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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2007

Course Title : CSS 322 – Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 7 January 2008, 9:00 – 12:00

Instructions:

- This examination paper has 20 pages (including this page).
- Condition of Examination
  Closed book (No dictionary, **Non-programmable calculator 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.
- For you convenience, the mappings of English letters to numbers are given in the last page.

Answers

Part A - Multiple Choice Questions [14 marks]

Select the most accurate answer (only select one answer). Each correct answer is worth 2 marks.

1. If your computer could decrypt at a speed of 1 decryption per 1 nanosecond (ns), then a brute force attack on a 128-bit key would on average take:
   a) 2^{63} ns
   b) 2^{64} ns
   c) 2^{127} ns
   d) 2^{128} ns
   e) 2^{129} ns

2. What is the hardest type of attack to perform for most encryption algorithms:
   a) Chosen ciphertext
   b) Known plaintext
   c) Chosen plaintext
   d) Ciphertext only
   e) Chosen text

3. DES is no longer recommended for use because:
   a) The Feistel structure does not provide adequate security
   b) The default key size is too small
   c) It is inefficient when compared to Triple DES
   d) The S-Boxes used are not secure
   e) RSA is a better replacement

4. The Avalanche Effect is an indicator of the security of encryption algorithms. The aim is that:
   1. Small changes in the key produce large changes in the ciphertext
   2. Small changes in the key produce small changes in the ciphertext
   3. Small changes in the plaintext produce small changes in the ciphertext
   4. The ciphertext is not changed if the same key is used, but with different plaintext

5. If using the Linear Congruential Pseudo Random Number Generator

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

   a) An attacker knowing the generator parameter values and previous random number, can predict the next random number.
   b) The same sequence of numbers will never be repeated.
   c) Reducing the size of the modulus *m*, gives a better random sequence.
   d) The same sequence of numbers is generated, even if the initial value of X_0 is changed.

Answers

6. End-to-end encryption:
   a) Requires encryption and decryption to occur at every device in the path (e.g. routers and switches)
   b) Can hide the network (e.g. Internet Protocol) and link layer headers so that attackers cannot determine the destination IP address
   c) Makes it easy to hide your traffic patterns (compared to link-level encryption)
   d) Allows users to create a secure connection without having to trust network operators
   5. Requires you to use symmetric key cryptography

7. The use of a Key Distribution Centre (KDC):
   a) Requires trust between users and the KDC
   b) Requires users to exchange Master Keys
   c) Requires a session key to be exchanged between a user and KDC
   d) Requires one Master Key for every pair of users
   e) Requires data to be sent between a pair of users to be encrypted with a Master Key

Answers

Part B – General Questions [86 marks]

Question 1 [6 marks]

a) Explain the difference between an active attack and a passive attack on network security. [3 marks]

An active attack modifies the system resources, while a passive attack does not.

Further explanation: Consider the normal system (i.e. sender and receiver) without an attack. For example, what messages does the sender send and what messages does the receiver receive. Now consider an attack is introduced into the system: for an active attack, the messages sent by the sender and/or the messages receiver by the sender will be different than normal system behaviour (that is, the system resources are altered). For a passive attack, the messages sent by the sender and received by the sender will be the same as normal system behaviour.

Note: It is not accurate to say that an "active attack modifies messages" – an active attack may not modify messages, but still modify system resources.

b) List *and describe* two active attacks and two passive attacks on network security. [3 marks]

Two passive attacks:

Release message contents. An attacker intercepts messages and reads the contents (hence the contents of an intended private message are released to unintended recipients).

Traffic analysis.

Answers

Question 2 [6 marks]

List *and describe* four security services desired in computer networks.

Answers

Question 3 [10 marks]

a) Encrypt the word “security” using the Vigenere cipher with keyword “crypto”. Assume a = 0, b = 1 and so on. (see the last page of the exam for the complete mappings). [5 marks]

b) Explain how the Vigenere cipher improves resistance against letter frequency attacks when compared to monoalphabetic ciphers. [2 marks]

c) Explain why the Vigenere cipher is still susceptible to letter frequency attacks (Hint: consider the lengths of the plaintext and keyword). [3 marks]

Answers

Question 4 [5 marks]

The plaintext P is encrypted using a rail-fence cipher to produce the ciphertext, C:

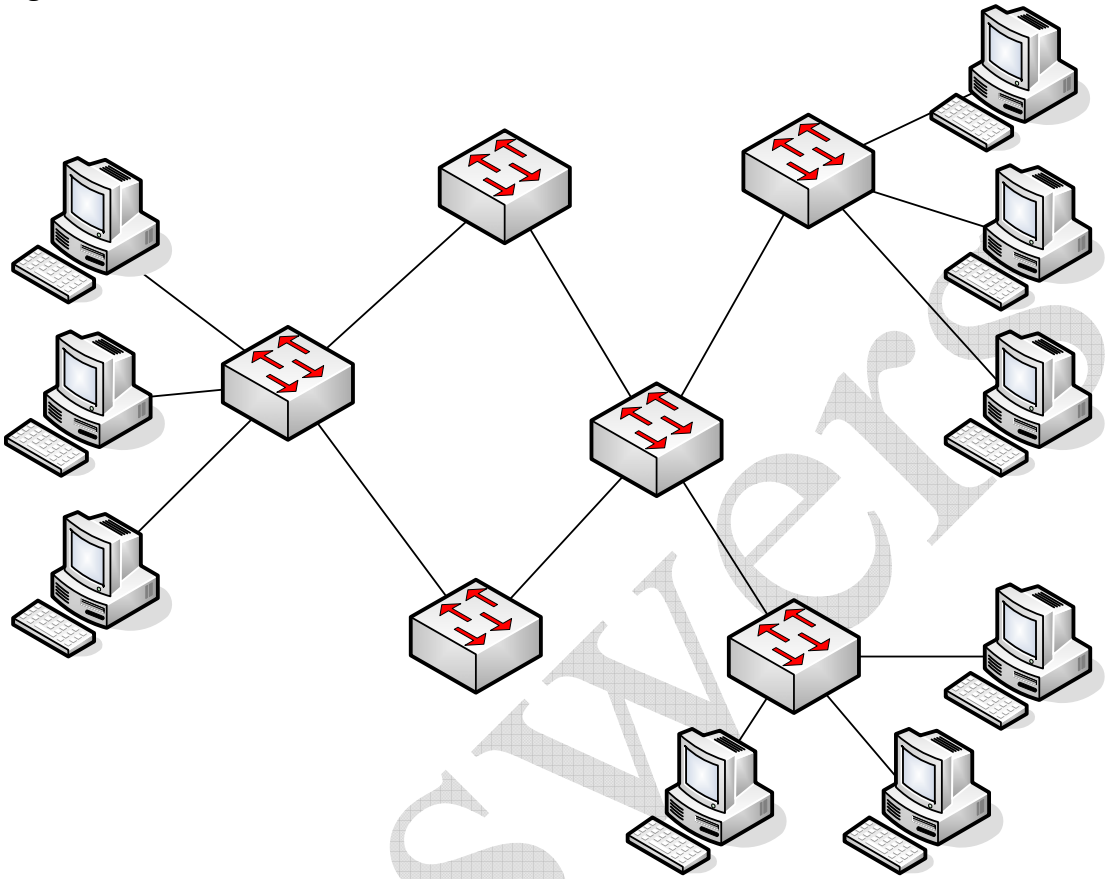
TMSUVSYHMANEIXAATIRTX

What is the plaintext P?

Answers

Question 5 [11 marks]

The following diagram shows a switched computer network, connecting 9 computers together via 6 switches. There are no other connections.



a) For the following cases, calculate the number of keys that are needed in the network assuming symmetric key encryption is used (explain your answer and/or show the calculations):
   i. Link level encryption is used (computer-to-switch, and switch-to-switch). [2 marks]

Answers

ii. End-to-end encryption at the Network layer (IP) is used. [2 marks]

iii. End-to-end encryption at the Application layer is used, assuming there are at most 5 different applications on each computer that need to use encryption. [2 marks]

b) Explain why a Key Distribution Centre (KDC) should be used when using end-to-end encryption in a network with many computers. (Hint: You may use the example network to help explain your answer.) [3 marks]

c) Explain a disadvantage of using a KDC. [2 marks]

Answers

Question 6 [9 marks]

Assume a symmetric key encryption algorithm encrypts the following 4-bit plaintext messages to the corresponding 4-bit ciphertext messages using a key K. For an input 16-bit plaintext message of 0111 1001 1011 0010, what is the ciphertext if the following modes of operation are used (assume any initial values used are all 0's):

Plaintext	Ciphertext	Plaintext	Ciphertext
0000	1110	1000	1100
0001	0101	1001	0100
0010	1001	1010	0110
0011	0010	1011	1101
0100	1111	1100	1000
0101	0111	1101	1011
0110	0000	1110	0011
0111	1010	1111	0001

a) Electronic Codebook [3 marks]

b) Cipher Block Chaining [3 marks]

Answers

c) Counter [3 marks]

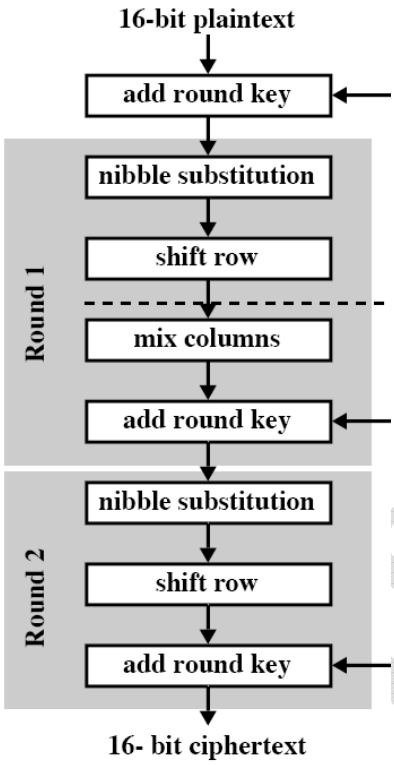
Answers

Question 7 [8 marks]

Assuming the plaintext P = 1001 0111 1001 0011 and the round keys are given as below, what is the output of Round 1 in Simplified AES?

Key 0 = 1000 1100 1010 1111
Key 1 = 0110 0101 1010 0011
Key 2 = 0100 0001 1101 1001

The encryption algorithm, encryption S-Box, mix column encryption and GF(2^4) addition and multiplication tables are shown below.



Encryption S-Box:

$$\begin{bmatrix} 1001 & 0100 & 1010 & 1011 \\ 1101 & 0001 & 1000 & 0101 \\ 0110 & 0010 & 0000 & 0011 \\ 1100 & 1110 & 1111 & 0111 \end{bmatrix}$$

Mix columns:

$$\begin{bmatrix} 1 & 4 \\ 4 & 1 \end{bmatrix} \begin{bmatrix} S_{0,0} & S_{0,1} \\ S_{1,0} & S_{1,1} \end{bmatrix} = \begin{bmatrix} S'_{0,0} & S'_{0,1} \\ S'_{1,0} & S'_{1,1} \end{bmatrix}$$

(your answer can continue to page 14)

Answers

GF(2^4) addition table:

+	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
1	1	0	3	2	5	4	7	6	9	8	B	A	D	C	F	E
2	2	3	0	1	6	7	4	5	A	B	8	9	E	F	C	D
3	3	2	1	0	7	6	5	4	B	A	9	8	F	E	D	C
4	4	5	6	7	0	1	2	3	C	D	E	F	8	9	A	B
5	5	4	7	6	1	0	3	2	D	C	F	E	9	8	B	A
6	6	7	4	5	2	3	0	1	E	F	C	D	A	B	8	9
7	7	6	5	4	3	2	1	0	F	E	D	C	B	A	9	8
8	8	9	A	B	C	D	E	F	0	1	2	3	4	5	6	7
9	9	8	B	A	D	C	F	E	1	0	3	2	5	4	7	6
A	A	B	8	9	E	F	C	D	2	3	0	1	6	7	4	5
B	B	A	9	8	F	E	D	C	3	2	1	0	7	6	5	4
C	C	D	E	F	8	9	A	B	4	5	6	7	0	1	2	3
D	D	C	F	E	9	8	B	A	5	4	7	6	1	0	3	2
E	E	F	C	D	A	B	8	9	6	7	4	5	2	3	0	1
F	F	E	D	C	B	A	9	8	7	6	5	4	3	2	1	0

GF(2^4) multiplication table:

	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E	F
2	0	2	4	6	8	A	C	E	3	1	7	5	B	9	F	D
3	0	3	6	5	C	F	A	9	B	8	D	E	7	4	1	2
4	0	4	8	C	3	7	B	F	6	2	E	A	5	1	D	9
5	0	5	A	F	7	2	D	8	E	B	4	1	9	C	3	6
6	0	6	C	A	B	D	7	1	5	3	9	F	E	8	2	4
7	0	7	E	9	F	8	1	6	D	A	3	4	2	5	C	B
8	0	8	3	B	6	E	5	D	C	4	F	7	A	2	9	1
9	0	9	1	8	2	B	3	A	4	D	5	C	6	F	7	E
A	0	A	7	D	E	4	9	3	F	5	8	2	1	B	6	C
B	0	B	5	E	A	1	F	4	7	C	2	9	D	6	8	3
C	0	C	B	7	5	9	E	2	A	6	1	D	F	3	4	8
D	0	D	9	4	1	C	8	5	2	F	B	6	3	E	A	7
E	0	E	F	1	D	3	2	C	9	7	6	8	4	A	B	5
F	0	F	D	2	9	6	4	B	1	E	C	3	8	7	5	A

Access

(use this page for your answer to Question 7)

Answers

Question 8 [10 marks]

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

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

a) A requirement of every encryption algorithm is that it is one-to-one. Explain what this means, using the Affine Caesar Cipher to show an example of a one-to-one mapping and an example of a mapping that isn't one-to-one. [4 marks]

Answers

b) In the Affine Caesar Cipher:

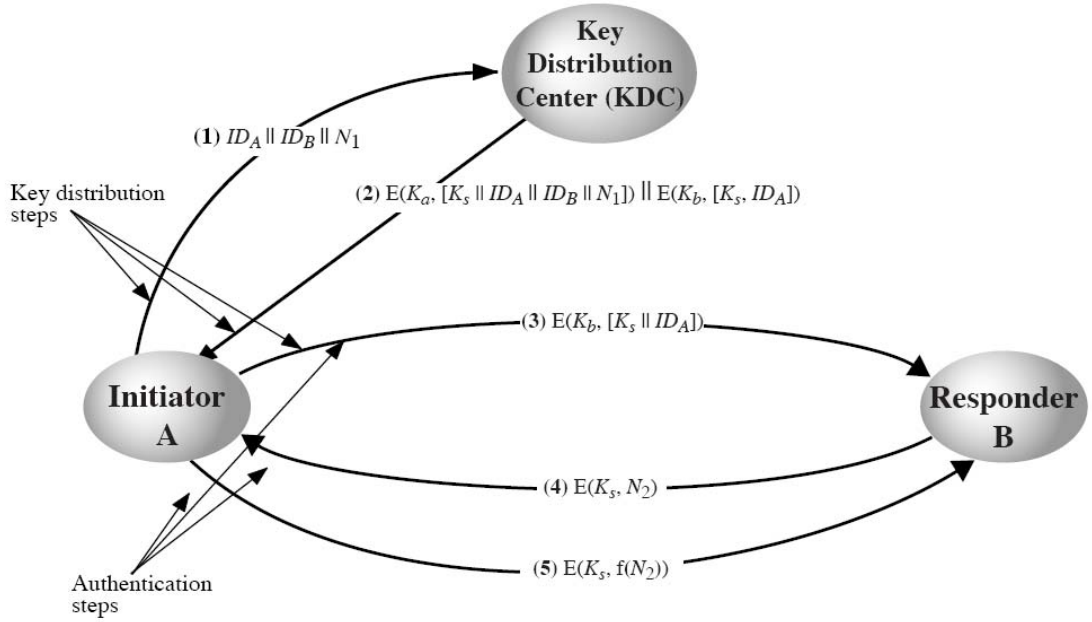
i. What values of *a* are allowed? [3 marks]

ii. What values of *b* are allowed? [3 marks]

Answers

Question 9 [15 marks]

The figure below shows a typical key distribution protocol when using a KDC. The values *N* are nonce values, used to identify the transaction – you can assume they are numbers chosen randomly by the sender, e.g. N_1 is a random number and N_2 is another random number.



a) Explain the purpose of the three keys used, and list who has access to each key. [3 marks]

b) If an attacker intercepts the message from A to B in Step 3, explain:
   a. Why the attacker cannot read K_s? [2 marks]

Answ

b. Why the attacker cannot masquerade as A (by not forwarding the message it intercepted, but instead sending a different message to B)? [2 marks]

c) If A and B want to communicate at a later stage (for example, the next day), should they repeat this entire process? Give an advantage and disadvantage of doing so. [3 marks]

d) Steps (4) and (5) are included to prevent a replay attack. The function *f()* in step (5) increments N_2 by 1. Explain what a replay attack is and how these steps prevent such an attack. [5 marks]

Answers

Question 10 [6 marks]

Assume you designed your own encryption algorithm, *A*, which uses 4-bit blocks and 2-bit keys. The ciphertext for a *selection* of plaintext and keys for the algorithm, *A*, are given below.

	Key			
Plaintext	**00**	**01**	**10**	**11**
0001	1101	0111	1101	0110
0101	0000	0110	0111	1010
0111	0101	1101	1111	0011
1000	0111	1000	1100	1101

To increase the strength of your algorithm, *A*, against brute-force attack, you apply the algorithm twice using a 4-bit key, *K*. The first two bits of *K* are used as a key into *A* to encrypt the plaintext to produce output *X*, and the second two bits of *K* are used as a key into *A* to encrypt *X* to produce the ciphertext. You call this new algorithm *Double-A*.

An attacker has discovered a pair of (plaintext, ciphertext) for *Double-A*:
(0101, 1101)

a) Use the meet-in-the-middle attack to determine the most likely key *K* used to produce this ciphertext. Show/explain your calculations/steps. [3 marks]

b) A limitation of the meet-in-the-middle attack is the amount of memory needed. Explain why, and give the approximate amount of memory needed to perform the attack on Double-DES (which uses two 56-bit keys)? [3 marks]

Answers

Mapping of English Letters to Numbers

a	0
b	1
c	2
d	3
e	4
f	5
g	6
h	7
i	8
j	9
k	10
l	11
m	12

n	13
o	14
p	15
q	16
r	17
s	18
t	19
u	20
v	21
w	22
x	23
y	24
z	25

Answers