



FINAL EXAMINATION / PEPERIKSAAN AKHIR
SEMESTER I – SESSION 2020 / 2021 / SEMESTER I – SESI 2020 / 2021

COURSE CODE : DDWC 3343
KOD KURSUS

COURSE NAME : COMPUTER SECURITY
NAMA KURSUS KESELAMATAN KOMPUTER

YEAR / PROGRAMME : 3 DDWC
TAHUN / PROGRAM

DURATION : 3 HOURS (INCLUDING SUBMISSION HOUR) – REFER ATTACHMENT 1
TEMPOH 3 JAM (TERMASUK MASA PENGHANTARAN) – RUJUK LAMPAIRAN 1

DATE : OCTOBER 2020
TARIKH OKTOBER 2020

INSTRUCTION / ARAHAN:

1. The question paper consists of **2 PARTS**: A and B.
*Kertas soalan terdiri daripada 2 **BAHAGIAN**: A dan B.*
 2. Answer **ALL** questions and write your answers on the question sheet.
*Jawab **SEMUA** soalan dan tulis jawapan anda pada kertas soalan.*
 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 **13** pages including the cover.
*Kertas soalan ini mengandungi **13** 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 / BAHAGIAN A

TRUE/FALSE : 10 MARKS

BENAR/SALAH : 10 MARKAH

Answer the following questions TRUE or FALSE in page 7.

Jawab soalan-soalan berikut BENAR atau SALAH di muka surat 7.

1. Interruption : some unauthorized party has gained access to an asset.
Gangguan: beberapa parti yang tidak diberi kebenaran mempunyai akses terhadap satu aset.
2. Career criminals are involved on most of the computer crimes reported to date.
Penjenayah bekerja terlibat dalam kebanyakan jenayah komputer yang dilaporkan hingga ke hari ini.
3. Cryptanalyst are people who study encryption and encrypted messages on behalf of a legitimate sender / receiver.
'Cryptanalyst' adalah orang yang belajar mengenkrip dan mendekrip mesej bagi pihak penghantar/ penerima yang sah di sisi undang-undang.
4. Permutation is a technique that randomly take a key from any piece of music with which the structure can be analyzed.
'Permutation' adalah teknik yang mengambil kekunci secara rawak daripada bahagian muzik yang mana strukturnya boleh dianalisa.
5. Worm: Replicates itself without limit to exhaust resource.
Cecacing: Menambah dirinya tanpa had untuk melemahkan sumber.
6. Executive design to assist individual programmers and to smooth transition from one user to another.
Eksekutif direkabentuk untuk membantu pengaturcara individu dan untuk melancarkan transisi dari satu pengguna kepada pengguna yang lain.

7. Fences are designed to prevent a faulty user program from destroying part of the resident's portion of the OS in the memory.

Pagar direkabentuk untuk menghalang program pengguna ralat daripada menghapuskan sebahagian daripada bahagian OS yang masih tinggal dalam ingatan.

8. The middle security policies in military are called confidential.

Polisi tengah keselamatan dalam ketenteraan dipanggil rahsia.

9. Logical database integrity: the structure of the database is preserved - modifying would not affect other field.

Integriti pangkalan data logik: struktur pangkalan data dipelihara - ubahsuai tidak akan memberi kesan kepada bahagian lain.

10. Port scan: Gathering discrete bits of information from various sources and then putting them together like the pieces of a puzzle.

Imbasan port: Mengumpulkan maklumat daripada pelbagai sumber dan kemudian meletakkannya bersama seperti mencantumkan teka-teki.

SECTION B / BAHAGIAN B

MATCH QUESTION : 20 MARKS

SOALAN PADANAN : 20 MARKAH

Write the correct answer in page 7.

Tulis jawapan yang betul di muka surat 7

Fill in the blank for the questions below with the answer choices given.

Isikan tempat kosong bagi soalan di bawah dengan pilihan jawapan yang disediakan.

Segmentation	Anonymity	Patents	Wiretap	Concurrency
Algorithm	Declare	Concurrency	Reverse Engineering	Forward Engineering
Redundancy	Logical Database Integrity	Application Proxies.	Physical Database Integrity	Sharing
Stateful Inspection	Inherently	Bounds Registers	Copyright	Eavesdrop

1. _____ provide base or starting address.
_____ *menyediakan alamat asas atau permulaan.*
2. _____ meaning that the structure of the database is preserved – modifying would not affect other field.
_____ *bermaksud bahawa struktur bagi pangkalan data adalah terpelihara – pengubahsuaian tidak akan melibatkan medan yang lain.*
3. _____ will happened when there is no conflict if two users attempt to read the same data items.
_____ *akan berlaku apabila tiadakah konflik jika dua pengguna cuba membaca item data yang sama.*

4. A defensive missiles location is an example of _____ sensitive data.
Lokasi peluru berpandu pertahanan adalah contoh bagi data sensitif _____.

5. Because networks enable resource and workload sharing, more users have the potential to access networked systems. This statement referred to _____.
Kerana rangkaian membenarkan perkongsian sumber dan kerja, ramai pengguna mempunyai potensi untuk mencapai sistem rangkaian. Pernyataan ini merujuk kepada _____.

6. _____ intercepting communications through some effort.
_____ merupakan pintasan komunikasi dengan sedikit usaha.

7. Simulate the (proper) effects of an application so that the application will receive only requests to act properly referred to _____ type of firewall.
Simulasi kesan (sesuai) bagi aplikasi supaya apliasi tersebut akan menerima hanya permintaan untuk tindakan yang sesuai merujuk kepada jenis firewall _____.

8. The cryptosystem involves a set of rules for how to encrypt the plaintext and how to decrypt the cipher text. These rules are called _____.
Cryptosystem terdiri daripada set undang-undang tentang bagaimana untuk mengenkrip teks asal dan bagaimana untuk mendekrip teks cipher. Undang-undang ini dipanggil _____.

9. Trade secret is easily discovered by using _____.
Rahsia perniagaan mudah didapati dengan menggunakan _____.

10. _____ are designed to protect the expression of idea.
_____ direkabentuk untuk memelihara ekpresi idea.

Section A / *Bahagian A*

1		6	
2		7	
3		8	
4		9	
5		10	

Section B / *Bahagian B*

1		6	
2		7	
3		8	
4		9	
5		10	

SECTION C / BAHAGIAN C

STRUCTURE : 70 MARKS

STRUKTUR : 70 MARKAH

Answer all the following questions.

Jawab semua soalan-soalan berikut.

1. A **threat** is blocked by **control** of **vulnerability**. Give the meaning of threat, control and vulnerability? [6 M]
Ancaman dihalang oleh kawalan terhadap kebolehceroohan. Berikan maksud ancaman, kawalan dan kebolehceroohan?

2. Explain the **MOM syndrome** (*Method, Opportunity, Motive*) in context of an attacker? [9 M]
Terangkan sindrom MOM (Method, Opportunity, Motive) dalam konteks seorang penyerang

3. Policies and procedure are one of the methods in defending our computer from any threat. Explain the method with an example. [4 M]
Polisi dan prosedur adalah satu daripada kaedah untuk mempertahankan komputer kita daripada sebarang ancaman. Terangkan kaedah ini beserta satu contoh talian.
4. What is the difference between symmetric and asymmetric encryption? [4 M]
Apakah perbezaan antara enkripsi 'symmetric' dan 'asymmetric'?
5. Two simple form of encryption are substitution and transposition. Explain briefly the different between these two types of encryption. [4 M]
Dua bentuk mudah dalam enkripsi adalah 'substitution' dan transposition'. Terangkan secara ringkas perbezaan di antara kedua jenis enkripsi ini.

6. Vernam ciphers are devised by Gilbert Vernam for AT&T. Encrypt the plaintext below by using the Vernam ciphers technique and given random number. Write your calculation. [10 M]

'Vernam ciphers' dicipta oleh Gilbert Vernam untuk AT&T. Enkrip meses asal di bawah dengan menggunakan teknik 'Vernam ciphers' dan nombor rawak yang diberikan. Tuliskan kira-kira anda.

Plaintext : LAUT CHINA SELATAN JAM TUJUH
Random number : 54, 11, 34, 21, 21, 45, 65, 89, 77, 42, 44, 67, 13, 14,
90, 67, 13, 18, 67, 83, 67, 88, 49, 68.

7. In the taxonomy, the inadvertent flaws fall into six categories. Give **five (5)** of inadvertent flaws that you know. [5 M]

*Dalam taxonomi, kecelaan yang tidak disengajakan jatuh kepada enam kategori. Berikan **lima (5)** daripada kecelaan yang tidak disengajakan yang anda tahu.*

8. List **four (4)** object that need to be protected in operating system. [2 M]

*Senaraikan **empat (4)** objek yang perlu dilindungi dalam sistem pengoperasian.*

9. Explain **five (5)** methods that an attacker could use to attacks on password. [5 M]

*Terangkan **lima (5)** kaedah yang boleh digunakan oleh penyerang untuk menyerang kata laluan.*

10. Below are the table qualities of security and trustedness. Fill the appropriate content for the blank space in the figure. [10 M]

Di bawah adalah jadual kualiti bagi keselamatan dan kebolehpercayaan. Penuhkan ruang kosong dalam jadual tersebut dengan kandungan yang sesuai.

Secure	Trusted
<i>Either-or.</i> Something either is or is not secure.	
	Property of <i>receiver</i> .
<i>Asserted</i> based on product characteristics.	
	<i>Relative</i> : viewed in context of use.
<i>A goal</i> .	

11. Database concerns about reliability and integrity can be viewed from three dimensions. Name those **three (3)** dimensions. [3 M]

*Kepentingan pangkalan data terhadap kebolehpercayaan dan integriti boleh dilihat daripada tiga dimensi. Namakan **ketiga-tiga (3)** dimensi tersebut.*

12. Anonymity is one of a threat in network. What are the meanings of anonymity in network? [2 M]

'Anonymity' adalah salah satu ancaman terhadap rangkaian. Apakah maksud anonymity dalam rangkaian?

13. Explain **three (3)** methods that we can use to protect our program and data. [6 M]
*Terangkan **tiga (3)** kaedah yang boleh kita gunakan untuk melindungi program dan data kita.*

End of Question / Tamat Soalan