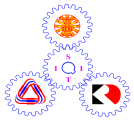
Name ….....ID …..... Section ….....Seat No.....



Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination: Semester 2/2008

Course Title : CSS322 Security and Cryptography

Instructor : Dr Steven Gordon

Date/Time : Thursday 8 January 2009, 9:00 to 12:00

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 [10 marks]

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), followed by applying a Playfair cipher with the key “minewas” (padding with the special character 'x' was necessary). Find P and K. Hints: P is in English, the first word is 4 letters in length, and the last letter (of P) is not a vowel.

C = qtiygktmbswecmvzcymeumecbv

Question 2 [16 marks]

The encryption algorithm of RSA is defined as:

$$C = M^e \bmod n$$

a) What is the decryption algorithm of RSA? [1 mark]

b) What is the public key in RSA? [1 mark]

c) What is the private key in RSA? [1 mark]

d) Describe the steps for generating the public/private key pair. You must state the conditions/properties of any values to be selected or calculated. (You do not need to explain why those conditions are necessary) [5 marks]

Based on the definition of RSA, there are three theoretical approaches for an attacker, knowing only public information, to discover the private information and/or a plaintext message.

e) What public information is it assumed that an attacker knows in RSA? (Refer to the variables defined in parts (a) to (d)). [1 mark]

f) Describe one of the three theoretical approaches that an attacker can use. [5 marks]

g) What makes the above approach practically impossible for an attacker to use? [2 marks]

Question 3 [14 marks]

Table 1 shows all possible plaintext/ciphertext block pairs when using a symmetric key encryption algorithm *E* using key *k*.

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

Table 1: Symmetric cipher

In the following questions, you must assume all initial values are 0. Consider the ciphertext message, C = 010001110111.

a) Decrypt *C* if Electronic Code Book (ECB) mode of operation was used in encryption.[3 marks]

b) Decrypt *C* if Cipher Block Chaining (CBC) mode of operation was used in encryption. [3 marks]

c) Decrypt *C* if Counter (CTR) mode of operation was used in encryption.[3 marks]

d) Explain an advantage of CBC (when compared to ECB).[2 marks]

e) Explain an advantage of CTR (when compared to CBC). [3 marks]

Question 4 [19 marks]

Figure 1 shows an example key distribution method for public key systems.

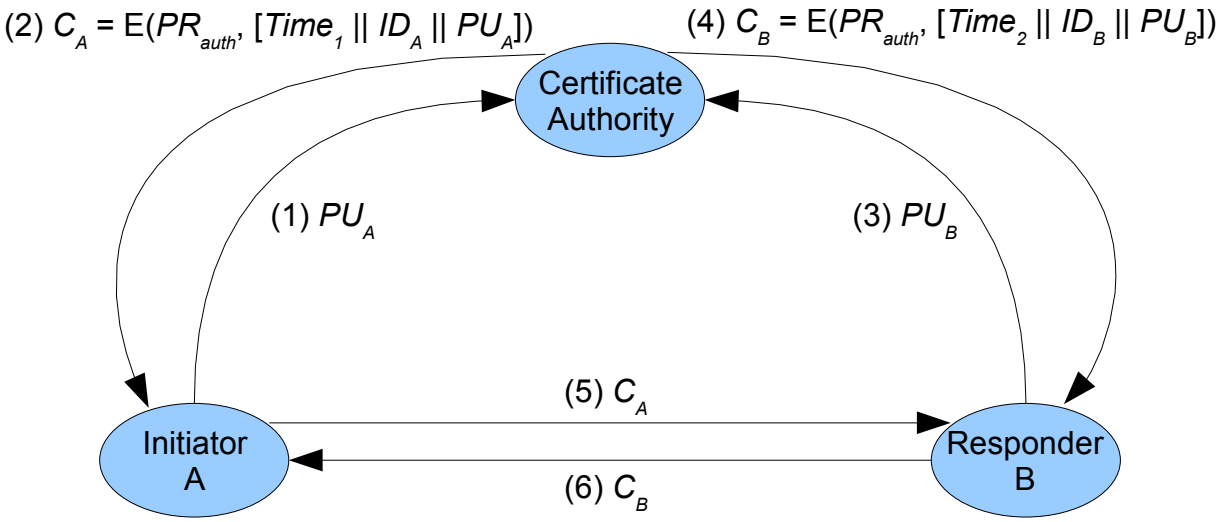


Figure 1: Certificate Authority Key Distribution Scheme

a) The procedure in Figure 1 assumes each node already has (or knows) some keys. List those keys for each node:

   i. Certificate Authority (Auth) [1 mark]

   ii. User A [1 mark]

   iii. User B [1 mark]

b) After the procedure is complete, list the keys that each node has/knows:

   i. Certificate Authority (Auth) [1 mark]

   ii. User A [1 mark]

   iii. User B [1 mark]

c) Explain the purpose of messages 1 and 2, including what is the purpose of a C_A. Also indicate whether these messages are transferred in a secure medium or not and why. [3 marks]

d) Must message 1 (and 2) be sent before message 3 (and 4)? Explain why or why not. [2 marks]

e) After all steps are complete, explain why B knows it has the public key that belongs to A (and not a forged public key). Also state any assumptions for this to be true. [2 marks]

Assume the key exchange is complete:

f) Explain what A does to send a confidential message to B, and why it is considered confidential. [2 marks]

g) Explain what B does to send a signed (but not confidential) message to A, and why the message is considered signed or authenticated. [2 marks]

h) Explain how the certificate authority key distribution scheme in Figure 1 offers an advantage over the public-key authority scheme shown in Figure 2. [2 marks]

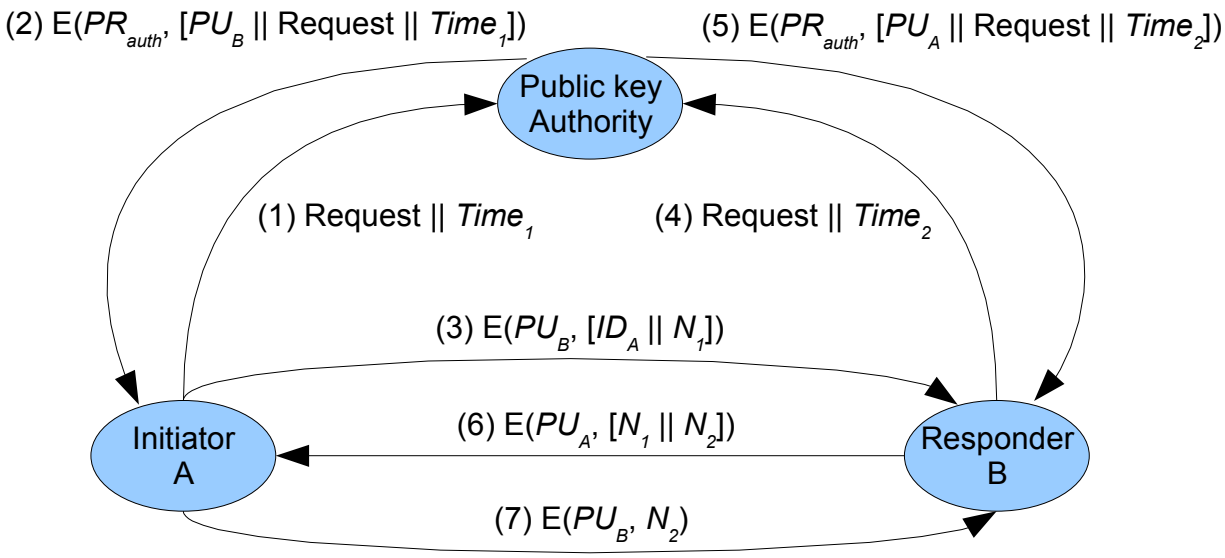


Figure 2: Public Key Authority scheme

Question 5 [10 marks]

a) If you wanted to compare two encryption algorithms, A and B, with respect to the avalanche effect, explain two methods in which they can be compared. [6 marks]

b) If you wanted to compare two encryption algorithms, A and B, with respect to the randomness of the output they produce, explain two simple tests that can be performed. [4 marks]

Question 6 [9 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). [5 marks]

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

Question 7 [10 marks]

Consider a general mono-alphabetic cipher operating on a language which has 36 characters. There is a total of 1,000,000 words within the dictionary of this language. Assume an attacker has access to a computer system that can decrypt (and test for valid word and/or phrases in the dictionary) at a rate of 10^9 decryptions per second.

a) If the attacker attempts a brute force attack in a ciphertext encrypted using this cipher, what is the maximum time the attack will take? [3 marks]

b) Explain what language analysis is, and explain how it can potentially make an attack on a mono-alphabetic cipher very easy (compared to an attack on a poly-alphabetic cipher). [4 marks]

c) If for the language used in the mono-alphabetic cipher, the average frequency of each of the 36 letters in most plaintexts is the same, then is language analysis still possible with the cipher? [3 marks]

Question 8 [12 marks]

a) List the names of three security services desired in computer networks. For each service, describe what the service means. [6 marks]

b) For each of the three services from part (a), list and describe an attack on that service. For each attack, also indicate if it is active or passive. [6 marks]