UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER II – SESSION 2021 / 2022 / *SEMESTER II – SESI 2021 / 2022*
PROGRAM KERJASAMA

COURSE CODE *KOD KURSUS*	:	DDWC 3343
COURSE NAME *NAMA KURSUS*	:	COMPUTER SECURITY *KESELAMATAN KOMPUTER*
YEAR / PROGRAMME *TAHUN / PROGRAM*	:	3 DDWC
DURATION *TEMPOH*	:	3 HOURS (INCLUDING SUBMISSION HOUR) – REFER ATTACHMENT 1 *3 JAM (TERMASUK MASA PENGHANTARAN) – RUJUK LAMPAIRAN 1*
DATE *TARIKH*	:	JUNE / JULY 2022 *JUN/ JULAI 2022*

INSTRUCTION / *ARAHAN:*

1. The question paper consists of **3 PARTS**: A, B and C.
   *Kertas soalan terdiri daripada **3 BAHAGIAN**: A, B dan C.*

2. Answer **ALL** questions and write your answers on the answer sheet.
   *Jawab **SEMUA** soalan dan tulis jawapan anda pada kertas jawapan.*

3. Write your name, matric no., identity card no., course code, course name, section no. and lecturer's name on the first page (in the upper left corner) and every page thereafter on the answer sheet.
   Tulis nama anda, no. matrik, no. kad pengenalan, kod kursus, nama kursus, no. seksyen dan nama pensyarah pada muka surat pertama (penjuru kiri atas) kertas jawapan dan pada setiap muka surat jawapan.

4. Each answer sheet must have a page number written at the bottom right corner.
   Setiap helai kertas jawapan mesti ditulis nombor muka surat pada bahagian bawah penjuru kanan.

5. Answers should be handwritten, neat and clear.
   Jawapan hendaklah ditulis tangan, kemas dan jelas menggunakan huruf cerai.

WARNING / *AMARAN*

Students caught copying / cheating during the examination will be liable for disciplinary actions and the faculty may recommend the student to be expelled from sitting for exam.
Pelajar yang ditangkap meniru / menipu semasa peperiksaan akan dikenakan tindakan disiplin dan pihak fakulti boleh mengesyorkan pelajar diusir dari menduduki peperiksaan.

This examination paper consists of **12** pages including the cover.
*Kertas soalan ini mengandungi **12** muka surat termasuk kulit hadapan.*

ONLINE EXAMINATION RULES AND REGULATIONS
PERATURAN PEPERIKSAAN SECARA DALAM TALIAN

1. Student must carefully listen and follow instructions provided by invigilator.
   Pelajar mesti mendengar dan mengikuti arahan yang diberikan oleh pengawas peperiksaan dengan teliti.

2. Student is allowed to start examination only after confirmation of invigilator if all needed conditions are implemented.
   Pelajar dibenarkan memulakan peperiksaan hanya setelah pengesahan pengawas peperiksaan sekiranya semua syarat yang diperlukan telah dilaksanakan.

3. During all examination session student has to ensure, that he is alone in the room.
   Semasa semua sesi peperiksaan pelajar harus memastikan bahawa dia bersendirian di dalam bilik.

4. During all examination session student is not allowed to use any other devices, applications except other sites permitted by course lecturer.
   Sepanjang sesi peperiksaan pelajar tidak dibenarkan menggunakan peranti dan aplikasi lain kecuali yang dibenarkan oleh pensyarah kursus.

5. After completing the exam student must inform invigilator via the set communication platform (eg. WhatsApp etc.) about completion of exam and after invigilator's confirmation leave examination session.
   Selepas peperiksaan selesai, pelajar mesti memaklumkan kepada pengawas peperiksaan melalui platform komunikasi yang ditetapkan (contoh: Whatsapp dan lain-lain) mengenai peperiksaan yang telah selesai dan meninggalkan sesi peperiksaan selepas mendapat pengesahan daripada pengawas peperiksaan.

6. Any technical issues in submitting answers online have to be informed to respective lecturer within the given 30 minutes. Request for re-examination or appeal will not be entertain if complains are not made by students to their lecturers within the given 30 minutes.
   Sebarang masalah teknikal dalam menghantar jawapan secara dalam talian perlu dimaklumkan kepada pensyarah masing-masing dalam masa 30 minit yang diberikan. Permintaan untuk pemeriksaan semula atau rayuan tidak akan dilayan sekiranya aduan tidak dibuat oleh pelajar kepada pensyarah mereka dalam masa 30 minit yang diberikan.

7. During online examination, the integrity and honesty of the student is also tested. At any circumstances student is not allowed to cheat during examination session. If any kind of cheating behaviour is observed, UTM have a right to follow related terms and provisions stated in the respective Academic Regulations and apply needed measures.
   Semasa peperiksaan dalam talian, integriti dan kejujuran pelajar juga diuji. Walau apa pun keadaan pelajar tidak dibenarkan menipu semasa sesi peperiksaan. Sekiranya terdapat sebarang salah laku, UTM berhak untuk mengikuti terma yang dinyatakan dalam Peraturan Akademik.

SECTION A / *SEKSYEN A*

OBJECTIVES QUESTIONS / *SOALAN OBJEKTIF*

10 MARKS / *10 MARKAH*

Instruction: Circle your correct answer / *Arahan: Bulatkan jawapan yang betul*

---

1. Which of the following is **FALSE** regarding security risk on e-commerce?
   *Antara berikut, yang manakah **SALAH** berkaitan risiko keselamatan e-dagang?*
   A. Unauthorized transaction appears on your credit card statement.
      Transaksi tanpa kebenaran muncul pada penyata kad kredit anda.
   B. Rely on the internet that might exposed your ID or password to public.
      Bergantung pada internet yang mungkin mendedahkan ID atau kata laluan anda kepada umum.
   C. Identity theft by unknown user.
      Kecurian identiti oleh pengguna yang tidak dikenali.
   D. Legal and Ethical controls action of user.
      Tindakan kawalan undang-undang dan Etika pengguna.

2. To determine whom, you are talking to before revealing sensitive information is a precaution step to avoid network security problem for _____.
   Untuk menentukan dengan siapa, anda bercakap dengan sebelum mendedahkan maklumat sensitif adalah langkah berjaga-jaga untuk mengelakkan masalah keselamatan rangkaian untuk _____.
   A. secrecy / *kerahsiaan*
   B. Authentication / *Pengesahan*
   C. Non-repudiation / *Bukan penolakan*
   D. Data integrity / *Integriti data*

3. Which of the following is **FALSE** about cryptography?
   *Antara berikut, yang manakah **SALAH** tentang kriptografi?*
   A. Cryptography means hidden writing.
      Kriptografi bermaksud tulisan tersembunyi.
   B. A tool for secrecy, integrity, authentication and non-repudiation.
      Alat untuk kerahsiaan, integriti, pengesahan dan bukan penolakan.
   C. The process of coding message so that its meaning is concealed.
      Proses pengekodan mesej supaya maksudnya disembunyikan.
   D. Cryptography used to counter passive and active attack.
      Kriptografi digunakan untuk menentang serangan pasif dan aktif.

4. _____will allow the attacker only monitors the traffic attacking the confidentiality of the data.
   _____*akan membenarkan penyerang hanya memantau trafik yang menyerang kerahsiaan data.*
   A. Passive attack / *Serangan Pasif*
   B. Active attack / *Serangan aktif*
   C. Cryptanalysis / *Analisis kriptografi*
   D. Brute-force attack / Serangan kekerasan

5. Which of the following is asymmetric key cipher?
   Antara berikut, yang manakah sifir kekunci asymmetric?
   A. AES
   B. DES
   C. RSA
   D. Substitution cipher

6. Intruder may insert spurious transactions to a network communication system is the example for _____.

   *Penceroboh boleh memasukkan transaksi palsu ke sistem komunikasi rangkaian adalah contohnya*_____.

   A. Modification. / *Pengubahsuaian*
   B. Fabrication. / *Fabrikasi*
   C. Interruption. / *Gangguan*
   D. Interception. / *Pemintasan*

7. _____ is a principle of adequate protection.

   _____ *adalah prinsip perlindungan yang mencukupi.*

   A. Digital vulnerabilities / *Kelemahan digital*
   B. Storage media / *Media simpanan*
   C. Software vulnerabilities / *Kelemhan perisian*
   D. Hardware vulnerabilities / *Kelemahan perkakasan*

8. _____ is the he importance of security that allow recipient to determine if the message has been altered during transmission.

   _____ *ialah kepentingan keselamatan yang membolehkan penerima menentukan sama ada mesej telah diubah semasa penghantaran.*

   A. Confidentiality / *Kerahsiaan*
   B. Integrity / *Intergriti*
   C. Authentication / *Pengesahan*
   D. Non-repudiation / *Bukan penolakan*

9. Which of the following is **FALSE** about confidentiality?

   *Antara berikut yang manakah **SALAH** tentang kerahsiaan?*

   A. Ensures that computer-related assets are accessed only by authorized parties.
      Memastikan bahawa aset berkaitan komputer hanya diakses oleh pihak yang diberi kuasa.
   B. Confidentiality is sometimes called secrecy or privacy.
      Kerahsiaan kadangkala dipanggil kerahsiaan atau privasi
   C. If some person or system has legitimate access to a particular set of objects, that access should not be prevented.
      Jika sesetengah orang atau sistem mempunyai akses yang sah kepada set tertentu daripada objek, akses itu tidak seharusnya dihalang
   D. Not only reading but also viewing, printing, or simply knowing that particular asset exists.
      Bukan sahaja membaca tetapi juga melihat, mencetak, atau sekadar mengetahui aset tertentu itu wujud

10. Which of the following statement related for amateur's people involved in computer crime?

    Manakah antara pernyataan berikut yang berkaitan dengan golongan amatur yang terlibat dalam jenayah computer?

    A. Normal people who observe a weakness in a security system.
       Orang biasa yang memerhatikan kelemahan dalam sistem keselamatan.
    B. Universities or college students attempt to access computing facilities which they have not being authorized.
       Universiti atau pelajar kolej cuba untukakses kemudahan pengkomputeran yang mereka tidak dibenarkan.
    C. Most computer criminals are ordinary computer professionals orusers doing their jobs and discover that they have access tosomething valuable.
       Kebanyakan penjenayah komputer adalah profesional komputer biasa atau pengguna melakukan kerja mereka dan mendapati bahawa mereka mempunyai akses kepada sesuatu yang berharga.
    D. Majority of cyber crime is perpetrators to date.
       Majoriti jenayah siber adalah pelaku sehingga kini.

SECTION B / *SEKSYEN B*

STRUCTURED QUESTIONS / *SOALAN STRUKTUR*

60 MARKS / *60 MARKAH*

Instruction: This section have **FIVE (5)** questions. Answer all questions.

*Arahan: Bahagian ini mengandungi **LIMA (5)** soalan. Jawab semua soalan.*

---

1. Explain the following term in the context of computer security. Give the example for each context.

   Terangkan istilah berikut dalam konteks keselamatan komputer. Berikan contoh bagi setiap konteks.

   a. Spyware / *Perisian Pengintip*

      i. Explanation / *Penjelasan*:

      ii. Example / *Contoh*:

   b. Logic Bomb / *Bom logik*

      i. Explanation / *Penjelasan*:

      ii. Example / *Contoh*:

   c. Trapdoor / *Perangkap pintu*

      i. Explanation / *Penjelasan*:

      ii. Example / *Contoh*:

   d. Worm / *Cecacing*

      i. Explanation / *Penjelasan*:

      ii. Example / *Contoh*:

   e. Rootkit / *Rootkit*

      i. Explanation / *Penjelasan*:

      ii. Example / *Contoh*:

[10 MARKS / *10 MARKAH*]

2. Give the character and situation for each type of malicious code below:
Berikan contoh ciri ciri dan situasi bagi setiap jenis kod hasad di bawah:

Malicious Code / *Kod Jahat*	**Character /*Ciri-Ciri***	**Situation / *Situasi***
Integrity / *Keutuhan*		
Vulnerabilities / *Kelemahan*		
Threat / *Ancaman*		
Malware / *Peranti jahat*		
Confidentiality / *Kerahsiaan*		

[10 MARKS / *10 MARKAH*]

3. The following are among the database system security requirements.
Berikut adalah antara keperluan keselamatan sistem pangkalan data.

a. Each requirement listed, give reason why are they needed for the security of the database.
Bagi setiap keperluan yang disenaraikan, berikan sebab mengapa ia diperlukan untuk keselamatan pangkalan data.
   i. Data redundancy / *Keterlaluan data*
   ii. Data security / *Keselamatan data*
   iii. Physical database integrity / *Keutuhan fizikal pangkalan data:*

[6 MARKS / *6 MARKAH*]

b. List and explain **TWO (2)** methods that can be used to maintain database integrity in DBMS.
*Senaraikan dan terangkan **DUA (2)** kaedah yang boleh digunakan untuk mengekalkan integriti pangkalan data dalam DBMS.*

[4 MARKS / *4 MARKAH*]

4. Answer the question below regarding cryptography encryption and Diffie-Hilman algorithm.
Jawab soalan di bawah berkenaan penyulitan kriptografi dan algoritma Diffie-Hilman.

a. Compare symmetric and asymmetric encryption. You may explain your comparison by using any drawing and visualization.
Bandingkan penyulitan simetri dan asimetri. Anda boleh menerangkan perbandingan anda dengan menggunakan sebarang kaedah lukisan dan visualisasi.

[7 MARKS / *7 MARKAH*]

b. If p=7 and g=4 and user choose private key $X_A = 4$, what is the public key Y_A?
Jika p=7 dan g=4 dan pengguna memilih kunci persendirian XA = 4, apakah kunci awam Y_A

[3 MARKS / *3 MARKAH*]

c. Referring on question a, if user B has private key $X_B = 3$, what is B public key (Y_B)?
Merujuk kepada soalan a, jika pengguna B mempunyai kunci persendirian XB = 3, apakah kunci awam (YB) B?

[3 MARKS / *3 MARKAH*]

d. Base on answer in question a and b, what is shared key of user A and B?
Berdasaran jawapan bagi soaan a dan b, apakah kunci yang dikongsi antara pengguna A dan B?

[2 MARKS / *2 MARKAH*]

5. Authentication and verification are very important for computer system.
Pengesahan dan pengenal pastian adalah sangat penting untuk sistem komputer.

a. Give the advantages and disadvantages for authentication and verification implementation for computer system.
Berikan kelebihan dan kekurangan bagi pelaksanaan pengesahan dan pengesahan bagi sistem komputer.

[4 MARKS / *4 MARKAH*]

b. List **FIVE (5)** precaution that we can do to prevent unauthorized activity.
*Senaraikan **LIMA (5)** langkah berjaga-jaga yang boleh kita lakukan untuk mencegah aktiviti yang tidak dibenarkan.*

i.
ii.
iii.
iv.
v.

[5 MARKS / *5 MARKAH*]

c. Cerdik Library system was assigned you to develop a system that will consider all security measure for admin and user. List **THREE (3)** possibilities for precaution and prevention that you should consider to develop the system.
*Sistem Perpustakaan Cerdik telah menugaskan anda untuk membangunkan sistem yang akan mempertimbangkan semua langkah keselamatan untuk pentadbir dan pengguna. Senaraikan **TIGA (3)** kemungkinan untuk langkah berjaga-jaga dan pencegahan yang perlu anda pertimbangkan untuk membangunkan sistem*

[6 MARKS / *6 MARKAH*]

SECTION C/ *SEKSYEN C*

SUBJECTIVES QUESTIONS / *SOALAN SUBJEKTIF*

30 MARKS / *30 MARKAH*

Instruction: Answer all questions.

Arahan: Jawab semua soalan.

---

1. Intrusion detection system (IDS) is a device, typically another separate computer, that monitors activity to identify malicious or suspicious events. The security precaution is very important especially for COMB BANK system.

   Sistem pengesanan pencerobohan (IDS) ialah peranti, biasanya komputer berasingan lain, yang memantau aktiviti untuk mengenal pasti peristiwa berniat jahat atau mencurigakan. Langkah berjaga-jaga keselamatan adalah sangat penting terutamanya untuk sistem COMB BANK.

   a. Visualize IDS work mechanism for COMB BANK system.

      Visualisasikan mekanisme kerja IDS untuk sistem COMB BANK.

      [8 MARKS / *8 MARKAH*]

   b. List **SEVEN (7)** function of IDS for COMB BANK system.

      *Senaraikan **TUJUH (7)** fungsi IDS untuk sistem COMB BANK.*

      i.

      ii.

      iii.

      iv.

      v.

      vi.

      vii.

      [7 MARKS / *7 MARKAH*]

2. Rancak Music Entertainment is planning to make an album for their singer in the form of DVD.
Hiburan muzik Rancak sedang merancang untuk membuat album untuk penyanyi mereka dalam bentuk DVD.

   a. There is common legal device for program and data protection act that can be imply for Rancak Music Entertainment. Explain the precaution that you can take as a manager to protect the data and avoid plagiarism.
   Terdapat peranti undang-undang biasa untuk program dan akta perlindungan data yang boleh membayangkan Rancak Music Entertainment. Terangkan langkah berjaga-jaga yang boleh anda ambil sebagai pengurus untuk melindungi data dan mengelakkan plagiarism.

   [7 MARKS / *7 MARKAH*]

   b. Explain the criteria of patent, copyright and trade secret.
   Terangkan kriteria paten, hak cipta dan rahsia perdagangan.

   [8 MARKS / *8 MARKAH*]

- END OF QUESTIONS -

- SOALAN TAMAT -