UNIVERSITI SAINS MALAYSIA

First Semester Examination
2010/2011 Academic Session

November 2010

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 **SEVEN** printed pages before you start the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **TIGA** soalan di dalam **TUJUH** 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, $|P| = |C| = 32$ bits.
- Key size, $|k| = 16$ bits.

(i) How many possible transformations are there from 32-bit plaintext block to 32-bit ciphertext block?

(10/100)

(ii) How many possible transformations are there from plaintext block to ciphertext block provided by a 16-bit key?

(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?

(10/100)

(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?

(10/100)

(v) Justify your answer in 1(a)(iv).

(20/100)

(b) In earlier computer systems, a password is hashed after its input and is compared to the stored (hashed) reference password. Therefore, on the computer system, only the hashed versions of the passwords are stored.

(i) Assume you are a hacker and you got access to the hashed password list. Discuss which of the three attacks below leads to a successful attack. Exactly describe the consequences of each of the attacks:

- Attack A: You can break the one-way property of h.
- Attack B: You can find second preimages for h.
- Attack C: You can find collisions for h.

(30/100)

(ii) Why is this technique of storing hashed passwords often extended by the use of a so-called salt? (A salt is a random value appended to the password before hashing. Together with the hash, the value of the salt is stored in the list of hashed passwords.)

(10/100)

2. (a) Assume a variant of the OFB mode by which we only feedback the 8 most significant bits of the cipher output. We use AES and fill the remaining 120 input bits to the cipher with 0's (zeros).

(i) Draw a block diagram of the scheme.

(10/100)

(ii) Why is this scheme weak if we encrypt moderately large blocks of plaintext, say100 KByte?

(10/100)

(iii) Based on your answer in 2(a)(ii), what is the maximum number of known plaintexts an attacker needs to completely break the scheme?

(20/100)

(iv) Let the feedback byte be denoted by FB. Does the scheme become cryptographically stronger if we feedback the 128-bit value FB,FB, . . . ,FB to the input (copy the feedback byte 16 times and use it as AES input)?

(20/100)

(b) Answer the following short questions regarding Advance Encryption Standard (AES) cipher.

(i) Shown below is the S-Box used for encryption in Simplified AES. Create the corresponding decryption S-Box for Simplified AES. (Note: Shaded boxes show hexadecimal numbers; unshaded boxes show binary numbers. *i* and *j* are row index and column index, respectively.)

		j			
		00	01	10	11
i	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

Note: Image was taken from: W. Stallings, "Cryptography and Network Security: Principles and Practice", 4th edition, Pearson Education, 2006.

(20/100)

(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.

(20/100)

3. (a) In Diffie-Hellman key exchange protocol, assume Malory can manipulate messages between Alice and Bob. Develop an active attack against the Diffie–Hellman key exchange protocol with Malory being the man-in-the-middle.

(20/100)

(b) For digital signature:

(i) Does confidentiality always guarantee integrity? Justify your answer.

(10/100)

(ii) In which order should confidentiality and integrity be assured?

(10/100)

(c) For RSA:

(i) Let the two primes $p = 41$ and $q = 17$ be given as set-up parameters for RSA. Which of the parameters $e_1 = 32$, $e_2 = 49$ is a valid RSA exponent?

(5/100)

(ii) Justify your answer.

(15/100)

(d) Consider a system in which a key k_{AB} is established using the Diffie–Hellman key exchange protocol, and the encryption keys $k_{(i)}$ are then derived by computing:

$$k_{(i)} = h(k_{AB}, i)$$

where i is just an integer counter, represented as a 32-bit variable. The values of i are public. The derived keys are used for the actual data encryption with a symmetric algorithm. New keys are derived every 60 seconds during the communication session.

(i) Assume the Diffie–Hellman key exchange is done with a 512-bit prime, and the encryption algorithm is AES. Is the key derivation necessary? Justify your answer.

(20/100)

(ii) Describe an attack that would require the least computational effort.

(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, $|P| = |C| = 32$ bit.
- Saiz kunci, $|k| = 16$ bit.

(i) Ada berapa banyak transformasi dari 32 bit blok teks-nyata kepada 32 bit blok teks-sulit?

(10/100)

(ii) Ada berapa banyak transformasi dari blok teks-nyata kepada blok teks-sulit yang diberikan oleh kunci bersaiz 16 bit?

(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*?

(10/100)

(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.

(10/100)

(v) Beri justifikasi kepada jawapan anda di 1(a)(iv).

(20/100)

(b) Dalam penggunaan sistem komputer yang awal, kata laluan akan dicincang selepas diinput, dan dibandingkan dengan kata laluan rujukan (telah dicincang) yang disimpan. Oleh itu hanya versi kata laluan yang telah dicincang sahaja yang disimpan di sistem komputer.

(i) Andaikan anda adalah penggodam komputer dan anda mendapat akses kepada senarai kata laluan tercincang. Bincangkan serangan yang mana daripada tiga serangan di bawah yang membolehkan serangan berkesan dilakukan. Perincikan akibat setiap satu serangan:

- Serangan A: Anda dapat memecahkan sifat sehala *h*.
- Serangan B: Anda boleh mencari praimej kedua untuk *h*.
- Serangan C: Anda boleh mencari pelanggaran untuk *h*.

(30/100)

(ii) Kenapa teknik penyimpanan kata laluan tercincang selalunya dilakukan dengan apa yang dipanggil *salt*? (*Salt* adalah nilai rawak yang dikepilkan bersama kata laluan sebelum cincangan dilakukan. Bersama dengan hasil cincang, nilai *salt* disimpan bersama dalam senarai kata laluan tercincang.)

(10/100)

2. (a) Andaikan satu variasi kaedah OFB yang mana kita hanya bawa ke depan 8 bit terpenting dari hasil sifer. Kita gunakan AES dan penuhkan 120 bit selebihnya dengan bit-bit 0 (kosong) kepada sifer.

(i) Lukis gambar rajah blok untuk skema tersebut.

(10/100)

(ii) Kenapa skema ini lemah jika kita sulitkan blok teks nyata yang agak besar, katakan 100 KBait?

(10/100)

(iii) Berdasarkan kepada jawapan anda pada 2(a)(ii), apakah jumlah maksimum teks-nyata yang diketahui nilainya, yang diperlukan oleh penyerang untuk memecahkan sama sekali skema ini?

(20/100)

(iv) Anggapkan bait suap balik ditandakan dengan FB. Adakah skema itu menjadi lebih kuat pada erti-kata kriptografi, jika kita suap balik nilai 128 bit dengan FB,FB, . . . ,FB kepada input (salin nilai bait suap balik 16 kali dan gunakannya sebagai input kepada AES)?

(20/100)

(b) Jawab soalan-soalan pendek berikut mengenai sifer *Advance Encryption Standard (AES)*.

(i) Ditunjukkan di bawah ialah Kotak-S yang digunakan untuk penyulitan oleh *Simplified AES*. Bina Kotak-S untuk penyahsulitan yang sepadan untuk *Simplified AES*. (Nota: Kotak terlorek menunjukkan nombor perenambelasan; kotak tidak terlorek menunjukkan nombor perduaan. *i* dan *j* ialah indeks baris dan indeks lajur, masing-masing.)

		j			
		00	01	10	11
i	00	9	4	A	B
	01	D	1	8	5
	10	6	2	0	3
	11	C	E	F	7

Nota: Imej diambil daripada: W. Stallings, "Cryptography and Network Security: Principles and Practice", 4th edition, Pearson Education, 2006.

(20/100)

(ii) Dalam AES-128, kunci pusingan yang digunakan pada operasi pra-pusingan adalah sama dengan kunci sifer. Adakah kes yang sama berlaku pada AES-192? Jelaskan.

(20/100)

3. (a) Dalam protokol pertukaran kunci Diffie-Hellman, anggapkan Malory boleh memanipulasi maklumat antara Alice dan Bob. Hasilkan satu serangan aktif terhadap protokol pertukaran kunci Diffie-Hellman dengan Malory menjadi *man-in-the-middle*.

(20/100)

(b) Untuk tandatangan digital:

(i) Adakah kerahsiaan data sentiasa menjamin integriti data? Beri justifikasi kepada jawapan anda.

(10/100)

(ii) Pada turutan, bagaimanakah kerahsiaan dan integriti data patut dipastikan?

(10/100)

(c) Untuk RSA:

(i) Anggapkan dua nombor perdana $p = 41$ dan $q = 17$ diberikan sebagai parameter awalan untuk RSA. Parameter yang manakah $e_1 = 32$, $e_2 = 49$ adalah eksponen RSA yang sah?

(5/100)

(ii) Beri justifikasi kepada jawapan anda.

(15/100)

(d) Anggapkan satu sistem di mana satu kunci k_{AB} telah dijana dengan menggunakan protokol pertukaran kunci Diffie–Hellman, dan kunci-kunci penyulitan $k_{(i)}$ adalah kemudiannya diterbitkan dengan mengira:

$$k_{(i)} = h(k_{AB}, i)$$

di mana i hanyalah satu kaunter integer, yang diwakilkan oleh pemboleh ubah 32 bit. Nilai i diketahui umum. Kunci-kunci terbitan digunakan untuk penyulitan data yang sebenar dengan penggunaan algoritma simetri. Kunci-kunci baru diterbitkan setiap 60 saat semasa sesi komunikasi.

(i) Anggapkan protokol pertukaran kunci Diffie–Hellman dilakukan dengan nombor perdana 512 bit, dan algoritma penyulitan adalah AES. Adakah proses terbitan kunci itu perlu? Beri justifikasi kepada jawapan anda.

(20/100)

(ii) Terangkan satu serangan yang memerlukan usaha pengiraan yang tersedikit.

(20/100)