UNIVERSITI SAINS MALAYSIA

First Semester Examination
2011/2012 Academic Session

January 2012

CCS523 – Computer Security and Cryptography

[Keselamatan Komputer dan Kriptografi]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

- Please ensure that this examination paper contains **THREE** questions in **NINE** printed pages before you start the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **TIGA** soalan di dalam **SEMBILAN** muka surat yang bercetak sebelum anda memulakan peperiksaan ini.]*

- Answer all **THREE (3)** questions.

  *[Jawab kesemua **TIGA (3)** soalan.]*

- You may answer the questions either in English or in bahasa Malaysia.

  [Anda dibenarkan menjawab soalan sama ada dalam bahasa Inggeris atau bahasa Malaysia.]

- You may bring in and use a scientific and programmable calculator.

  [Anda dibenarkan membawa dan mengguna kalkulator saintifik dan kalkulator boleh-program.]

- In the event of any discrepancies, the English version shall be used.

  [Sekiranya terdapat sebarang percanggahan pada soalan peperiksaan, versi bahasa Inggeris hendaklah diguna pakai.]

1. (a) Given a plaintext block P and a ciphertext block C, a block cipher X is defined as $C = X_k(P)$, with the following specification:

- Block size, $|P| = |C| = m$ bits.
- Key size, $|k| = n$ bits.

(i) How many possible transformations are there from a plaintext block to a ciphertext block?

(10/100)

(ii) How many possible transformations are there from a plaintext block to a ciphertext block if the transformation was governed by a key k?

(10/100)

(iii) Assume a cipher block, DX, defined as $C = DX(P) = X_{k2}(X_{k1}(P))$, is created by cascading two blocks of cipher X with two different keys, *k1* and *k2*. What is the effective key size for block cipher DX considering meet-in-the-middle attack?

(20/100)

(iv) How many pair(s) of plaintext-ciphertext block are needed for meet-in-the-middle attack discussed in 1(a)(iii), so that false keys can be rule out with a reasonable likelihood? Justify your answer.

(20/100)

(b) The following questions are related to hash function. Where appropriate, please sketch your propose solutions.

(i) Device a hypothetical block cipher based on MD5 hash function. (Hint: Consider Feistel structure).

(20/100)

(ii) The structure of Merkel-Damgard hash construction is inherently sequential. Propose a modified version of the Merkel-Damgard hash construction that can take advantage of the parallel processing.

(20/100)

2. (a) Below is the encryption code for RC6-128.

```
B = B + S[ 0 ]
D = D + S[ 1 ]
for  i  =  1  to  20  do
    {
        t  =  ( B  x  ( 2B  + 1 ) )  <<<  5
        u  =  ( D  x  ( 2D + 1 ) )  <<<  5
        A  =  ( ( A ⊕ t )  <<<  u )  +  S[ 2i ]
        C  =  ( ( C  ⊕ u )  <<<  t )  +  S[ 2i + 1 ]
        (A, B, C, D)  =  (B, C, D, A)
     }
```

(i) Draw a block diagram of the encryption scheme.

(20/100)

(ii) Write the corresponding decryption code for RC6-128.

(20/100)

(b) Below is a list of modes of operation for DES:

- Triple DES in the CFB mode with $k = 32$.
- Double DES with two keys k_1, k_2.
- DES in the OFB mode with $k = 8$.
- DES in the ECB mode.

(i) Arrange the transformations according to their speed in software (start from the fastest transformation).

(10/100)

(ii) Arrange the transformations according to their security (start from the least secure).

(10/100)

(c) In one faculty, it is known that a lecturer will resign. In that faculty there are three cryptographers, who are curious to know if one of them is the one who will leave the faculty. This group of three cryptographers agreed that even if one of them will leave the faculty, the identity of the person should not be revealed, however the group should know that one of them is leaving. Therefore, they agreed to run the following protocol:

a. They agreed on a set of RSA parameters {n, $\phi(n)$, p, q and M}.
b. Each of the three cryptographers, c_i where $i \in \{0,1,2\}$, choose a random number r_i such that $r_i < \phi(n)$ and $gcd(r_i, \phi(n)) = 1$.
c. Cryptographer c_i submits his/her random number to cryptographer $c_{(i+1) \bmod 3}$.
d. Each cryptographer c_i will calculate $s_i = M^{d_i \times r_{(i-1) \bmod 3}} \bmod n$, where $r_i \times d_i \equiv 1 \bmod \phi(n)$.
e. If there is a cryptographer c_i who will be leaving the faculty, then he/she will further calculate $s_i = (s_i + 1) \bmod n$.
f. Cryptographer c_i then publish his/her s_i.
g. With all the s_i's, all the three cryptographer will execute the following code to determine if any one of them is leaving.

```
If (M == f(s0, s1, s2)) then
   None of the three is leaving
Else
   One of the three is leaving
```

(i) Write the function $f(s_0, s_1, s_2)$.

(20/100)

(ii) What happen if in step (a), $M > n$? Why?

(20/100)

3. (a) Consider the RSA algorithm:

(i) Finding the multiplicative inverse is one of the steps in RSA key generation. Even though it is not cost effective, multiplicative inverse can be calculated from Euler Theorem ($a^{\phi(n)} \equiv 1 \bmod n$). Based on Euler Theorem, find a multiplicative inverse of 2 in Z_{21}. Show your work.

(20/100)

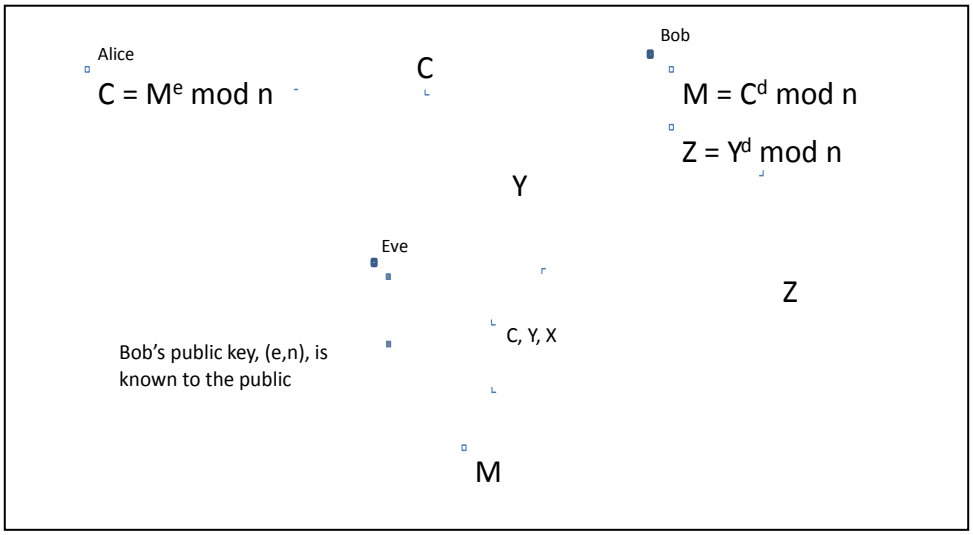
(ii) What is the problem in choosing 2 as the public key e?

(10/100)

(iii) Suppose Bob leaks his RSA private key. Rather than generating a new modulus, he decides to generate a new public and a new private key based on the old modulus. Why this is not a good practice?

(20/100)

(iv) It is possible to mount a chosen ciphertext attack on RSA. Derive the steps of the chosen ciphertext attack as depicted by the black boxes in the following figure.



(20/100)

(b) Answer the following short questions.

(i) Why MIME protocol does not used SSL to establish secure communication?

(10/100)

(ii) List **two** (2) advantages of SSL compared to IPSec.

(20/100)

1. (a) Diberi blok teks-nyata P dan blok teks-sulit C, satu blok sifer X didefinisikan sebagai $C = X_k(P)$, dengan spefikasi seperti berikut:

- Saiz block, $|P| = |C| = m$ bit.
- Saiz kunci, $|k| = n$ bit.

(i) Ada berapa banyak transformasi dari blok teks-nyata kepada blok teks-sulit?

(10/100)

(ii) Ada berapa banyak transformasi dari blok teks-nyata kepada blok teks-sulit jika transformasi tersebut tertakluk kepada kunci k?

(10/100)

(iii) Andaikan blok sifer, DX, didefinisikan sebagai $C = DX(P) = X_{k2}(X_{k1}(P))$, telah direka dengan menggabungkan dua blok sifer X dengan menggunakan dua kunci yang berlainan, *k1* dan *k2*. Apakah saiz kunci efektif bagi blok sifer DX setelah mengambil kira serangan *meet-in-the-middle*?

(20/100)

(iv) Berapa pasang teks-nyata-teks-sulit yang diperlukan untuk serangan *meet-in-the-middle* seperti yang dibincangkan pada 1(a)(iii), supaya kunci palsu dapat diasingkan dengan kebarangkalian yang munasabah. Jelaskan jawapan anda.

(20/100)

(b) Soalan-soalan di bawah adalah berkenaan dengan fungsi cincang. Di mana perlu, tolong lakarkan cadangan selesaian.

(i) Cadangkan satu lakaran blok sifer berdasarkan fungsi cincang MD5. (Petua: Pertimbangkan struktur Feistel).

(20/100)

(ii) Struktur pembinaan fungsi cincang Merkel-Damgard secara sedia ada adalah berjujukkan. Cadangkan versi pembinaan fungsi cincang Merkel-Damgard yang diubah-suai supaya dapat mengambil faedah dari pemprosesan selari.

(20/100)

2. (a) Di bawah adalah kod enkripsi untuk RC6-128.

```
B = B + S[ 0 ]
D = D + S[ 1 ]
for  i  =  1  to  20  do
    {
        t  =  ( B  x  ( 2B  + 1 ) )  <<<  5
        u  =  ( D  x  ( 2D + 1 ) )  <<<  5
        A  =  ( ( A ⊕ t )  <<<  u )  +  S[ 2i ]
        C  =  ( ( C  ⊕ u )  <<<  t )  +  S[ 2i + 1 ]
        (A, B, C, D)  =  (B, C, D, A)
     }
```

(i) Lukis gambar-rajah blok untuk skema enkripsi tersebut.

(20/100)

(ii) Tulis kod dekripsi yang bersepadanan untuk RC6-128.

(20/100)

(b) Di bawah adalah senarai mod of operation untuk DES:

- Triple DES dalam mod CFB dengan k=32.
- Double DES dengan dua kunci k_1, k_2.
- DES dalam mod OFB dengan k=8.
- DES dalam mod ECB.

(i) Aturkan transformasi di atas mengikuti kelajuan mereka jika diimplementasi pada softwer (mulakan dengan yang terpantas).

(10/100)

(ii) Aturkan transformasi di atas mengikuti tahap keselamatan (mulakan dengan yang paling selamat).

(10/100)

(c) Dalam satu fakulti, telah diketahui bahawa ada seorang pensyarah akan meletakkan jawatan. Dalam fakulti tersebut terdapat tiga orang *cryptographer*, yang ingin tahu tahu jika seorang daripada mereka adalah pensyarah yang akan meninggalkan fakulti. Kumpulan tiga *cryptographer* itu bersetuju jika seorang daripada mereka akan meninggalkan fakulti, identiti orang tersebut tidak patut didedahkan, bagaimanapun kumpulan itu perlu tahu jika seorang daripada mereka akan meninggalkan kumpulan itu. Lantarannya, mereka bersetuju untuk menjalankan protokol berikut:

a. Mereka bersetuju menggunakan satu set parameter RSA {n, $\phi(n)$, p, q and M}.
b. Setiap seorang *cryptographer*, c_i di mana $i \in \{0,1,2\}$, memilih satu nombor rawak r_i di mana $r_i < \phi(n)$ dan $gcd(r_i, \phi(n)) = 1$.
c. Cryptographer c_i mengemukakan nombor rawak beliau kepada cryptographer $c_{(i+1) \bmod 3}$.
d. Setiap cryptographer c_i akan mengira $s_i = M^{d_i \times r_{(i-1) \bmod 3}} \bmod n$, di mana $r_i \times d_i \equiv 1 \bmod \phi(n)$.
e. Jika terdapat cryptographer c_i yang akan meninggalkan fakulti, beliau seterusnya akan mengira $s_i = (s_i + 1) \bmod n$.
f. Cryptograher c_i seterusnya mengemukakan nilai s_i.
g. Dengan semua nilai s_i, kesemua cryptographer akan melaksanakan kod berikut untuk mengetahui jika salah seorang daripada mereka akan meninggalkan fakulti.

```
If (M == f(s0, s1, s2)) then
   None of the three is leaving
Else
   One of the three is leaving
```

(i) Tuliskan fungsi $f(s_0, s_1, s_2)$.

(20/100)

(ii) Apa akan terjadi jika pada langkah (a), $M > n$? Kenapa?

(20/100)

3. (a) Pertimbangkan algoritma RSA:

(i) Mencari songsangan pendaraban adalah salah satu dari langkah dalam penjanaan kunci RSA. Walaupun ia kurang berkesan dari segi kos, songsangan pendaraban boleh dihitung dengan menggunakan Teorem Euler ($a^{\phi(n)} \equiv 1 \bmod n$). Berdasarkan kepada Teorem Euler, cari songsangan pendarapan untuk 2 di dalam Z_{21}. Tunjukkan jalan kerja anda.

(20/100)

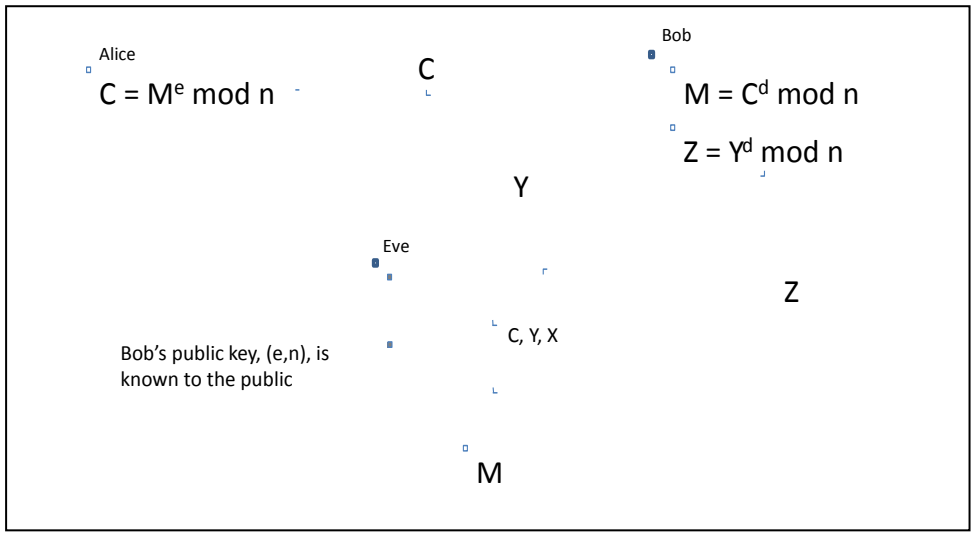
(ii) Apakan masalahnya apabila memilih nilai 2 sebagai nilai kunci umum *e*?

(10/100)

(iii) Andaikan kunci persendirian RSA Bob telah bocor. Daripada menjana satu modulus baru, dia memutuskan untuk menjana satu kunci umum baru dan satu kunci persendirian baru berdasarkan kepada modulus yang lama. Mengapa ini bukan satu amalan yang baik

(20/100)

(iv) Ia adalah satu kemungkinan untuk menyerang RSA dengan cara serangan pilihan teks-sulit. Hasilkan langkah-langkah serangan pilihan teks-sulit tersebut sebagaimana yang digambarkan oleh kotak-kotak hitam pada gambar rajah berikut:



(20/100)

(b) Jawab soalan-soalan pendek berikut.

(i) Kenapa protocol MIME tidak menggunakan SSL untuk mengwujudkan situasi komunikasi selamat?

(10/100)

(ii) Senaraikan dua kelebihan SSL jika dibandingkan dengan IPSec.

(20/100)