UNIVERSITI SAINS MALAYSIA

First Semester Examination
2014/2015 Academic Session

December 2014/January 2015

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 **FOUR** questions in **THIRTHEEN** printed pages before you begin the examination.

  *[Sila pastikan bahawa kertas peperiksaan ini mengandungi **EMPAT** soalan di dalam **TIGA BELAS** 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) Assume a variant of the CFB mode by which we only feedback the 8 most significant bits of the cipher output. We use AES-128 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, say 100 KByte?

(20/100)

(iii) 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) A private television company, e-ASTRO, wishes to broaden their market by broadcasting their television programs to Internet users who wish to subscribe to their programs. When a person subscribes, she is given a software decoder with a number of secret keys embedded in it. e-ASTRO encrypts the broadcast using a Rijndael with key K. The secret keys in each legitimate decoder can be used to derive K and enable legitimate subscribers to tune in. When a subscriber cancels her subscription, e-ASTRO will encrypt future broadcasts using a new key K'. All valid decoders should be able to derive K', while the cancelled subscriber should not.

(i) Suppose the total number of potential subscribers is less than $n = 10^6$. Let $R_1, R_2, \ldots, R_n$ be 128-bit random values. The decoder shipped to subscriber a number u contains all the R_i's except for R_u (since $n = 10^6$, that means each decoder contains $10^6 - 1 = 999{,}999$ random values). Let S be the set of currently subscribed users. Show that e-ASTRO can construct a key K used to encrypt the broadcast so that any subscriber in S can derive K (from the R_i's in her decoder) while any subscriber outside of S cannot derive K. You should use a one-way SHA-1 hash function for your construction. You may assume that the set S is known to everyone through broadcast. Briefly explain how the subscribers and e-ASTRO can construct key K and why your construction satisfies the required properties.

(25/100)

(ii) Based on your construction in part (i), can two cancelled subscribers combine the secrets embedded in their decoder to build a new operational decoder? Explain.

(25/100)

2. (a) Consider the following scheme:

* Pick an odd number, *e*.
* Pick two prime numbers, *p* and *q*, such that *((p-1)(q-1) - 1) mod e = 0*.
* Calculate *n* and *d* as follows:
  $n = pq$
  $d = ((p-1)(q-1)(e-1) + 1) / e$
* Note: $e, p, q, d \in (0, n)$

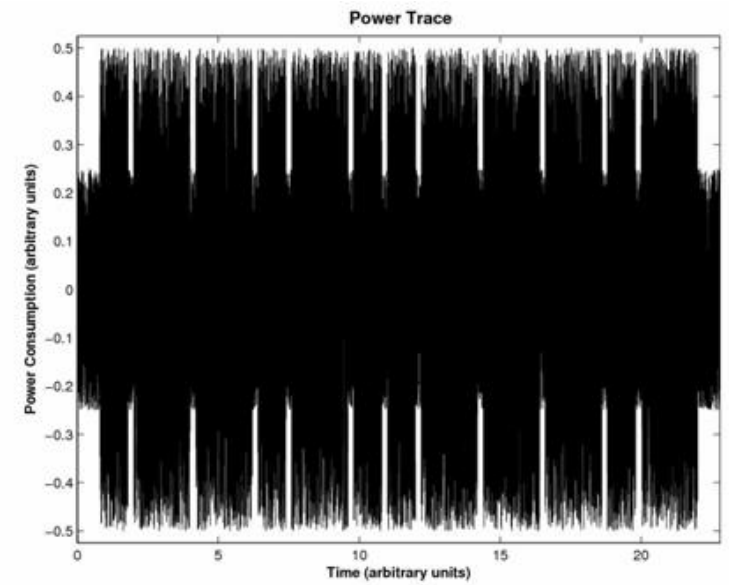
(i) Can *e, d* and *n* always be used as the parameters of RSA? Justify your answer.

(25/100)

(ii) What are the pros and cons of such scheme?

(25/100)

(b) The figure below shows the power trace of a Diffie-Hellman key-exchange implementation on a microprocessor. You can assume the trace was done when Alice calculates her shared-key, *SK*, on a public terminal. The goal is to extract the private key A_{pr} which is used by Alice during the shared-key calculation, $SK = B_{pu}^{Apr} \bmod p$ (Note that the same calculation can be done on Bob's side to recover Bob's shared key). It can be seen clearly the intervals of high activity between short periods of less activity (In fact, the longer ones appear to be about twice as long). This behavior is explained by the square-and-multiply algorithm (refer to Question 2(b)(i) for the algorithm). If an exponent bit has the value 0, only a squaring is performed. If an exponent bit has the value 1, a squaring together with a multiplication is computed. Therefore, this timing behavior reveals, immediately, the key.



(i) Reducing the number of operations in the square-and-multiply algorithm can improve the algorithm performance. Although the number of squarings is fixed, the number of multiplications can be reduced. Your task is to come up with a modified version of the square-and-multiply algorithm which requires fewer multiplications. Give a detailed description on how the new algorithm works.

Hint: Try to develop a generalization of the square-and-multiply algorithm which processes more than one bit at a time. The basic idea is to handle k (e.g., $k = 3$) exponent bit per iteration rather than one bit in the original square-and-multiply algorithm.

Note: The table below shows the Square-and-Multiply Algorithm for Modular Exponentiation.

Algorithm	Algorithm example
Input: base element x exponent $H = \sum_{i=0}^{t} h_i 2^i$ with $h_i \in 0,1$ and $h_t = 1$ modulus n **Output**: $x^H \bmod n$ **Initialization**: $r = x$ **Algorithm**: 1 FOR $i = t - 1$ DOWNTO 0 1.1 $r = r^2 \bmod n$ 1.2 IF $h_i = 1$ 1.2.1 $r = r \cdot x \bmod n$ 2 RETURN (r)	Calculate: $x^{26} = x^{11010} = x^{(h4h3h2h1h0)}$. The algorithm scans the exponent bits, starting on the left with h_4 and ending with the rightmost bit h_0. **Steps** #0 $x = x^{\mathbf{1}}$ — initial setting, bit processed: $h_4 = 1$ #1*a* $(x^1)^2 = x^2 = x^{\mathbf{10}}$ — SQ, bit processed: h_3 #1*b* $x^2 \cdot x = x^3 = x^{10}x^1 = x^{\mathbf{11}}$ — MUL, since $h_3 = 1$ #2*a* $(x^3)^2 = x^6 = (x^{11})^2 = x^{\mathbf{110}}$ — SQ, bit processed: h_2 #2*b* — no MUL, since $h_2 = 0$ #3*a* $(x^6)^2 = x^{12} = (x^{110})^2 = x^{\mathbf{1100}}$ — SQ, bit processed: h_1 #3*b* $x^{12} \cdot x = x^{13} = x^{1100}x^1 = x^{\mathbf{1101}}$ — MUL, since $h_1 = 1$ #4*a* $(x^{13})^2 = x^{26} = (x^{1101})^2 = x^{\mathbf{11010}}$ — SQ, bit processed: h_0 #4*b* — no MUL, since $h_0 = 0$

(25/100)

(ii) What is the impact of the "timing attack" on the newly modified square-and-multiply algorithm? Explain your answer.

(25/100)

3. (a) Classify each of the following as a violation of confidentiality, integrity, availability, or of some combination thereof.

(i) Eve installs Firesheep and hijacks Alice's Facebook session. She reads Bob's messages to Alice and sends a response.

(5/100)

(ii) Julia hacks the website of www.visa.com and adds a message in support of wikileaks.

(5/100)

(iii) Claire installs a sniffer and captures her office mate's traffic.

(5/100)

(iv) Alex posts a message on 4chan, a popular online forum, asking people to visit the slashdot.org website at 2 p.m tomorrow.

(5/100)

(v) Nick pretends to be a system administrator and calls Ellen from the human resources at his company, to ask for her password. He then logs in as Ellen and increases his salary by 20 percent.

(5/100)

(vi) Ann mounts a man-in-the-middle attack by ARP spoofing and redirects all traffic at her student house through her own computer.

(5/100)

(b) Draw a matrix that shows relationship between security services and attacks

(10/100)

(c) The Needham Schroeder protocol is reproduced below.

(1) A → S: A, B, Na
(2) S →A: E(Kas: *Na*, B, Kab, E(Kbs: Kab, A))
(3) A →B: E(Kbs: Kab, A)
(4) B →A: E(Kab: Nb)
(5) A→B: E(Kab: Nb)

(i) Describe (briefly) an attack that may be possible if field *Na* was omitted.

(10/100)

(ii) Describe (briefly) an attack that may be possible if message 5 was omitted.

(10/100)

(d) (i) What is the basic difference between X.509 and PGP in terms of key hierarchies and key trust?

(20/100)

(ii) Consider the following threats to Web Security and describe how each is countered by a particular feature of SSL.

- Brute-force Cryptanalytic Attack: An exhaustive search of key space for a conventional encryption algorithm.
- Replay attack: Earlier SSL handshake messages are replayed.
- Password sniffing: Passwords in HTTP or other application traffic are eavesdropped.
- IP Spoofing: Uses forged IP address to fool a host into accepting bogus data.

(20/100)

4. (a) A corporation establishes routers R1 and R2 at different branches. They enable machines in different branches to communicate securely over the Internet by implementing IPSec at the routers only. That means that when a machine A inside the first network sends an IP packet to a machine B in the second network, the router R1 intercepts the IP packet in transit and encapsulates it into an IPSec packet. At the other end, R2 recovers the original IP packet to be routed in the second network to machine B. Which of the IPSec modes, i.e. tunnel or transport, and AH or ESP, should be used if it was desired that no Internet eavesdroppers learn about the identities A and B of the communicating parties?

(15/100)

(b) (i) An e-commerce company host its site on an Apache-based Linux Web server. There is a worm called "WormBaTTZ", which exploits a buffer overflow bug in the Apache Web server package that can result in a remote root compromise.

Construct a simple threat model that describes the risk this represents: attacker(s), attack-vector, vulnerability, assets, likelihood of occurrence, likely impact, and plausible mitigations.

(35/100)

(ii) Read this excerpt from the news:

The program, Runescape Gold Hack, promised to give the gamer free virtual currency to use in the game - but it in fact was being used to steal log-in details from unsuspecting users. "When the researchers looked at the source code we found interesting information," explained Mr Ben-Itzhak to the BBC. "We found that the malware was trying to steal the data from people and send it to a specific email address."

Explain where this malware is positioned within the types of malware. Recommend effective measures to protect the user against this malware.

(20/100)

(c) List and explain **three** (**3**) network threats that a firewall does not protect against.

(15/100)

(d) Complexity of mobile operating system leads to security threats such as malware attack. List **three** (**3**) approaches to reduce operating system complexity in mobile architecture.

(15/100)

1. (a) Andaikan satu variasi mod CFB yang mana kita hanya suap balik 8 bit paling bererti dari hasil sifer. Kita gunakan AES-128 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 sederhana besar, katakan 100 KBait?

(20/100)

(iiii) Anggapkan bait suap balik ditandakan dengan FB. Adakah skema itu menjadi lebih kuat dalam 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) Sebuah syarikat televisyen persendirian, e-ASTRO, ingin memperluaskan pasaran mereka dengan menyiarkan siaran televisyen mereka kepada penguna Internet yang ingin melanggan siaran mereka. Apabila seseorang melanggan, dia akan diberi sebuah perisian nyah-kod yang mengandungi beberapa kekunci rahsia terbenam di dalamnya. e-ASTRO sulitkan siaran mereka mengunakan Rijndael dengan kekunci *K*. Kekunci-kekunci rahsia yang terdapat di dalam setiap penyahkod yang sah boleh digunakan untuk memperoleh *K* yang membolehkan pelanggan sah menerima siaran. Bila seseorang pelanggan membatalkan langganan, e-ASTRO akan sulitkan siaran-siaran masa hadapan dengan mengunakan kekunci baru *K'*. Semua pennyahkod yang sah akan boleh memperoleh *K'*, tetapi tidak untuk pelanggan yang telah membatalkan langganan mereka.

(i) Andaikan jumlah bakal pelanggan adalah kurang dari $n = 10^6$. Biar $R_1, R_2, \ldots, R_n$ adalah nilai-nilai 128-bit yang rawak. Penyahkod yang dihantar kepada pelanggan *u* mengandungi semua R_i kecuali R_u (oleh kerana $n = 10^6$, ini bermakna setiap penyahkod mengandungi 10^6-1 = 999,999 nilai rawak). Biar *S* adalah set pelanggan-pelanggan semasa yang sah. Tunjukkan e-ASTRO boleh membina kekunci *K* untuk digunakan untuk menyulitkan siaran supaya semua pelanggan-pelanggan dari set *S* boleh memperoleh *K* (dari R_i yang terdapat pada penyahkodnya) manakala semua pelanggan bukan dari set S tidak berupaya untuk membina *K*. Anda perlu menggunakan fungsi cincang satu hala SHA-1 dalam penyelesaian anda. Anda boleh anggapkan set *S* diketahui umum melalui siaran yang disiarkan. Secara ringkas terangkan bagaimana pelanggan dan e-ASTRO boleh membina kekunci *K* dan kenapa penyelesaian anda memenuhi ciri-ciri yang diperlukan.

(25/100)

(ii) Berdasarkan pada penyelesaian (i) anda, bolehkah dua pelanggan yang telah memberhentikan langganan mereka menyatukan rahsia yang terbenam dalam penyahkod mereka untuk membina penyahkod baharu yang boleh berfungsi? Jelaskan.

(25/100)

2. (a) Pertimbangkan skema berikut:

* Pilih nombor janggal, *e*.
* Pilih dua nombor perdana, *p* dan *q*, di mana $((p-1)(q-1) - 1) \bmod e = 0$.
* Kira *n* dan *d* seperti berikut:
  $n = pq$
  $d = ((p-1)(q-1)(e-1) + 1) / e$
* Nota: $e, p, q, d \in (0, n)$

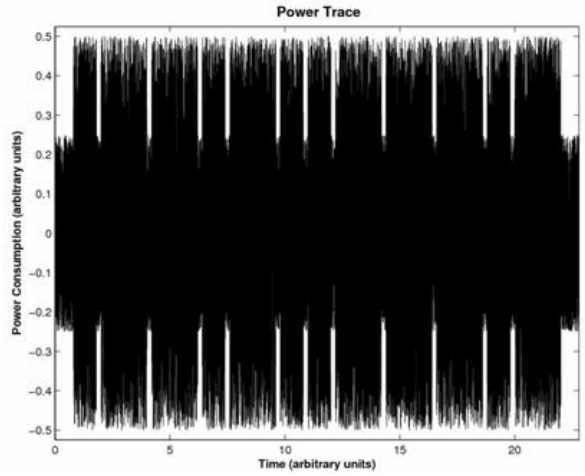
(i) Bolehkah *e, d* dan *n* sentiasa digunakan sebagai parameter RSA? Beri justifikasi kepada jawapan anda.

(25/100)

(ii) Apakah kelebihan dan kekurangan skema tersebut?

(25/100)

(b) Rajah di bawah menunjukkan satu surih kuasa pelaksanaan pertukaran kunci Diffie-Hellman pada sebuah mikropemproses. Anda boleh menganggap surih itu dilakukan apabila Alice mengira kunci kongsi beliau, *SK*, pada terminal awam. Matlamatnya adalah untuk mengekstrak kunci persendirian A_{pr} yang digunakan oleh Alice semasa pengiraan kunci kongsi, $SK = B_{pu}^{Apr} \bmod p$ (Perhatikan bahawa pengiraan yang sama boleh dilakukan di bahagian Bob untuk mendapatkan kembali kunci kongsi Bob). Dapat dilihat dengan jelas selang aktiviti yang tinggi antara tempoh singkat yang kurang aktiviti (Malah, julat aktiviti tinggi adalah kira-kira dua kali ganda julat aktiviti rendah). Kelakuan ini dijelaskan oleh algoritma kuasa-dua-dan-darab *(square-and-multiply)* (rujuk kepada Soalan 2(b)(i) untuk algoritma tersebut). Jika bit eksponen mempunyai nilai 0, hanya kuasa-dua dilakukan. Jika bit eksponen mempunyai nilai 1, kuasa-dua bersama-sama dengan pendaraban adalah dikira. Oleh itu kelakuan pemasaan ini mendedahkan kunci secara terus.



(i) Mengurangkan bilangan operasi dalam algoritma kuasa-dua-dan-darab *(square-and-multiply)* boleh meningkatkan prestasi algoritma tersebut. Walaupun bilangan kuasa-dua ditetapkan, bilangan pendaraban boleh dikurangkan. Tugas anda ialah untuk menghasilkan satu versi algoritma kuasa-dua-dan-darab *(square-and-multiply)* yang telah diubah suai di mana versi tersebut memerlukan kurang bilangan pendaraban. Beri penerangan terperinci bagaimana algoritma baru tersebut berfungsi.

Petunjuk: Cuba generalisasikan algoritma kuasa-dua-dan-darab *(square-and-multiply)* yang memproses lebih daripada satu bit pada satu masa. Idea asas ialah untuk mengendalikan k (contohnya, $k = 3$) bit eksponen pada setiap lelaran dan bukannya satu bit seperti yang terdapat dalam algoritma asal kuasa-dua-dan-darab *(square-and-multiply)*.

Nota: Jadual di bawah menunjukkan algoritma Kuasa-Dua-dan-Darab *(square-and-multiply)* untuk Pengeksponenan Modular

Algorithm	Algorithm example
Input: base element x exponent $H = \sum_{i=0}^{t} h_i 2^i$ with $h_i \in 0,1$ and $h_t = 1$ modulus n **Output**: $x^H \bmod n$ **Initialization**: $r = x$ **Algorithm**: 1 FOR $i = t - 1$ DOWNTO 0 1.1 $r = r^2 \bmod n$ 1.2 IF $h_i = 1$ 1.2.1 $r = r \cdot x \bmod n$ 2 RETURN (r)	Calculate: $x^{26} = x^{11010} = x^{(h4h3h2h1h0)}$. The algorithm scans the exponent bits, starting on the left with h_4 and ending with the rightmost bit h_0. **Steps** #0 $x = x^{\mathbf{1}}$ — initial setting, bit processed: $h_4 = 1$ #1*a* $(x^1)^2 = x^2 = x^{\mathbf{10}}$ — SQ, bit processed: h_3 #1*b* $x^2 \cdot x = x^3 = x^{10}x^1 = x^{\mathbf{11}}$ — MUL, since $h_3 = 1$ #2*a* $(x^3)^2 = x^6 = (x^{11})^2 = x^{\mathbf{110}}$ — SQ, bit processed: h_2 #2*b* — no MUL, since $h_2 = 0$ #3*a* $(x^6)^2 = x^{12} = (x^{110})^2 = x^{\mathbf{1100}}$ — SQ, bit processed: h_1 #3*b* $x^{12} \cdot x = x^{13} = x^{1100}x^1 = x^{\mathbf{1101}}$ — MUL, since $h_1 = 1$ #4*a* $(x^{13})^2 = x^{26} = (x^{1101})^2 = x^{\mathbf{11010}}$ — SQ, bit processed: h_0 #4*b* — no MUL, since $h_0 = 0$

(25/100)

(ii) Apakah kesan daripada "serangan pemasaan" ke atas algoritma kuasa-dua-dan-darab *(square-and-multiply)* yang baru diubahsuai? Jelaskan jawapan anda.

(25/100)

3. (a) Klasifikasi setiap yang berikut sebagai pencabolan kerahsian, integriti, kebolehsediaan atau kombinasi mana-mana di atas.

(i) Eve memasang *Firesheep* dan merampas sesi Facebook Alice. Dia membaca dan membalas mesej yang dihantar oleh Bob kepada Alice.

(5/100)

(ii) Julia menggodam tapak web www.visa.com dan memasukkan mesej bertujuan menyokong *wikileaks*.

(5/100)

(iii) Claire memasang program penghidu dan memerangkap trafik kawan sekerjanya.

(5/100)

(iv) Alex menghantar mesej melalui 4chan, sebuah forum atas talian popular, dan meminta orang ramai melawat tapak web slashdot.org pada pukul 2 petang esok.

(5/100)

(v) Nick menyamar sebagai pentadbir sistem dan menelefon Ellen dari jabatan sumber manusia di syarikatnya untuk meminta kata laluannya. Dia kemudiannya log masuk sebagai Ellen dan menaikkan gajinya sebanyak 20 peratus.

(5/100)

(vi) Ann menjalankan serangan man-in-the middle melalui perdayaan ARP dan mengubah hala trafik ke rumah pelajarnya melalui komputer peribadinya.

(5/100)

(b) Lukiskan matriks yang menunjukkan hubungan antara servis keselamatan dan serangan.

(10/100)

(c) Protocol Needham Schroeder dihasilkan seperti berikut.

(1) A → S: A, B, Na
(2) S →A: E(Kas: *Na*, B, Kab, E(Kbs: Kab, A))
(3) A →B: E(Kbs: Kab, A)
(4) B →A: E(Kab: Nb)
(5) A→B: E(Kab: Nb)

(i) Huraikan (secara ringkas) suatu serangan yang mungkin terjadi jika medan *Na* dihapuskan.

(10/100)

(ii) Huraikan (secara ringkas) suatu serangan yang mungkin terjadi jika mesej 5 dihapuskan.

(10/100)

(d) (i) Nyatakan perbezaan asas antara X.509 dan PGP dari segi hierarki kekunci dan kebolehpercayaan kekunci?

(20/100)

(ii) Pertimbangkan ancaman yang terjadi ke atas Sesawang Keselamatan dan bincangkan bagaimana setiap yang berikut dapat dikendalikan dengan sifat tertentu SSL.

- Serangan Brute-force Cryptanalytic: Sebuah pencarian ruangan kekunci yang lengkap untuk algoritma enkripsi konvensional.
- Serangan Ulangan-tayang: Mesej SSL jabat-tangan terdahulu akan diguna pakai.
- Penghiduan Kata Laluan: Kata laluan pada HTTP dan aplikasi trafik yang lain di curi dengar.
- Perdayaan IP: Penggunaan alamat IP palsu untuk menipu sebuah hos untuk menerima data palsu.

(20/100)

4. (a) Sebuah syarikat menetapkan penghala R1 dan R2 di cawangan yang berbeza. Penghala ini membolehkan mesin di cawangan yang berbeza untuk berkomunikasi dengan selamat melalui Internet dengan melaksanakan IPSec di penghala sahaja. Ini bermakna apabila mesin A dalam jaringan pertama mengirimkan bingkisan IP untuk mesin B dalam jaringan kedua, penghala R1 memintas bingkisan IP dalam transit dan merangkumkannya menjadi sebuah bingkisan IPSec. Pada hujung yang lain, R2 mendapat balik IP asal yang akan dihantar dalam jaringan kedua untuk mesin B. Mod IPSec yang manakah, manakah, iaitu terowong atau pengangkutan, dan AH atau ESP, yang harus digunakan supaya tiada penyadap Internet dapat mengetahui identiti pihak berkomunikasi iaitu A dan B.

(15/100)

(b) (i) Sebuah syarikat e-dagang menghoskan tapak webnya pada pelayan sesawang Linux berasaskan Apache. Terdapat cecacing dinamakan “WormBaTTZ”, yang akan mengekplotasikan pepijat limpahan penimbal dalam pakej pelayan web Apache yang menyebabkan terjadinya remote root.

Bina sebuah model ancaman mudah yang menghuraikan risiko yang diberi dari segi berikut: penyerang, vektor-serangan, kelemahan, aset, kebarangkalian kejadian, impak/kesan yang mungkin dan kaedah mitigasi munasabah.

(35/100)

(ii) Baca petikan ini dari berita:

Program Runescape Gold Hack, berjanji akan memberikan peminat permainan video mata wang maya percuma untuk digunakan dalam permainan - tetapi ia sebenarnya telah digunakan untuk mencuri maklumat log masuk dari pengguna yang tidak curiga. "Ketika para penyelidik melihat kod sumber kami menemukan maklumat yang menarik," jelas Encik Ben-Itzhak kepada BBC. "Kami mendapati bahawa perisian hasad itu cuba untuk mencuri data dari orang dan menghantarkannya ke alamat e-mel yang khusus."

Jelaskan kedudukan *perisian hasad* ini dalam jenis *perisian hasad*. Syorkan langkah-langkah yang berkesan untuk melindungi pengguna terhadap *perisian hasad* ini.

(20/100)

(c) Senaraikan dan terangkan **tiga** (**3**) ancaman rangkaian yang tidak dilindungi oleh tembok api.

(15/100)

(d) Kerumitan sistem operasi mudah-alih menyebabkan ancaman keselamatan seperti serangan *perisian hasad*. Senaraikan **tiga** (**3**) pendekatan yang boleh mengurangkan kerumitan sistem operasi dalam seni bina mudah-alih.

(15/100)