UNIVERSITI SAINS MALAYSIA

First Semester Examination
2016/2017 Academic Session

December 2016 / January 2017

CCS523 – Computer Security & 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 **SIX** printed pages before you begin the examination.

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

- Answer **ALL** questions.

  *[Jawab **SEMUA** 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.]

- 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) The Affine encryption function for a single letter is defined as: [$E(x) = (ax + b) \bmod n$], where modulus n is the size of the alphabet, while a and b are the keys of the cipher. The value a must be chosen such that a and n are relatively prime. The corresponding decryption function is defined as [$D(y) = a^{-1} (y-b) \bmod n$], where a^{-1} is the modular multiplicative inverse of a modulo n. Two groups of student use the Affine cipher to communicate securely. The first group uses Cambodian characters which has 34 characters (including space) while the second group uses Roman characters which has 27 characters (including space).

Fungsi penyulitan Affine untuk satu huruf ditakrifkan sebagai: [$E(x) = (ax + b) \bmod n$], di mana modulus n adalah saiz abjad, manakala a dan b adalah kunci sifer. Nilai a mesti dipilih supaya a dan n adalah perdana relatif. Fungsi penyahsulitan yang sepadan, ditakrifkan sebagai [$D(y) = a^{-1} (y-b) \bmod n$], di mana a^{-1} adalah berdaraban modular songsang bagi modulo n. Dua kumpulan pelajar menggunakan sifer Affine untuk berkomunikasi dengan selamat. Kumpulan pertama menggunakan abjad-abjad Kemboja yang mempunyai 34 aksara (termasuk ruang) manakala kumpulan kedua menggunakan abjad-abjad Roman yang mempunyai 27 aksara (termasuk ruang).

(i) Which group has more unique keys that they can use in their respective encryption systems? Why?

Kumpulan mana mempunyai kunci-kunci unik yang lebih banyak yang mereka boleh gunakan dalam sistem penyulitan masing-masing. Kenapa?

(20/100)

(ii) One of the students in group two received $y=3$. Given that $a=4$ and $b=4$, what is the corresponding plaintext value?

Seorang pelajar dari kumpulan kedua menerima y=3. Diberikan a=4 dan b=4, apakah nilai teks biasa yang sepadan?

(30/100)

(b) Below are pseudocodes for ARC4 and AES.

Di bawah adalah pseudo-kod ARC4 dan AES.

(i) Modify the code so that the stream cipher produces 4 bits of output at a time, instead of 8 bits at a time. In your answer, please highlight the changes.

Ubah suai kod supaya aliran cipher menghasilkan 4 bit output pada satu-satu masa, dan bukannya 8 bit pada satu-satu masa. Dalam jawapan anda, sila nyatakan perubahan-perubahan yang berlaku dalam jawapan anda.

```
function foo(int[] Key)
    int i, j;
    int[] S;

    for i from 0 to 255
        S[i] := i;
    end_for
    j := 0;
    for i from 0 to 255
        j := (j + S[i] + Key[i mod keylength]) mod 256;
        swap(S[i],S[j]);
    end_for

    i := 0;  j := 0;
    while GeneratingOutput:
        i := (i + 1) mod 256;
        j := (j + S[i]) mod 256;
        swap(S[i],S[j]);
        output S[(S[i] + S[j]) mod 256];
    end_while
end_foo
```

(25/100)

(ii) Modify the following code so that the cipher able to process 256-bit plaintext block with 256-bit key size. State the changes In your answer.

Ubah suai kod supaya sifer tersebut agar dapat memproses blok teks biasa 256-bit dengan sais kunci 256-bit. Nyatakan perubahan-perubahan yang berlaku dalam jawapan anda.

```
Constants: int Nb = 4;
           int Nr = 10;
Inputs: array in  of 4*Nb bytes;
        array out of 4*Nb bytes;
        array w of 4*Nb*(Nr+1) bytes;
        state, 2-dim array of 4*Nb bytes,
               4 rows and Nb cols;

function cipher(byte[] in, byte[] out, byte[] w)
     byte[][] state := new byte[4][Nb];
     state := in;

     AddRoundKey(state, w, 0, Nb - 1);
     for (int round = 1; round < Nr; round++)
         SubBytes(state);
         ShiftRows(state);
         MixColumns(state);
         AddRoundKey(state, w, round*Nb,(round+1)*Nb - 1);
     end_for

     SubBytes(state);
     ShiftRows(state);
     AddRoundKey(state, w, Nr*Nb, (Nr+1)*Nb - 1);
     out := state;
end_cipher
```

(25/100)

2. (a) Diffie-Hellman key exchange protocol was designed to negotiate a secret key between two parties in an open network such as Internet.

Protokol pertukaran kunci Diffie-Hellman telah direka untuk menentukan kunci rahsia antara dua pihak dalam sesuatu rangkaian terbuka seperti Internet.

(i) Modify Diffie-Hellman key exchange protocol so that it can be used to negotiate secret key for three parties.

Ubah suai protokol pertukaran kunci Diffie-Hellman supaya ia boleh digunakan untuk menentukan kunci rahsia untuk tiga parti.

(20/100)

(ii) Extend your solution in (i) so that your protocol can be used to negotiate secret key for n parties. Your solution should have the time complexity of at most *O(n log n).*

Lanjutkan penyelesaian anda di bahagian (i) supaya protokol anda boleh digunakan untuk berunding kunci rahsia untuk n pihak-pihak. Penyelesaian anda perlu mempunyai kekompleksan masa tidak melebihi O(n log n).

(20/100)

(b) Answer each of the following questions with at most four sentences of answers for each.

Jawab setiap soalan-soalan berikut dengan jawapan yang tidak melebihi empat ayat setiap satu.

(i) What is the characteristics of a good firewall implementation?

Apakah ciri-ciri pelaksanaan tembok api yang baik?

(10/100)

(ii) When is a DMZ required? How can it be implemented?

Bila DMZ diperlukan? Bagaimana ia boleh dilaksanakan?

(10/100)

(iii) Explain briefly the meaning of X.509.

Terangkan secara ringkas maksud X.509.

(10/100)

(iv) Explain briefly the meaning of PKI.

Terangkan secara ringkas maksud PKI.

(10/100)

(v) In the context of dynamic biometric user authentication, explain the terms: enrolment, verification and identification.

Dalam konteks pengesahan pengguna biometrik dinamik, jelaskan peristilahan berikut: pendaftaran, pengesahan dan pengenalpastian.

(10/100)

(vi) What is S/MIME? How is it implemented?

Apakah S/MIME? Bagaimana ia dilaksanakan?

(10/100)

3. (a) Alice, Bob, Carol and Dave are four Deputy Vice Chancellors working at one of the local universities. Since the current Vice Chancellor is retiring, they are interested to know if any one of them had been offered to take the post of the Vice Chancellor. However, they want to ensure that no one (including them) should come to know who will be the next Vice Chancellor. Unfortunately, they cannot trust any arbitrator. They only have AES and limited number of secret keys (secret keys between: Alice & Bob, Bob & Carol, Carol & Dave, Dave & Alice). Propose a protocol for them accomplish the task.

Alice, Bob, Carol dan Dave adalah empat Timbalan Naib Canselor yang bekerja di salah sebuah universiti tempatan. Oleh sebab Naib Canselor semasa akan bersara, mereka berminat untuk mengetahui jika salah seorang daripada mereka telah ditawarkan untuk mengambil jawatan Naib Canselor. Namun, mereka mahu memastikan bahawa tidak ada seorangpun daripada mereka mengetahui siapa yang akan menjadi Naib Canselor yang akan datang. Malangnya, mereka tidak boleh mempercayai mana-mana penimbang tara. Mereka hanya mempunyai AES dan bilangan kunci rahsia yang terhad (kunci rahsia antara: Alice & Bob, Bob & Carol, Carol & Dave, Dave & Alice). Cadangkan satu protokol untuk mereka menyelesaikan tugas itu.

(40/100)

(b) The iterated structure of hash function proposed by Merkle is the structure of most hash function in use today (MD-5, SHA-1, etc.).

Struktur fungsi hash berulang yang dicadangkan oleh Merkle adalah struktur fungsi hash yang paling banyak digunakan pada hari ini (MD-5, SHA-1, dan lain-lain).

(i) Draw a diagram showing the construct of the iterated hash function structure proposed by Merkle.

Lukiskan gambar rajah yang menunjukkan struktur fungsi hash berulang yang dicadangkan oleh Merkle.

(10/100)

(ii) If you have to add an XOR function to enhance the security of Merkle's iterated hash function, where would you put the XOR function and why? Use appropriate diagram to explain your answer.

Jika anda perlu menambah fungsi XOR untuk meningkatkan keselamatan fungsi hash berulang Merkle, di mana anda akan meletakkan fungsi XOR tersebut dan mengapa? Guna gambar rajah yang sesuai untuk menjelaskan jawapan anda.

(10/100)

(iii) Construct a parallel hash function based on Merkle iterated hash function structure. Use appropriate diagram to illustrate your idea.

Bina satu fungsi hash selari berdasarkan struktur fungsi hash berulang Merkle. Guna gambar rajah yang sesuai untuk menggambarkan idea anda.

(10/100)

(c) Below are the statements taken from a report belong to a company that had been a victim of an organized cyber-attack.

Berikut adalah kenyataan-kenyataan yang diambil daripada laporan yang dimiliki oleh sebuah syarikat yang telah menjadi mangsa serangan siber terancang.

1. The first attack began around 11:10 UTC on Friday October 21, 2016. We began to see elevated bandwidth against our Managed DNS platform in the Asia Pacific, South America, Eastern Europe, and US-West regions.
2. High-volume floods of TCP and UDP packets, both with destination port 53 from a large number of source IP addresses were present.
3. At roughly 15:50 UTC a second attack began against our Managed DNS platform. This attack was more globally diverse, but employed the same protocols as the first attack.
4. We estimate at the time of this report, there are up to 100,000 malicious endpoints. We are able to confirm that a significant volume of attack traffic originated from Mirai-based botnets.

(i) Explain the type of attack experienced by this organization.

Terangkan jenis serangan yang dialami oleh organisasi ini.

(10/100)

(ii) What is "Mirai"?

Apakah itu "Mirai"?

(10/100)

(iii) Give **one** (**1**) suggestion to prevent such attack in the future.

*Beri **satu** (**1**) cadangan untuk mencegah serangan itu pada masa depan.*

(10/100)