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

Sirindhorn International Institute of Technology
Thammasat University

Midterm Examination Answers: 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

Answer

Given C, we decrypt using the Playfair cipher:

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

qt → pr iy → ev gk → fh tm → ow bs → sa we → en cm → ae vz → uy
cy → er me → wn um → ou ec → ye bv → sx

Intermediate value is:

I = prevfhowsaenaeuyerwnouyes (x is removed from end)

Since there are 25 characters, and no padding was necessary, then the transposition cipher most likely has 5x5 rows/columns:

I = prevf howsa enaeu yerwn ouyes

or

p	h	e	y	o
r	o	n	e	u
e	w	a	r	y
v	s	e	w	e
f	a	u	n	s

Consider the first character of each block: pheyo. How can those letters be re-arranged to make a 4 letter word. Since the last letter of P is not a vowel, then of "fauns" the last character of the first row must end with 'p', 'y' or 'o'.

If it ends with 'p' we have 'heyo' remaining. The 4 letter words: ?

If it ends with 'y' we have 'pheo' remaining. The 4 letter words: 'hope', ?

If it ends with 'o' we have 'phey' remaining. The 4 letter words: ?

So if the first 5 characters are 'hopey' then K must be 25134 giving:

h	o	p	e	y

o	u	r	n	e
w	y	e	a	r
s	e	v	e	w
a	s	f	u	n

P = hope your new years eve was fun

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]

Answer

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

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

Answer

$$PU = \{e, n\}$$

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

Answer

$$PR = \{d, n\}$$

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]

Answer

Select two large prime integers, p and q.

Calculate $n = p * q$ and $\Phi(n) = (p-1)*(q-1)$.

Select e such that it is relatively prime with $\Phi(n)$ or $gcd(e, \Phi(n)) = 1$

Calculate d, the multiplicative inverse of e in mod $\Phi(n)$.

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]

Answer

Attacker knows: e, n, C

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

Answer

Approach 1. Determine p and q by factoring n into its prime factors, so that $\Phi(n)$ can be

easily calculated, and subsequently *d*.

Approach 2. Given *C*, *e* and *n*, calculate the inverse of $C = M^e \bmod n$. That is, find an *M* such that: $e = discretelog_{M,n}(C)$.

Approach 3. From *n*, calculate $\Phi(n)$ without knowing *p* and *q*.

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

Answer

Approach 1. Determining the prime factors of a large number is computationally hard.

Approach 2. Calculating the discrete logarithm (inverse exponential) for large numbers is computationally hard.

Approach 3. Calculating $\Phi(n)$ for large *n* is computationally hard.

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]

Answer

There are 3 blocks of input ciphertext: 0100 0111 0111

With ECB each block is decrypted to obtain the plaintext.

P = 1011 0010 0010

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

Answer

With CBC, the ciphertext block is decrypted and then XOR with the previous block (or IV).

C1: 0100 C2: 0111 C3: 0111

O1: 1011 O2: 0010 O3: 0010

IV: 0000 CP: 0100 CP: 0111

P1: 1011 P2: 0110 P3: 0101

P = 1011 0110 0101

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

Answer

With CTR, a counter is encrypted with the output XOR with the ciphertext.

T1: 0000 T2: 0001 T3: 0010

O1: 1100 O2: 1111 O3: 0111

C1: 0100 C2: 0111 C3: 0111

P1: 1000 P2: 1000 P3: 0000

P = 1000 1000 0000

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

Answer

ECB produces the same output ciphertext block if the input plaintext block is the same. Whereas, CBC can produce a different output ciphertext block, even if two input blocks are the same. This makes CBC harder to perform language analysis against.

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

Answer

Each block operation in CTR only depends on the plaintext and counter, not on the previous block. In CBC, each block depends on the previous block. CTR can implement the encryption of blocks in parallel, making it potentially faster than CBC.

Question 4 [19 marks]

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

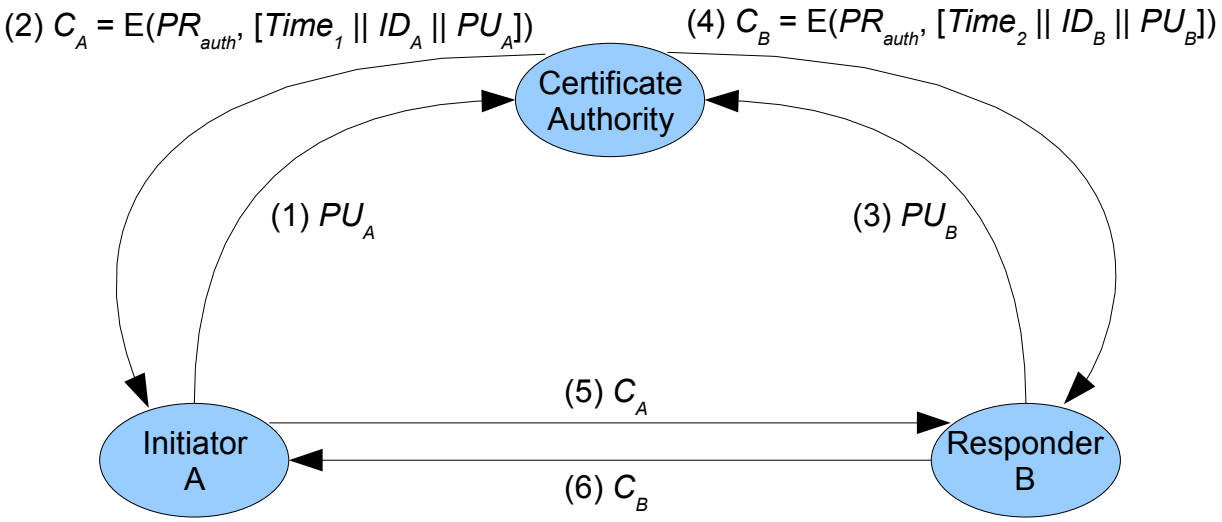

Figure 1: Certificate Authority Key Distribution Scheme

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]

Answer

PR_{auth}, PU_{auth}

ii. User A [1 mark]

Answer

PR_A, PU_A, PU_{auth}

iii. User B [1 mark]

Answer

PR_B, PU_B, PU_{auth}

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

i. Certificate Authority (Auth) [1 mark]

Answer

PR_{auth},PU_{auth}, PU_A, PU_B

ii. User A [1 mark]

Answer

PR_A, PU_A, PU_{auth}, PU_B

iii. User B [1 mark]

Answer

PR_B, PU_B, PU_{auth}, PU_A

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]

Answer

These messages are for A to obtain a certificate (C_A). A informs the CA of its public key, and the CA issues a certificate including that public key, the identity of A, all signed with the CA's private key (PR_{auth}). These steps must be performed in a secure medium, for example A physically visiting CA, because the CA must be certain that PU_A actually belongs to A.

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

Answer

No. A and B may obtain their certificate from the CA at any time, so long as they are obtained before A initiates communications with B.

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]

Answer

The certificate C_A received by B is signed with CA's private key. As B has CA's public key (and we assume B trusts/knows it is in fact CA's public key), then B can validate that the public key included in the certificate belongs to A.

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]

Answer

A encrypts the message using the public key of B and sends the cipher text to B. Only B has the corresponding private key, and so only B can decrypt the message.

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]

Answer

B encrypts the message using the private key of B. When A receives it, A can decrypt with B's public key, therefore being certain that it came from B (because only B has the corresponding private key).

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]

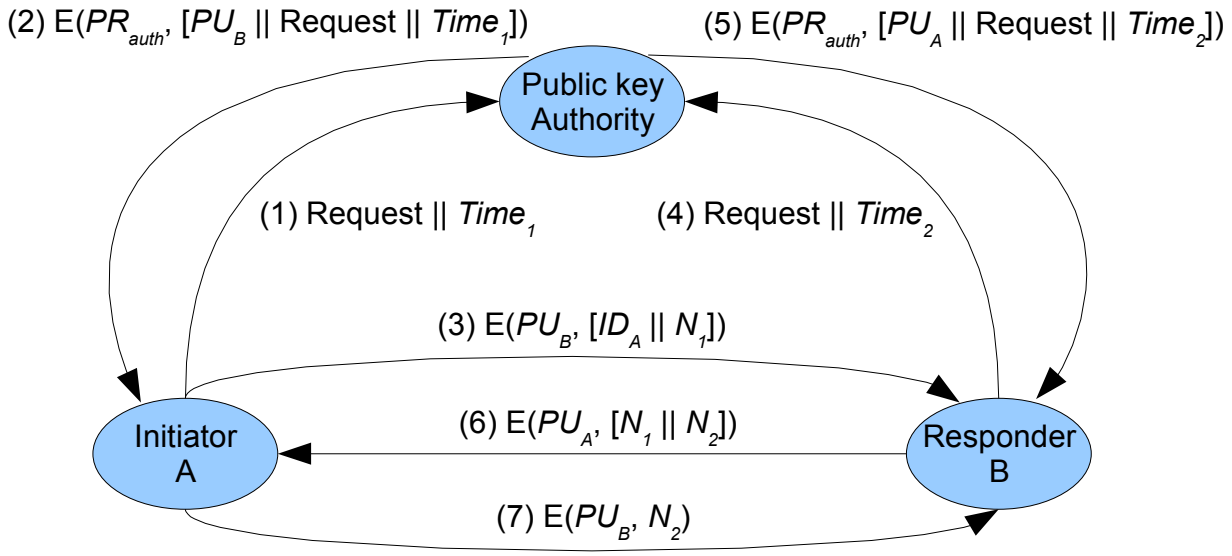

Figure 2: Public Key Authority scheme

Answer

With the public-key authority, every time A wants to exchange keys with a new user, both A and the new user must make a request to the authority. This can create a performance bottleneck at the authority. Whereas with a certificate authority, a certificate is obtain once by each user. When A wants to exchange keys with a new user, A simply sends the certificate to the user.

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]

Answer

Method 1. Take a plaintext P and key K and encrypt P using both A and B to obtain Ca1 and Cb2. Now change P by a single bit (using the same K), encrypt to obtain Ca2 and Cb2. Compare the number of bits different in Ca1-Ca2 and Cb1-Cb2. Repeat this process for many different plaintexts and then compare the average number of bits in ciphertext between both algorithms.

Method 2. Same as Method 1 except instead of changing a bit in the plaintext, change a bit in the key.

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]

Answer

Perform multiple encryptions (using different keys and plaintexts) and:

Test 1. Count the number of 1's and 0's in the output. Should be equal number.

Test 2. Select an M-bit block of the output and perform Test 1.

Test 3. Count the length of sequences of 1's (and similar for 0's) – the lengths should be small.

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]

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 $\oplus$ Ka

A sends Mab to B

At B: Mba = Mab $\oplus$ Kb

B sends Mba to A

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

The property of $\oplus$ is: if A $\oplus$ B = C then A = B $\oplus$ C

So if Ka = Kb, then Mab = R $\oplus$ Ka and Mba = Mab $\oplus$ Ka = R $\oplus$ Ka $\oplus$ Ka = R $\oplus$ 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 $\oplus$ Ka and Mba = Mab $\oplus$ Ka = R

Mab $\oplus$ Mba = R $\oplus$ Ka $\oplus$ R = Ka

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]

Answer

With 36 characters, there is 36! possible combinations of a mono-alphabetic cipher. The maximum time an attacker will take is if they attempt all 36! combinations:

$36!/10^9$ seconds

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]

Answer

Language analysis involves using statistics of the most common letters, pairs of letters etc. in pieces of text in a particular language, to determine the most likely mapping from input characters to output characters in an alphabetic cipher. With a mono-alphabetic cipher one plaintext letter always maps to the same ciphertext letter. Therefore by counting the number of occurrences of a letter in the ciphertext, the attacker can match it to the plaintext letter with the same expected number of occurrences.

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]

Answer

Yes. Even though single characters have the same frequency, pairs or triple of characters may have different frequency distributions. Therefore language analysis can take advantage of the expected frequency of a pair of characters.

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]

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) 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]

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).