UNIVERSITI SAINS MALAYSIA

First Semester Examination
2015/2016 Academic Session

December 2015/January 2016

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 **NINE** printed pages before you begin 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** 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) A Feistel Network (FN) is a special form of Substitution-Permutation network.

(i) However, in a standard FN, only half of the input is changed in a round. This design affects negatively on the diffusion speed of the plaintext. Provide **two (2)** improvement proposals to the FN structure, to increase the plaintext diffusion speed. Sketch your proposals.

(20/100)

(ii) Many block ciphers are based on the design of FN, however there are few notable ciphers that are not based on FN, for example IDEA and AES. Name the non-linear operations found on IDEA and AES.

(10/100)

(b) Parties $A_{1,\ldots,}A_n$ and B wish to generate a secret conference key. All parties should know the conference key, but an eavesdropper should not be able to obtain any information about the key. They decide to use the following variant of Diffie-Hellman: there is a public prime p and a generator g of Z_p^*. User B picks a secret random $b \in [0, p-1]$ and computes $y = g^b \bmod p$. Each party A_i picks a secret random $a_i \in [0, p-1]$ satisfying $gcd(a_i, p-1) = 1$ and computes $x_i = g^{ai} \bmod p$. User A_i sends x_i to B. User B responds to party i by sending $z_i = x^{bi} \bmod p$.

(i) Show that party i given z_i (and a_i) can determine y.

(20/100)

(ii) Explain why this implies that y can be used as the conference key.

(10/100)

(c) Answer each of the following questions with a four-sentence answer at most.

(i) Explain the difference between digital signature and MAC. Can one be used in place of the other?

(10/100)

(ii) Briefly explain the purpose of certificate chains.

(10/100)

(iii) A server can authenticate a remote workstation by asking it to sign a random message. Why is this method worse than a customized authentication protocol, such as Fiat-Shamir?

(10/100)

(iv) When designing the security component of a large system, should you use an off the shelf standardized cipher or design your own proprietary one?

(10/100)

2. (a) Among the categories of virus; boot sector and macro are two different types of virus which by order of categories mentioned above infect the system boot files and applications that are embedded with macro functionality. Encrypting the executable files can protect software systems. When a program is invoked, the executable files are decrypted and executed. Consider an administrator has two possibilities to store the necessary cryptographic keys:

- The key is stored on a smart card held by an authorised employee with appropriate administrative rights.
- The key is stored in a tamper-resistant device that decrypts and executes commands.

(i) Compare the security of these alternatives.

(20/100)

(ii) How could an attacker bypass these controls?

(10/100)

(iii) To which extent can these controls protect against viral infections?

(10/100)

(b) Answer each of the following questions with a four-sentence answer at most.

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

(10/100)

(ii) When is DMZ required? How is it implemented?

(10/100)

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

(10/100)

(iv) Explain briefly the meaning of PKI.

(10/100)

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

(10/100)

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

(10/100)

3. (a) Consider the following two e-vote protocols in order that voters can send their votes electronically to the Election Authority (EA).

Protocol A:

1. Each voter casts the vote and encrypts it with the public key of the EA.
2. Each voter sends the encrypted vote to the EA.
3. The EA decrypts all the votes to retrieve the original vote, tabulates all the votes, and announces the result of the election.

Protocol B:

1. Each voter casts the vote, and signs it with her private key.
2. Each voter then encrypts the signed vote with the public key of the EA.
3. Each voter sends the vote to the EA.
4. The EA decrypts the vote with its private key, and verifies the signature of the voter with the help of the voter's public key.
5. The EA then tabulates all the votes, and announces the result of the election.

(i) Show that Protocol B is more secure than Protocol A from the perspective of the voters.

(10/100)

(ii) Show that Protocol B is more secure than Protocol A from the perspective of the EA.

(10/100)

(iii) Show that even Protocol B is still lacking in terms of privacy.

(20/100)

(b) Below is a secret splitting scheme. The scheme is devised such a way that neither Alice nor Bob has access to the complete secret, but they can combine their secrets to come up with the required combined secret. The scheme works as follows (Note: Trent is the trusted party).

1. Suppose that the plaintext secret (e.g. a combined password, which needs to be split into two parts) is P.
2. Trent generates a random number R, whose length in bits is exactly the same as that of P.
3. Trent performs an XOR operation on P and R to generate the combined secret, S, as follows: $S = P \oplus R$.
4. Trent now sends S to Alice and R to Bob.

Device a similar protocol, but now the plaintext needs to be distributed to three parties (Alice, Bob and Cindy). All three parties need to combine their secrets to come up with the combined secret.

(30/100)

(c) Below is a scenario of an attack. Note that Tsutomu Shimomura had a trusted relationship between his home computer (X), and the computers at the University of Southern California (Y).

1. Kevin first flooded Tsutomu's home computer (X) with a series of SYN requests, causing it to virtually come to a halt.
2. Kevin then sent a SYN request to the main server (Y) at the University. In this packet, Kevin put the source address as X. That is, the source address was spoofed.
3. The server (Y) detected this as an attempt to establish a request for a TCP connection, and responded back with a SYN ACK response. As expected, the SYN ACK response went back to Tsutomu's home computer (X), because that was the source address in the original SYN request of step 2.
4. Kevin had flooded X in step 1. So, X was not able to see Y's response.

(i) What type of attack is this?

(10/100)

(ii) What are the possible steps after step 4, that Kevin need to take?

(20/100)

1. (a) *Feistel Network* (FN) adalah satu bentuk khas rangkaian *Substitution-Permutation*.

(i) Walau bagaimanapun, dalam FN piawai, hanya separuh daripada input berubah dalam satu pusingan. Reka bentuk ini memberi kesan negatif kepada kelajuan penyebaran teks-nyata. Berikan **dua** (**2**) cadangan penambahbaikan kepada struktur FN, untuk meningkatkan kelajuan penyebaran teks-nyata. Lakarkan cadangan anda.

(20/100)

(ii) Banyak algoritma rahsia blok adalah berdasarkan kepada reka bentuk FN, walau bagaimanapun terdapat beberapa algoritma rahsia blok yang tidak berdasarkan kepada FN, sebagai contoh IDEA dan AES. Namakan operasi tidak linear yang terdapat pada IDEA dan AES.

(10/100)

(b) Pihak $A_{1,...,}A_n$ dan *B* ingin menjana kunci persidangan rahsia. Semua pihak perlu mengetahui kunci persidangan tersebut, tetapi pada masa yang sama pencuri-dengar tidak akan mendapat apa-apa maklumat tentang kunci persidangan itu. Mereka membuat keputusan untuk menggunakan varian algoritma Diffie-Hellman seperti berikut: terdapat nombor perdana awam *p* dan penjana *g* untuk Z_p^*. Pengguna *B* menjana nilai rahsia rawak $b \in [0, p-1]$ dan mengira $y = g^b \bmod p$. Setiap pihak A_i menjana nilai rahsia rawak $a_i \in [0, p-1]$ yang memenuhi $gcd(a_i, p-1) = 1$ dan mengira $x_i = g^{ai} \bmod p$. Pengguna A_i menghantar x_i kepada *B*. Pengguna *B* membalas kepada pihak *i* dengan menghantar $z_i = x^{bi} \bmod p$.

(i) Tunjukkan bahawa parti *i* yang diberi z_i (dan a_i) boleh menentukan *y*.

(20/100)

(ii) Terangkan mengapa *y* boleh digunakan sebagai kunci persidangan itu.

(10/100)

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

(i) Terangkan perbezaan di antara tandatangan digital dan MAC. Bolehkah alatan tersebut digunakan di tempat yang satu lagi?

(10/100)

(ii) Terangkan secara ringkas maksud rantaian sijil.

(10/100)

(iii) Pelayan boleh mengesahkan stesen-kerja jauh dengan meminta stesen tersebut untuk menandatangani mesej secara rawak. Mengapa kaedah ini lebih bahaya daripada protokol pengesahan seperti protokol Fiat-Shamir?

(10/100)

(iv) Apabila mereka-bentuk komponen sistem keselamatan yang besar, adakah anda perlu menggunakan algoritma-rahsia yang terdapat di pasaran, atau mereka-bentuk sistem anda sendiri?

(10/100)

2. (a) Antara klasifikasi virus; virus sektor but dan virus makro adalah dua jenis virus yang masing-masing menyerang fail sistem but dan aplikasi yang menggunakan fungsi makro. Penyulitan atur cara boleh laku melindungi sistem perisian. Apabila program digunakan, atur cara boleh laku dinyah-sulit dan dilaksanakan. Pertimbangkan seorang pentadbir komputer yang mempunyai dua alternatif untuk menyimpan kekunci kriptografi iaitu:

- Kekunci ditempatkan di dalam sebuah kad pintar kepunyaan pekerja yang mempunyai kuasa akses kawalan.

- Kekunci ditempatkan di dalam alat tahan-perubahan yang juga berfungsi untuk menyah-sulit dan melaksanakan arahan.

(i) Bandingkan kedua-kedua alternatif tersebut dari segi keselamatan?

(20/100)

(ii) Bagaimanakah seorang penyerang dapat melepasi kawalan keselamatan ini?

(10/100)

(iii) Bagaimanakah kawalan keselamatan yang diperoleh daripada kedua-dua kaedah penyimpanan kekunci ini memberi jaminan terhadap serangan virus.

(10/100)

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

(i) Apakah ciri-ciri pelaksanaan *firewall* yang baik?

(10/100)

(ii) Bilakah DMZ diperlukan? Bagaimana ia dilaksanakan?

(10/100)

(iii) Terangkan secara ringkas maksud X.509.

(10/100)

(iv) Terangkan secara ringkas maksud PKI.

(10/100)

(v) Dalam konteks pengesahan pengguna biometrik dinamik, jelaskan terminologi berikut: pendaftaran, pengesahan dan pengenalan.

(10/100)

(vi) Apakah S/MIME? Bagaimana ia dilaksanakan?

(10/100)

3. (a) Pertimbangkan dua protokol e-undi berikut supaya pengundi boleh menghantar undi mereka secara elektronik kepada Lembaga Pilihan Raya (EA).

Protokol A:

1. Setiap pengundi membuang undi dan menyulitkan undi dengan kunci awam daripada EA.
2. Setiap pengundi menghantar undi yang telah disulitkan kepada EA.
3. EA menyah-sulit semua undi untuk mendapatkan undi asal, mengira semua undi, dan mengumumkan keputusan pilihan raya itu.

Protokol B:

1. Setiap pengundi membuang undi, dan menandatangani undi tersebut dengan kunci peribadinya.
2. Setiap pengundi kemudian menyulitkan undi yang ditandatangani dengan kunci awam daripada EA.
3. Setiap pengundi menghantar undi kepada EA.
4. EA menyah-sulit undi dengan kunci peribadi, dan mengesahkan tandatangan pengundi dengan bantuan kunci awam pengundi.
5. EA kemudian mengira semua undi, dan mengumumkan keputusan pilihan raya itu.

(i) Tunjukkan bahawa Protokol B adalah lebih selamat daripada Protokol A dari perspektif pengundi.

(10/100)

(ii) Tunjukkan bahawa Protokol B adalah lebih selamat daripada Protokol A dari perspektif EA.

(10/100)

(iii) Tunjukkan bahawa walaupun Protokol B masih tidak mencukupi dari segi privasi.

(20/100)

(b) Di bawah adalah skim pemisahan rahsia. Skim ini dirancang sedemikian rupa sehingga Alice mahupun Bob tidak mempunyai akses kepada rahsia yang lengkap, tetapi mereka boleh menggabungkan rahsia mereka untuk mendapatkan rahsia gabungan yang diperlukan. Skim ini berfungsi seperti berikut (Nota: Trent adalah parti yang dipercayai).

1. Katakan rahsia teks-nyata (misalnya kata laluan gabungan, yang perlu berpecah kepada dua bahagian) adalah P.
2. Trent menjana nombor rawak R, panjangnya dalam bit adalah sama dengan panjang P.
3. Trent melakukan operasi XOR pada P dan R untuk menjana rahsia gabungan, S, seperti berikut: $S = P \oplus R$
4. Sekarang Trent menghantar S kepada Alice dan R kepada Bob.

Bangunkan protokol yang sama, tetapi sekarang teks-nyata perlu diagihkan kepada tiga parti (Alice, Bob dan Cindy). Ketiga-tiga parti perlu menggabungkan rahsia mereka untuk mendapatkan rahsia gabungan.

(30/100)

(c) Di bawah adalah senario serangan. Ambil perhatian bahawa komputer rumah (X) Tsutomu Shimomura mempunyai hubungan saling mempercayai dengan komputer di University of Southern California (Y).

1. Langkah pertama, Kevin membanjiri komputer rumah Tsutomu (X) dengan permintaan SYN, menyebabkan computer itu hampir terhenti.
2. Kemudian Kevin menghantar permintaan SYN kepada pelayan utama (Y) di Universiti. Dalam paket ini, Kevin meletakkan alamat sumber sebagai X. Iaitu, alamat sumber telah diperdaya.
3. Pelayan (Y) mengesan usaha ini sebagai permintaan untuk mewujudkan sambungan TCP, dan memberi maklum balas kembali dengan sambutan SYN ACK. Seperti yang dijangka, sambutan SYN ACK kembali ke komputer rumah Tsutomu (X), kerana itu adalah alamat sumber dalam permintaan SYN asal pada langkah 2.
4. Kevin telah membanjiri X dalam langkah 1. Jadi, X tidak dapat melihat tindak balas Y.

(i) Apakah jenis serangan ini?

(10/100)

(ii) Apakah langkah-langkah, selepas langkah 4 yang mungkin diambil oleh Kevin?

(20/100)