UNIVERSITI SAINS MALAYSIA

First Semester Examination
[Peperiksaan Semester Pertama]

Academic Session 2008/2009
[Sidang Akademik 2008/09]

November 2008

CCS523 – Computer Security and Cryptography
[Keselamatan Komputer & Kriptografi]

Duration : 2 hours
[Masa : 2 jam]

INSTRUCTIONS TO CANDIDATE:
[ARAHAN KEPADA CALON:]

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

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **TIGA** soalan di dalam **LAPAN** 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.]

---

1. (a) Questions regarding AES algorithm.

(i) Following is the AES encryption pseudocode. Write the corresponding AES decryption pseudocode.

```
Function AESCipher (InBlock[0 … 16], OutBlock[0 … 16], W[0 … 43])
{
        BlockToState (Inblock, S)

        S ← AddRoundKey (S, W[0 … 3])
        for (r = 1 to 10)                    // r defines the round
        {
                S ← SubBytes (S)
                S ← ShiftRows (S)
                if (r ≠ 10)
                        S ← MixColumns (S)
                S ← AddRoundKey (S, W[(r × 4) … ((r × 4) + 3)])
        }

        StateToBlock (S, OutBlock)
        return (OutBlock)

}
```

(10/100)

(ii) In AES-128, the round key used in the pre-round operation is the same as the cipher key. Is this the case for AES-192? Explain.

(10/100)

(b) In a Feistel round, the round function is the most expensive computational element and only half of the input is scrambled. Propose **two (2)** different methods that can scramble both half's of the input while still utilizing one round function.

(20/100)

(c) A student proposes a key-dependent expansion-permutation in order to enhance the DES round function. Give **two (2)** reasons why this might not be a good idea.

(20/100)

(d) Questions regarding CBC mode of operation.

(i) If bits 7 and 8 in ciphertext block 9 are corrupted during transmission, find the possible corrupted bits in the plaintext.

(10/100)

(ii) Device a method to include a checksum in every CBC blocks. Draw the corresponding modified CBC encryption and decryption diagram.

(10/100)

(iii) In mode of operation, padding must be added to the last block if the last block is less than n bits long (where n is the size of a block). Ciphertext stealing is a technique that can be applied to mode of operation which does not require padding. Given is a process of ECB encryption with ciphertext stealing being implemented. In this technique, the last two blocks P_{N-1} (n bits long) and P_N (m bits long, where $m \leq n$) are encrypted differently, as shown. The $\boldsymbol{head}_{m}(X)$ function selects the leftmost m bits while the $\boldsymbol{tail}_{n-m}(X)$ function selects the rightmost n-m bits.

$X = EK(PN-1) \rightarrow CN = \boldsymbol{head}m(X)$
$Y = PN \mid \boldsymbol{tail}n-m(X) \rightarrow CN-1 = EK(Y)$

Draw (only the last two blocks) the corresponding CBC encryption and decryption with ciphertext stealing technique in place.

(20/100)

2. (a) Consider the RSA algorithm.

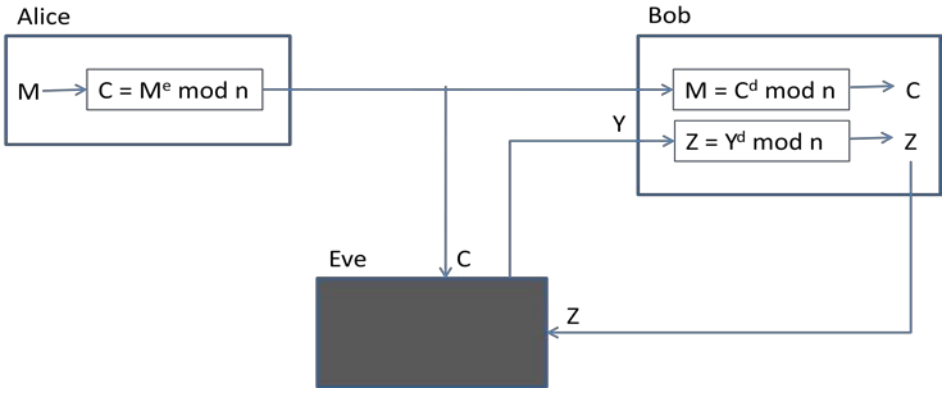
(i) Among other calculations, finding a multiplicative inverse of a number is one of the important steps in RSA key generation procedure. Derive a method based on Euler Theorem ($a^{\phi(n)} \equiv 1 \bmod n$) that can find multiplicative inverse for some numbers without the use of the Euclidean Extended Algorithm.

(20/100)

(ii) Similar to 2(a)(i), derive a method based on Fermat Little Theorem ($a^{p-1} \equiv 1 \bmod p$) that can find multiplicative inverse for some numbers without the use of the Euclidean Extended Algorithm.

(10/100)

(iii) It is possible to mount a chosen ciphertext attack on RSA. Based on the following figure, derive the steps of the chosen ciphertext attack as depicted by a black box in the figure.



(20/100)

(iv) A cryptography lecturer has three teaching assistants. They communicate securely using RSA algorithm. They also agree to use a **same small** value, *e*, as one of their encryption parameters to aid in the encryption process. In one occasion, the lecturer sends a set of question papers (message *M*) to the assistants for validity checking. Show that a student can mount an attack to recover the question papers, assuming the student has an access to the corresponding ciphertexts ($C_1 = M^e \bmod n_1$, $C_2 = M^e \bmod n_2$, $C_3 = M^e \bmod n_3$) while the ciphertexts were sent through the open network. [Hint: Consider using Chinese Remainder Theorem in this attack.]

(20/100)

(b) Questions regarding El-Gamal public-key algorithm.

(i) Alice sends to Bob the ciphertext as tuple (C_1, C_2). What happens if the value C_1 and C_2 are swapped during transmission?

(10/100)

(ii) By using El-Gamal algorithm, Alice sends a short message to Bob using a specific word processor which has a fix header such as "*%PDF-1.5%µµµµ1 0 obj<</Type/Catalog/Pages 2 0 R/Lang(en-US)…*" when view as text. It turns out that Alice's short message document was divided into two blocks, *Ma* and *Mb*, where *Ma* contains the information about the fix header while *Mb* is the actual message. Eve intercepts the corresponding ciphertext blocks (Ca_1, Ca_2) and (Cb_1, Cb_2). Show how Eve can use a known-plaintext attack to find the value of *Mb*.

(20/100)

3. (a) In Diffie-Hellman protocol, what happens if both Alice and Bob have accidentally chosen the same value for their private keys?

(20/100)

(b) Explain why asymmetric key system cannot be used in creating a MAC?

(20/100)

(c) Consider SHA-512 hash function.

(i) Compare the compression function of SHA-512 (without the final adding) with 80 rounds Feistel cipher. Show the similarities and differences.

(20/100)

(ii) Show that SHA-512 is subjected to meet-in-the middle attack if the final adding operation is removed from the compression function.

(20/100)

(d) Explain why NIST specification insists that if the value of $S_2 = 0$ in DSS, the two signatures must be recalculated using a new *r*?

(20/100)

1. (a) Soalan-soalan mengenai algoritma AES.

(i) Berikut adalah pseudokod enkripsi AES. Tulis pseudokod dekripsi AES yang sepadan.

```
Function AESCipher (InBlock[0 … 16], OutBlock[0 … 16], W[0 … 43])
{
        BlockToState (Inblock, S)

        S ← AddRoundKey (S, W[0 … 3])
        for (r = 1 to 10)                    // r defines the round
        {
                S ← SubBytes (S)
                S ← ShiftRows (S)
                if (r ≠ 10)
                        S ← MixColumns (S)
                S ← AddRoundKey (S, W[(r × 4) … ((r × 4) + 3)])
        }

        StateToBlock (S, OutBlock)
        return (OutBlock)

}
```

(10/100)

(ii) Untuk AES-128, kekunci pusingan yang digunakan untuk pusingan permulaan adalah sama dengan kekunci sifer. Adakah kes yang sama berlaku untuk AES-192? Terangkan.

(10/100)

(b) Dalam satu pusingan Feistel, fungsi pusingan mempunyai kos pengiraan tertinggi dan hanya separuh dari input disulitkan. Cadangkan **dua (2)** cara yang berbeza yang dapat menyulitkan kedua-dua bahagian daripada input dan masih menggunakan satu fungsi pusingan sahaja.

(20/100)

(c) Seorang pelajar memperkenalkan *expansion-permutation* yang bergantung kepada nilai kekunci untuk menambahbaikkan fungsi pusingan DES. Beri **dua (2)** alasan mengapa cara ini mungkin bukan satu cadangan yang baik.

(20/100)

(d) Soalan-soalan mengenai mod operasi CBC.

(i) Jika bit ke 7 dan 8 dari blok ke 9 korup semasa transmisi, cari bit yang mungkin korup pada teks-nyata.

(10/100)

(ii) Bangunkan satu cara untuk menggunakan *checksum* pada setiap blok CBC. Lukis gambar rajah enkripsi dan dekripsi CBC yang telah diubah.

(10/100)

(iii) Dalam mod operasi, proses pemenuhan bit perlu dilakukan ke atas blok terakhir jika blok terakhir bersais kurang dari *n* bit panjang (di mana *n* adalah size blok). *Ciphertext stealing* adalah teknik tanpa perlu proses pemenuhan bit yang boleh dilaksanakan ke atas mod operasi. Diberi adalah proses enkripsi ECB dengan penggunaan teknik *ciphertext stealing*. Dalam teknik ini, dua blok terakhir P_{N-1} (dengan saiz blok *n* bit) dan P_N (dengan saiz blok *m* bit, di mana $m \leq n$) dienkripkan dengan cara berlainan daripada biasa, seperti yang ditunjukkan. Fungsi $\boldsymbol{head}_m(X)$ mengambil *m* bit terkiri manakala fungsi $\boldsymbol{tail}_{n-m}(X)$ mengambil *n-m* bit terkanan.

$X = EK(PN-1) \rightarrow CN = \boldsymbol{head}m(X)$
$Y = PN \mid \boldsymbol{tail}n-m(X) \rightarrow CN-1 = EK(Y)$

Lukis (hanya dua blok terakhir) gambar rajah enkripsi dan dekripsi CBC yang menggunakan teknik *ciphertext stealing*.

(20/100)

2. (a) Anggapkan algoritma RSA.

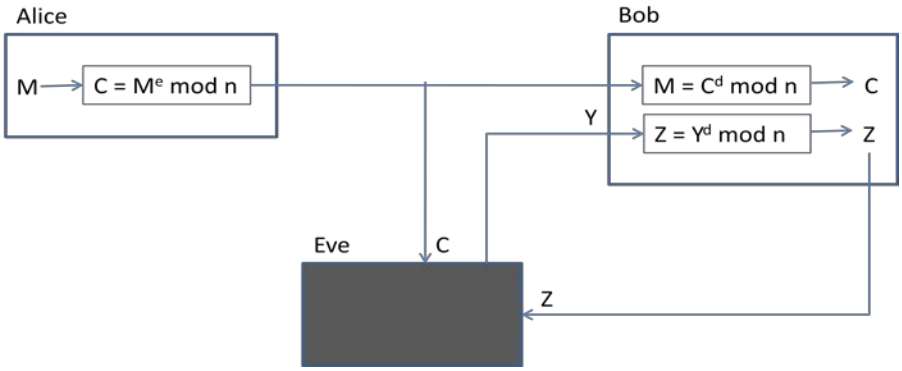
(i) Di antara banyak pengiraan, mencari pembalikan darab sesuatu nombor adalah salah satu langkah penting dalam proses penjanaan kunci-kunci RSA. Hasilkan satu cara berasaskan theorem *Euler* ($a^{\phi(n)} \equiv 1 \bmod n$) yang dapat mencari pembalikan darab untuk sebahagian nombor tanpa menggunakan algoritma *Extended Euclidean*.

(20/100)

(ii) Seperti bahagian 2(a)(i), hasilkan satu cara berasaskan teorem kecil *Fermat* ($a^{p-1} \equiv 1 \bmod p$) yang dapat mencari pembalikan darab untuk sebahagian nombor tanpa menggunakan algoritma *Extended Euclidean*.

(10/100)

(iii) Ia adalah satu kemungkinan untuk menyerang RSA dengan cara serangan *chosen ciphertext*. Berdasarkan kepada gambar rajah berikut, hasilkan langkah-langkah serangan *chosen ciphertext* tersebut sebagaimana yang digambarkan oleh kotak hitam pada gambar rajah.



(20/100)

(iv) Seorang pensyarah kriptografi mempunyai tiga orang penolong pengajar. Mereka berkomunikasi secara rahsia dengan menggunakan algoritma RSA. Mereka juga bersetuju untuk menggunakan nilai **kecil** yang **sama**, *e*, sebagai salah satu parameter enkripsi dengan tujuan untuk membantu proses enkripsi. Dalam satu kejadian, pensyarah tersebut menghantar satu set kertas soalan (maklumat *M*) kepada penolong-penolong pengajar beliau untuk membuat pengesahan. Tunjukkan bahawa seseorang pelajar boleh melakukan serangan untuk mendapatkan soalan-soalan tersebut, dengan anggapan bahawa pelajar tersebut memperolehi teks-teks nyata yang berkenaan ($C_1 = M^e \bmod n_1$, $C_2 = M^e \bmod n_2$, $C_3 = M^e \bmod n_3$) ketika teks-teks tersebut dihantar melalui rangkaian terbuka. [Petua: Pertimbangkan penggunaan teorem *Chinese Remainder* untuk serangan ini.]

(20/100)

(b) Soalan-soalan mengenai algoritma kekunci-awam El-Gamal.

(i) Alice menghantar kepada Bob teks-sulit dalam bentuk tuple (C_1, C_2). Apakah yang akan terjadi jika nilai C_1 dan C_2 tertukar semasa transmisi?

(10/100)

(ii) Dengan menggunakan algoritma El-Gamal, Alice menghantar maklumat pendek kepada Bob melalui penggunaan aplikasi *word processor* tertentu yang mempunyai kepala dokumen tetap seperti "*%PDF-1.5%μμμ1 0 obj<</Type/Catalog/Pages 2 0 R/Lang(en-US)…*" bila dilihat sebagai teks. Maklumat pendek Alice terbahagi kepada dua blok, *Ma* dan *Mb*, di mana *Ma* mengandungi maklumat tetap kepala dokumen manakala *Mb* adalah maklumat sebenar kepunyaan Alice. Eve memintas blok teks-sulit (Ca_1, Ca_2) dan (Cb_1, Cb_2). Tunjukkan bagaimana Eve boleh menggunakan serangan *known-plaintext* untuk mendapatkan nilai *Mb*.

(20/100)

3. (a) Untuk protokol Diffie-Hellman, apa akan terjadi jika kedua-dua Alice dan Bob secara tidak sengaja memiliki nilai kunci persendirian yang sama?

(20/100)

(b) Jelaskan mengapa sistem kekunci asimetri tidak boleh digunakan untuk menjanakan MAC?

(20/100)

(c) Pertimbangkan fungsi hash SHA-512.

(i) Bandingkan fungsi pemampatan SHA-512 (tanpa proses penambahan akhir) dengan sifer Feistel 80 pusingan. Tunjukkan persamaan dan kelainan mereka.

(20/100)

(ii) Tunjukkan SHA-512 boleh diserang secara *meet-in-the middle* jika proses penambahan akhir dikeluarkan dari fungsi pemampatan tersebut.

(20/100)

(d) Jelaskan mengapa spesifikasi NIST mendesak jika nilai $S_2 = 0$ untuk DSS, kedua-dua tanda-tangan perlu dikira semula dengan menggunakan nilai *r* yang baru?

(20/100)

- oooOooo -