



UNIVERSITI TUN HUSSEIN ONN MALAYSIA

PEPERIKSAAN AKHIR SEMESTER II SESI 2009/2010

NAMA MATA PELAJARAN : KESELAMATAN KOMPUTER

KOD MATAPELAJARAN : BIT 3133

KURSUS : 3 BIT

TARIKH PEPERIKSAAN : APRIL/MEI 2010

JANGKAMASA : 3 JAM

ARAHAN : JAWAB SEMUA SOALAN.

KERTAS SOALAN INI MENGANDUNGI LIMA (5) MUKASURAT

Instruction: Answer **ALL** questions.

- Q1 (a) Explain **FOUR (4)** factors why information security management is needed. (8 marks)
- (b) Discuss **THREE (3)** elements in information security. (12 marks)
- Q2 (a) Explain steps, how the Rivest, Shamir and Adleman (RSA) public and private keys are generated. (10 marks)
- (b) Define the following terms:
- (i) Malicious Code
 - (ii) Workstation Hijacking
 - (iii) Spyware
 - (iv) Cryptanalysis
 - (v) Trojan Horse
- (10 marks)
- Q3 (a) List **TWO (2)** examples of viruses and internet worms (4 marks)
- (b) Explain **FOUR (4)** phases of typical virus life time. (8 marks)
- (c) Describe **TWO (4)** differences between virus and internet worm. (8 marks)

Q4 A rapidly-growing online crime is phishing, in which victims are lured by an e-mail to log on to a website that appears genuine but that actually steals their passwords. You have been hired by a bank to help them improve the security of their online banking services against phishing attacks.

(a) Explain the strengths and weaknesses of the following four possible countermeasures:

(i) a handheld password calculator issued to each customer.

(4 marks)

(iii) displaying a unique picture to each customer during the login process.

(6 marks)

(iv) requiring that large payments, or payments to new recipients, be authorized by telephone or SMS.

(6 marks)

(b) You are told that the budget will accommodate only two of the above options. Which two would you recommend? Justify your recommendation.

(2 marks)

Arahan: Jawab **SEMUA** soalan.

- S1 (a) Jelaskan **EMPAT (4)** faktor kepentingan pengurusan keselamatan maklumat. (8 markah)
- (b) Bincangkan **TIGA (3)** elemen keselamatan maklumat. (12 markah)
- S2 (a) Jelaskan langkah-langkah penjaanaan kunci awam dan kunci peribadi dalam Sistem Kripto River, Shamir dan Adleman (RSA). (10 markah)
- (b) Berikan definisi terma-terma berikut:
- (i) Kod Hasad
 - (ii) *Workstation Hijacking*
 - (iii) *Spyware*
 - (iv) Juruanalisa Kripto
 - (v) Kuda Trojan
- (10 markah)
- S3 (a) Senaraikan **DUA (2)** contoh virus dan cecacing internet (4 markah)
- (b) Jelaskan **EMPAT (4)** kitar hayat virus yang biasa. (8 markah)
- (c) Nyatakan **DUA (2)** perbezaan antara virus dan cecacing internet. (8 markah)

S4 *Phising*, merupakan satu jenayah komputer yang membuatkan pengguna Internet mengakses laman web palsu melalui satu klik pautan di emel pengguna. Melalui laman web palsu ini, katanama dan katalaluan sistem dalam talian pengguna akan terdedah kepada orang yang melakukan *phising*. Kebiasaannya system dalam talian yang terdedah kepada ancaman ini ialah system perbankan internet. Anda, sebagai seorang konsultan telah diupah oleh sebuah bank untuk meningkatkan system perbankan dalam talian bank tersebut bagi menghadapi ancaman *phising*.

(a) Jelaskan **SATU (1)** kelebihan dan kekurangan bagi setiap pilihan di bawah untuk meningkatkan keselamatan perbankan internet

(i) membekalkan *handheld* yang menjana katalaluan kepada setiap pelanggan. (6 markah)

(ii) memaparkan imej unik dan rawak yang perlu dimasukkan setiap kali pelanggan *login*. (6 markah)

(iii) setiap transaksi yang melibatkan jumlah yang besar, atau pembayaran kepada penerima baru perlu pengesahan atau makluman melalui telefon atau khidmat sistem pesanan ringkas. (6 markah)

(b) Anda dimaklumkan bahawa pihak bank akan memilih hanya dua daripada pilihan di atas. Justifikasikan pilihan anda. (2 markah)