = (7^2 mod 47)^{30} mod 47

= 2^{30} mod 47

= (2^6 mod 47)^5 mod 47

= (17 mod 47)(289 mod 47)(289 mod 47) mod 47

= 17 x (7 x 7 mod 47) mod 47

= 34 mod 47

= 34

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]

Answer

Authentication: assure message and communicating parties are authenticate.

Confidentiality: keep message contents private/secret.

Integrity: assure data is not modified during transmission.

Non-repudiation: prevent sender or receiver from denying communications took place.

Access control: limit and control access to resources.

Availability: assure that the system is available to users.

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

Active attack

Passive attack

Answer

Authentication: masquerade – attacker pretends to be someone else (active)

Confidentiality: release message contents – an attacker intercepts messages and reads their contents (passive)

Integrity: modification – attacker modifies messages (active)

Non-repudiation: modification – an attacker modifies a message after being received to be able to deny receiving a particular message (active)

Access control: masquerade attacker pretends to be someone else in order to avoid access control mechanisms (active)

Availability: denial of service – an attacker overloads the computer system so it is no longer available (active).

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]

Answer

Lets define:

R = random bits

Ka = key held by A

Kb = key held by B

Mab = message sent by A to B

Mba = message sent by B to A

The scheme works as follows:

At A: Mab = R ⊕ Ka

A sends Mab to B

At B: Mba = Mab ⊕ Kb

B sends Mba to A

At A: A compares Mba with R; if they are equal, then Ka = Kb. Why?

The property of ⊕ is: if A ⊕ B = C then A = B ⊕ C

So if Ka = Kb, then Mab = R ⊕ Ka and Mba = Mab ⊕ Ka = R ⊕ Ka ⊕ Ka = R ⊕ 0 = R

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

Answer

If the attacker intercepts the two messages, they can find Ka (assuming keys are the same):

Mab = R ⊕ Ka and Mba = Mab ⊕ Ka = R

Mab ⊕ Mba = R ⊕ Ka ⊕ R = Ka