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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2006

Course Title : CSS 322 – Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Monday 8 January 2007, 9:00 – 12:00

Instructions:

- This examination paper has 15 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.

Part A - Multiple Choice Questions [20 marks]

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

1. A Certificate Authority:
   a) Certifies that two users have exchanged their public keys
   b) Certifies that the public key of a user, actually belongs to that user
   c) Creates and distributes session keys for users
   d) Is necessary for two users to communicate in private
   e) Is the same as a Key Distribution Centre

2. 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

3. 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

4. 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

5. The Avalanche Effect is an indicator of the security of encryption algorithms. The aim is that:
   a) Small changes in the key produce large changes in the ciphertext
   b) Small changes in the key produce small changes in the ciphertext
   c) Small changes in the plaintext produce small changes in the ciphertext
   d) The ciphertext is not changed if the same key is used, but with different plaintext

6. 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.

7. The RSA algorithm can be used for:
   a) Data encryption and digital signatures
   b) Data encryption, but not digital signatures
   c) Digital signatures, but not data encryption
   d) Neither data encryption nor digital signatures

8. The security of RSA:
   a) Depends on the difficulty in multiplying two large prime numbers
   b) Depends on the difficulty in factoring large numbers into their primes
   c) Cannot be attacked using a brute force approach
   d) Cannot be attacked using timing attacks

9. The Diffie-Hellman exchange is a method for exchanging:
   a) Secret values between two users
   b) Certificates between two users
   c) Nonce values between two users
   d) Sequence numbers between two users
   e) Encrypted files between two users

10. The component that provides the most *confusion* (in the security meaning of confusion) in DES is:
   a) Initial Permutation
   b) S-Boxes
   c) Exclusive OR operations
   d) Mix columns
   e) Using the round sub-key

Part B – General Questions [120 marks]

Question 1 [6 marks]

List *and describe* two active attacks and two passive attacks on network security.

Question 2 [6 marks]

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

Question 3 [5 marks]

Encrypt the word “security” using the Playfair cipher with keyword “cryptography”.

Question 4 [8 marks]

The plaintext P is encrypted using a transposition cipher with a 5 digit key to produce the ciphertext, C = “OCXLN!DIMGUEOKA”. What is P and what is the key?

Question 5 [5 marks]

a) Explain what unconditionally secure means.
b) Why is the one-time pad unconditionally secure?
c) Why is the one-time pad not practical to use?

Question 6 [3 marks]

When performing end-to-end encryption in a network with many users, a Key Distribution Centre (KDC) should be used. Explain a reason why.

Question 7 [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:

a) Electronic Codebook
b) Cipher Block Chaining
c) Counter

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

Question 8 [10 marks]

Using the RSA algorithm, where the ciphertext C = 146 and public key PU = {e=7, n=187}, determine the plaintext P and private key PR.

(Hint: if you do not have a calculator, the following table gives some selected calculations which may be useful)

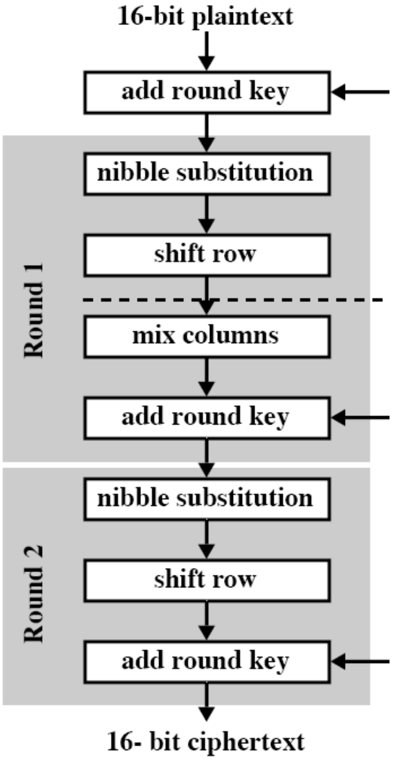
a	**b**	**c**	**a^b mod c**	**A**	**b**	**c**	**a^b mod c**
146	3	187	82	146	15	187	12
146	4	187	4	146	16	187	69
146	5	187	23	146	17	187	163
146	6	187	179	146	18	187	49
146	7	187	141	146	19	187	48
146	8	187	16	146	20	187	89
146	9	187	92	146	21	187	91
146	10	187	155	146	22	187	9
146	11	187	3	146	23	187	5
146	12	187	64	146	24	187	169
146	13	187	181	146	25	187	177
146	14	187	59	146	26	187	36

Question 9 [10 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:

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

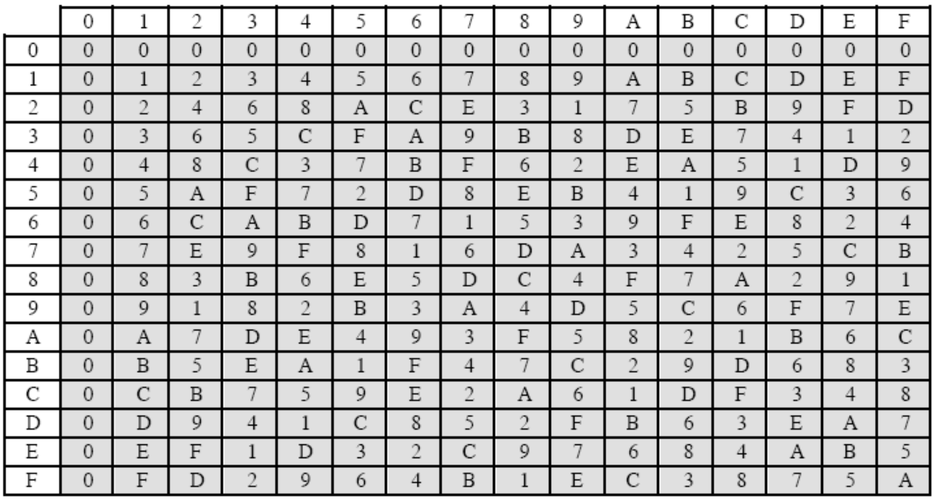
Mix columns:

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

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

Question 10 [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.

b) In the Affine Caesar Cipher:

   i. What values of *a* are allowed?

   ii. What values of *b* are allowed?

Question 11 [6 marks]

Assume Alice wants to send Bob a message over an un-secure network using public key cryptography.

a) If the necessary keys have already been created and exchanged, how does Alice use public key cryptography to ensure the message is kept private?

b) Once Alice and Bob have created a secure connection using public key cryptography, what may they do to overcome the computationally expensive encryption and decryption operations of the public key scheme?

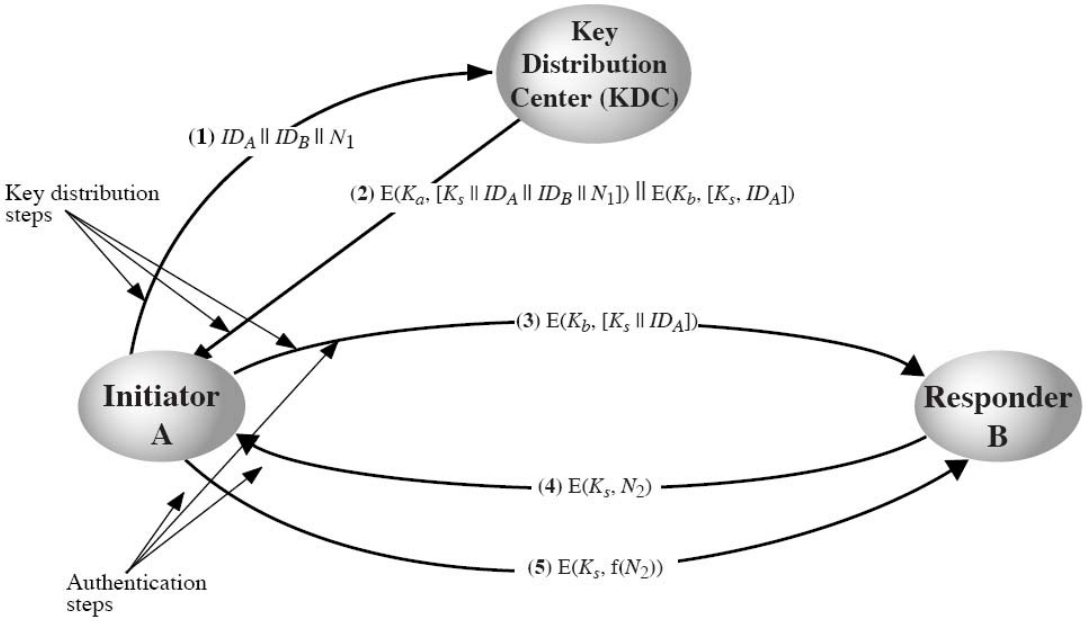
Question 12 [10 marks]

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.

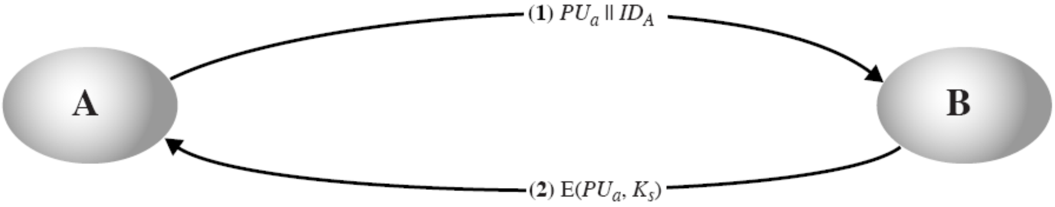
b) If A and B want to communicate at a later stage (for example, the next day), should they repeat this entire process? Give an advantage and disadvantage of doing so.

c) 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.


Key Distribution Center (KDC)
(1) $ID_A \| ID_B \| N_1$
Key distribution steps
(2) $E(K_a, [K_s \| ID_A \| ID_B \| N_1]) \| E(K_b, [K_s, ID_A])$
(3) $E(K_b, [K_s \| ID_A])$
Initiator A
Responder B
(4) $E(K_s, N_2)$
(5) $E(K_s, f(N_2))$
Authentication steps

Question 13 [10 marks]

The figure below shows a simple scheme for sharing a secret key between A and B. It assumes A and B have already exchanged public keys (e.g. using certificates). Explain how an attacker C can perform a man-in-the-middle attack to discover the secret key without A or B knowing. You may use a diagram, but you must also give a written explanation of the steps taken.



Question 14 [12 marks]

a) If A sends an unencrypted message M to B, and also sends the Message Authentication Code, what two security services does the system provide?

b) Explain what happens if an attacker C intercepts the message from A to B, modifies M (e.g. changes M to N) and then forwards the modified message, with the original MAC attached, to B.

c) What if C changes both the message M (to N), and calculates and sends the new MAC based on N?

Question 15 [10 marks]

Assume a digital signature is applied on the hash of a message (not the message itself), and A sends the message (M_A) and digital signature to B. If the hash function is not weak collision resistant, then explain how an attacker C can forge A’s digital signature on a new message from C (called M_C). Make sure you explain why B cannot detect this forgery.