UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER I – SESSION 2021 / 2022 / *SEMESTER I – SESI 2021 / 2022*

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) *3 JAM (TERMASUK MASA PENGHANTARAN)*
DATE *TARIKH*	: NOVEMBER / DECEMBER 2021 *NOVEMBER / DISEMBER 2021*

INSTRUCTION / *ARAHAN:*

1. The question paper consists of **4 PARTS**: A, B, C and D.
   *Kertas soalan terdiri daripada **4 BAHAGIAN**: A, B, C dan D.*
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 circumstance's 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.

Excerpts from online final exam guidelines
Petikan daripada panduan peperiksaan akhir dalam talian
Universiti Teknologi Malaysia

SECTION A / *SEKSYEN A*

TRUE OR FALSE QUESTIONS / *SOALAN BETUL ATAU SALAH* 10 MARKS / *10 MARKAH*

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

1.	Deniel of Service (DoS) is an example of fabrication security threat. *Deniel of Service (DoS) ialah contoh ancaman keselamatan fabrikasi.*	TRUE / FALSE *BETUL / SALAH*
2.	Interruption happened when the conversation between Azrul and Azri had been eavesdrop by Khairul. *Gangguan berlaku apabila perbualan antara Azrul dan Azri telah didengari oleh Khairul.*	TRUE / FALSE *BETUL / SALAH*
3.	Authentication will determine if the message has been altered during transmission or not. *Pengesahan akan menentukan sama ada mesej telah diubah semasa penghantaran atau tidak.*	TRUE / FALSE *BETUL / SALAH*
4.	Interruption can cause malfunction of an operating system file manager so that it cannot find a particular disk file. *Gangguan boleh menyebabkan kerosakan pada pengurus fail sistem pengendalian sehingga tidak dapat mencari fail cakera.*	TRUE / FALSE *BETUL / SALAH*
5.	Rohana receiving a message that modified by intruders. Its show that the message is non-repudiation. *Rohana menerima mesej yang diubah suai oleh penceroboh. Ia menunjukkan bahawa mesej itu bukan penolakan.*	TRUE / FALSE *BETUL / SALAH*
6.	Secret key for encryption is also known as session key. *Kunci rahsia untuk penyulitan juga dikenali sebagai kunci sesi.*	TRUE / FALSE *BETUL / SALAH*
7.	Digital signature is not implemented using Rivest Shamir Adleman algorithm (RSA). *Tandatangan digital tidak boleh dilaksanakan menggunakan algoritma Rivest Shamir Adleman (RSA).*	TRUE / FALSE *BETUL / SALAH*

8. Trapdoor is a malicious code that use to test the module for future modifications or enhancements. TRUE / FALSE
Trapdoor ialah kod berniat jahat yang digunakan untuk menguji modul untuk pengubahsuaian atau peningkatan pada masa hadapan. *BETUL / SALAH*

9. Mr Zakri withdraw his money and he lost 0.01 cents for each transaction. He considers he was attacked by Salami attack. TRUE / FALSE
Encik Zakri mengeluarkan wangnya dan dia kehilangan 0.01 sen bagi setiap transaksi. Dia menganggap dia telah diserang oleh serangan Salami. *BETUL / SALAH*

10. Logic bomb will allow someone from remote location to take control of your computer. TRUE / FALSE
Bom logik akan membolehkan seseorang dari lokasi terpencil mengawal komputer anda. *BETUL / SALAH*

SECTION B / *SEKSYEN B*

MULTIPLE CHOICE QUESTIONS / *SOALAN OBJEKTIF*

10 MARKS / *10 MARKAH*

Instruction: Circle your correct answer in your answer sheet.

Arahan: Bulatkan jawapan yang betul di kertas jawapaan anda.

---

1. _____ is an asset of the system becoming lost, unavailable, or unusable.
   _____ *ialah aset sistem menjadi hilang, tidak tersedia atau tidak boleh digunakan.*
   A. Interruption / *Gangguan*
   B. Interception / *Pemintasan*
   C. Modification / *Pengubahsuaian*
   D. Fabrication / *Fabrikasi*

2. What is malicious code that often used to launch distributed denial of service (DDoS) attacks?
   Apakah kod berniat jahat yang sering digunakan untuk melancarkan serangan penolakan perkhidmatan (DDoS) yang diedarkan?
   A. Zombie / *Zombi*
   B. Logic bomb / *Bom logik*
   C. Rootkits / *Rootkits*
   D. Trapdoor */ Pintu perangkap*

3. Which of the followings are virus phase in virus operation?
   Manakah antara berikut meupakan fasa virus dalam pengendalian virus?
   A. Dormant / *Tidak aktif*
   B. Propagation / *Pembiakan*
   C. Triggering / *Mencetuskan*
   D. All above / *Semua di atas*

4. Log in and sign up process is a mechanism for _____.
   Proses log masuk dan daftar adalah mekanisme untuk _____.
   A. Authorization / *Keizinan*
   B. Integrity / *Integriti*
   C. Authentication / *Pengesahan*
   D. Privacy / *Peribadi*

5. Fence is a mechanism to protect memory and addressing. Where is usually fence implemented?
   Pagar adalah mekanisme untuk melindungi ingatan dan pengalamatan. Di mana biasanya pagar dilaksanakan?
   A. Software / *Perisian*
   B. Hardware / *Perkaakasan*
   C. Operating system / *Pengoperasian computer*
   D. System software / *Sistem perisian*

6. Who is the person that have a power to define rule, organize data and controls access of the data?
   Siapakah orang yang mempunyai kuasa untuk tetapkan peraturan, mengatur data dan mengawal capaian data tersebut?
   A. Database administrator / *Pentadbir pangkalan data*
   B. System Analyst / *Penganalisis Sistem*
   C. Project manager / *Pengurus projek*
   D. Project leader / *Ketua projek*

7. How user make a request for data results from database or for action on the data?
   Bagaimanakah pengguna membuat permintaan untuk keputusan data daripada pangkalan data atau untuk tindakan ke atas data?
   A. Normalization data / *Data normalisasi*
   B. Primary key / *Kunci utama*
   C. Query / *Pertanyaan*
   D. Entity / Entiti

8. Which of the following is **NOT** sensitivity label for integrity lock?
   *Manakah antara berikut **BUKAN** label sensitiviti untuk kunci integriti?*
   A. Unforgeable / *Tidak boleh dipalsukan*
   B. Concealed / *Disembunyikan*
   C. Sharable / *Boleh dikongsi*
   D. Unique / *Unik*

9. Which of the following policy statement is **NOT TRUE?**
   *Manakah antara pernyataan dasar berikut yang **TIDAK BENAR**?*
   A. Policy need an organization that understand the vulnerabilities to which it may be exposed.
      Dasar memerlukan organisasi yang memahami kelemahan yang mungkin terdedah kepadanya.
   B. A security plan must state the organization's policy on security.
      Pelan keselamatan mesti menyatakan polisi keselamatan organisasi.
   C. The requirements should address all aspects of security confidentiality, integrity, and availability.
      Keperluan harus menangani semua aspek kerahsiaan keselamatan, integriti dan ketersediaan.
   D. The policy must clearly state a plan and action for any lost or disaster for the system.
      Polisi mesti menyatakan dengan jelas rancangan dan tindakan untuk sebarang kehilangan atau bencana bagi sistem.

10. Gives the author the exclusive right to make copies of the expression and sell them to the public is a protecting program and data for _____.
    Memberi pengarang hak eksklusif untuk membuat salinan ungkapan dan menjualnya kepada orang ramai adalah program dan data yang melindungi untuk _____.
    A. Patent / *Paten*
    B. Copyrights / *Hak Cipta*
    C. Trade Secrets / *Rahsia Perdagangan*
    D. Policy / *Polisi*

ANSWER:

1	2	3	4	5	6	7	8	9	10

SECTION C / SEKSYEN C
STRUCTURED QUESTIONS / SOALAN BERSTRUKTUR
40 MARKS / 40 MARKAH

Instruction: Answer *ALL* questions in your answer sheet.
Arahan: Jawab SEMUA soalan di kertas jawapan anda.

---

1. Described malicious code below, and give a solution to solve the problem
   Terangkan kod hasad di bawah, dan berikan penyelesaian untuk menyelesaikan masalah

   a. Rootkits / *Rootkit* **[2 M]**
      i. Definition / *Definisi* :
      ii. Solutions / *penyelesaian* :

   b. Logic Bomb / *Bom Logik* **[2 M]**
      i. Definition / *Definisi* :
      ii. Solutions / *penyelesaian* :

   c. Salami Attack / *Serangan Salami* **[2 M]**
      i. Definition / *Definisi* :
      ii. Solutions / *penyelesaian* :
      :

2. Explain the **TWO (2)** differences between Data Encryption System (DES) and Advanced Encryption System (AES). Give **TWO (2)** example of each method. **[8 M]**
   2. Terangkan DUA (2) perbezaan antara Sistem Penyulitan Data (DES) dan Sistem Penyulitan Lanjutan (AES). Berikan DUA (2) contoh bagi setiap kaedah.

Cipher / *Cipher*	**Differents / *Perbezaan***	**Example / *Contoh***
Data Encryption System (DES) *Sistem Penyulitan Data (DES)*		
Advanced Encryption System (AES) *Sistem Penyulitan Lanjutan (AES)*		

3. Maisarah want to send a secret message to Aminah using public-key encryption. During message sending, Maisarah creates digital envelope when sending confidential message to Aminah.
Maisarah ingin menghantar mesej rahsia kepada Aminah menggunakan penyulitan kunci awam. Semasa penghantaran mesej, Maisarah mencipta sampul digital apabila menghantar mesej sulit kepada Aminah.

a. Explain the importance of digital envelope for Maisarah sending message to Aminah? **[2 M]**
Terangkan kepentingan sampul digital untuk Maisarah menghantar mesej kepada Aminah?

b. Illustrate the opening of the digital envelop by Aminah. [**6 M]**
Tunjukkan bagaimana pembukaan sampul surat digital oleh Zainab

c. Aminah get a message from Maisarah. She wants to make sure the message is from authenticated and authorized user. Modify a digital signature illustration in 3b to authenticate the message in the digital envelop. [**6 M]**
Aminah mendapat mesej daripada Maisarah. Dia mahu memastikan mesej itu daripada pengguna yang disahkan dan dibenarkan. Ubah suai ilustrasi tandatangan digital dalam 3b untuk mengesahkan mesej dalam sampul digital

4. Explain the advantages of using database: [**6M]**
Jelaskan kelebihan menggunakan pangkalan data:

a. Data sharing :
Perkongsian data :

b. Data redundancy :
Pertindihan data :

c. Data Integrity :
Intergriti data :

5. Khairul planning to build his own company. He wants to make sure his company protected by a good security to identifies and organizes the security activities for a computing system. As a network specialist, please help Mr Zamir to develop his company to make a security plan.

[6 M]

Khairul berhasrat untuk menubuhkan syarikatnya. Dia ingin memastikan syarikatnya memiliki sistem keselamatan yang bagus untuk mengenal pasti dan menyusun aktiviti sistem syarikatnya. Sebagai pakar rangkaian, bantu En Zamir untuk menyediakan plan keselamatan bagi syarikatnya.

SECTION D / *SEKSYEN D*
SUBJECTIVES QUESTIONS / *SOALAN SUBJEKTIF*
40 MARKS / *40 MARKAH*

Instruction: Answer *ALL* questions in your answer sheet.
Arahan: Jawab SEMUA soalan di kertas jawapan anda.

---

1. Give **THREE (3)** differences between cryptographic hash function and encryption. **[6 M]**
   *Berikan **TIGA (3)** perbezaan antara kriptografi fungsi hash and juga enkripsi*

2. DES is a block encryption consisting of 16 cycles of transposition and substitution process. One of the steps is DES key transformation. Explain DES key transformation and what is the size of DES key after transformation process. **[6 M]**
   DES adalah enkripsi blok yang merangkumi 16 pusingan proses transposisi dan penggantian. Salah satu dari langkah adalah langkah transformasi kunci DES. Jelaskan proses tranformasi kunci dan nyatakan saiz kunci DES selepas proses transformasi.

3. Answer the questions below regarding key generation in Diffie-HeIlman and RSA.
   Jawab soalan berikut mengenai penjanaan kunci dalam Diffie-Hellman and RSA

   a. Suppose the Diffie-Hellman public values p and g are 7 and 4, respectively. If user A choose private key $X_A = 4$. What is A's public key Y_A? **[3 M]**
      Katakan nilai umum bagi Diffie-Hellman p dan g adalah masing-masing 7 dan 4 Jika pengguna A memilih kunci peribadi $X_A = 4$. Apakah kunci umum pengguna A, Y_A ?

   b. Referring to 3 (a), if user B has private key $X_B = 5$, what is B's public key Y_B? **[3 M]**
      Merujuk kepada 3 (a), jika pengguna B mempunyai kunci peribadi $X_B = 5$ apakah kunci umum B, Y_B?

   c. What is the shared key? **[3 M]**
      Apakah kunci yang dikongsi?

d. Suppose that you are computing an RSA key pair. What is p and q and ϕ (n) for an n = 51? Find the RSA public key pair for this p and q. **[8 M]**

Andaikan bahawa anda mengira satu pasangan kunci RSA. Apakah p dan q dan ϕ(n) untuk n = 51? Cari kunci umum RSA dari pasangan p dan q ini.

e. Given p=17, q=11. Diana sending a message to Hajar using a public key, 7. Find the value of n and ϕn.

i. Form the value in 3(e), find a private key value using $d=e^{-1} \bmod \phi(n)$.

ii. What is the message received by Hajar if the message sending from Diana is 5?

iii. Form the value in 3(e)(i-ii), decrypt the message received by Hajar.

[11 M]

e. *Diberi p=17, q=11. Diana menghantar mesej kepada Hajar menggunakan kunci awam, 7. Cari nilai n dan ϕn.*

i. Bentukkan nilai dalam 3(e), cari nilai kunci persendirian menggunakan d=e-1 mod ϕ (n).

ii. Apakah mesej yang diterima oleh Hajar jika mesej yang dihantar daripada Diana adalah 5?

iii. Bentukkan nilai dalam 3(e)(i-ii), nyahsulit mesej yang diterima oleh Hajar.

END OF QUESTIONS

KERTAS SOALAN TAMAT