UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER II – SESSION 2022 / 2023
PROGRAM KERJASAMA

COURSE CODE *KOD KURSUS*	:	DDWD 3343
COURSE NAME *NAMA KURSUS*	:	COMPUTER SECURITY / *KESELAMATAN KOMPUTER*
YEAR / PROGRAMME *TAHUN / PROGRAM*	:	3 DDWD
DURATION *TEMPOH*	:	2 HOURS 30 MINUTES *2 JAM 30 MINIT*
DATE *TARIKH*	:	JUNE / JULY 2023 *JUN / JULAI 2023*

INSTRUCTION :
ARAHAN

ANSWER **ALL QUESTIONS** IN QUESTION BOOKLET.

*JAWAB **SEMUA SOALAN DI** DALAM BUKU SOALAN.*

(You are required to write your name and your lecturer's name on your answer script)
(Pelajar dikehendaki tuliskan nama dan nama pensyarah pada skrip jawapan)

NAME / *NAMA PELAJAR*	:	.....
I.C NO. / *NO. K/PENGENALAN*	:	.....
YEAR / PROGRAMME *TAHUN / PROGRAM*	:	.....
COLLEGE NAME *NAMA KOLEJ*	:	.....
LECTURER'S NAME *NAMA PENSYARAH*	:	.....

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

UTM | School of Professional and Continuing Education (SPACE)
UNIVERSITI TEKNOLOGI MALAYSIA

PUSAT PRGORAM KERJASAMA

PETIKAN DARIPADA PERATURAN AKADEMIK
ARAHAN AM – PENYELEWENGAN AKADEMIK

1. SALAH LAKU SEMASA PEPERIKSAAN

1.1. Pelajar tidak boleh melakukan mana-mana salah laku peperiksaan seperti berikut :-

1.1.1. memberi dan/atau menerima dan/atau memiliki sebarang maklumat dalam bentuk elektronik, bercetak atau apa jua bentuk lain yang tidak dibenarkan semasa berlangsungnya peperiksaan sama ada di dalam atau di luar Dewan/Bilik Peperiksaan melainkan dengan kebenaran Ketua Pengawas; atau

1.1.2. menggunakan maklumat yang diperoleh seperti di atas bagi tujuan menjawab soalan peperiksaan; atau

1.1.3. menipu atau cuba untuk menipu atau berkelakuan mengikut cara yang boleh ditafsirkan sebagai menipu semasa berlangsungnya peperiksaan; atau

1.1.4. lain-lain salah laku yang ditetapkan oleh Universiti (seperti membuat bising, mengganggu pelajar lain, mengganggu Pengawas menjalankan tugasnya).

2. HUKUMAN SALAH LAKU PEPERIKSAAN

2.1. Sekiranya pelajar didapati telah melakukan pelanggaran mana-mana peraturan peperiksaan ini, setelah diperakukan oleh Jawatankuasa Peperiksaan Fakulti dan disabitkan kesalahannya, Senat boleh mengambil tindakan dari mana-mana satu yang berikut :-

2.1.1. memberi markah SIFAR (0) bagi keseluruhan keputusan peperiksaan kursus yang berkenaan (termasuk kerja kursus); atau

2.1.2. memberi markah SIFAR (0) bagi semua kursus yang didaftarkan pada semester tersebut.

2.2. Jawatankuasa Akademik Fakulti boleh mencadangkan untuk diambil tindakan tatatertib mengikut peruntukan Akta Universiti dan Kolej Universiti, 1971, Kaedah-kaedah Universiti Teknologi Malaysia (Tatatertib Pelajar-pelajar), 1999 bergantung kepada tahap kesalahan yang dilakukan oleh pelajar.

2.3. Pelajar yang didapati melakukan kesalahan kali kedua akan diambil tindakan seperti di perkara dan dicadang untuk diambil tindakan tatatertib mengikut peruntukan Akta Universiti dan Kolej Universiti, 1971, Kaedah-kaedah Universiti Teknologi Malaysia (Tatatertib Pelajar-pelajar), 1999.

SECTION A / *SEKSYEN A*

TRUE FALSE QUESTIONS / *SOALAN BETUL SALAH*

10 MARKS /*10 MARKAH*

Instruction: Answer all questions in answer space provided in page 4.
Arahan: Jawab semua soalan di ruangan jawapan yang disediakan di muka surat 4.

1	The unauthorized party can be a person, program, or a computing system. *Pihak yang tidak dibenarkan boleh menjadi orang, program atau sistem pengkomputeran.*	TRUE / FASE *BETUL / SALAH*
2	A malicious is a destruction of a hardware device but not software. *Berniat jahat ialah pemusnahan peranti perkakasan tetapi bukan perisian*	TRUE / FASE *BETUL / SALAH*
3	Alter a program to performs additional computation is an example for fabrication. *Mengubah atur cara untuk melakukan pengiraan tambahan ialah contoh untuk fabrikasi.*	TRUE / FASE *BETUL / SALAH*
4	Encryption is the process transforming an encrypted message into the original. *Penyulitan ialah proses mengubah mesej yang disulitkan kepada yang asal.*	TRUE / FASE *BETUL / SALAH*
5	Cryptographer is person who is responsible to invent or discovers encryption. *Kriptografi ialah orang yang bertanggungjawab untuk mencipta atau menemui penyulitan.*	TRUE / FASE *BETUL / SALAH*
6	Hash function also called checksum or message digest. *Fungsi hash juga dipanggil checksum atau ringkasan mesej.*	TRUE / FASE *BETUL / SALAH*
7	Encryption is a method to covert a text to a plain text into ciphertext. *Penyulitan ialah kaedah untuk menyembunyikan teks kepada teks biasa kepada teks sifir.*	TRUE / FASE *BETUL / SALAH*

8 Hash function is irreversible function that easy to use and easy to invert. TRUE / FASE
Fungsi hash ialah fungsi tidak boleh balik yang mudah digunakan dan mudah diterbalikkan. *BETUL / SALAH*

9 The output of MD5 is based on the original plain text length. Short message will generate short key. TRUE / FASE
Output MD5 adalah berdasarkan panjang teks biasa asal. Mesej ringkas akan menghasilkan kunci pendek. *BETUL / SALAH*

10 Fault is incorrect step, command or process in computer programs caused by human mistake. TRUE / FASE
Kesalahan ialah langkah, arahan atau proses yang salah dalam program komputer yang disebabkan oleh kesilapan manusia *BETUL / SALAH*

QUESTION NUMBER	ANSWER
1	
2	
3	
4	
5	
6	
7	
8	
9	
10	

SECTION B / *SEKSYEN B*

SUBJECTIVES QUESTIONS / *SOALAN SUBJEKTIF*

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. Encrypt following message using Ceaser cipher by following requirement:
Sulitkan mesej berikut menggunakan sifir Ceaser dengan keperluan berikut:

a. Message / *Mesej* = "MATTA" key = F [2 M]

b. Message/ *Mesej* = "KAKI" key= 5 [2 M]

c. Message / *Mesej* = "ALLY" key= G [2 M]

d. Explain **TWO (2)** the disadvantages of Ceaser cipher based on encryption on Q1(a-c).
*Terangkan **DUA (2)** keburukan asas sifir Ceaser pada penyulitan pada Q1(q-c).*

[4 M]

2. Explain **TWO (2)** advantages of the Cryptographic Hash Function implementation.
*Jelaskan **DUA (2)** kelebihan menggunakan pelaksanaan Fungsi Hash Kriptografi.* [4 M]

3. Explain type of attack for cryptoanalysis below and give an example situation for each attack.
Terangkan jenis serangan untuk analisis kripto di bawah dan berikan contoh situasi untuk setiap serangan. [6 M]

a) Passive attack / *serangan pasif* :

b) Active attack / *serangan aktif* :

c) Brute- force attack / *serangan kekerasan* :

4. Malware is a threat that can harm our device:
'Malware' adalah ancaman yang boleh memudaratkan peranti kita:

a. How Trojan and worm harm to our device? [4 M]
Bagaimana Trojan dan cecacing memberi mudarat kepada peranti kita?

b. Explain the **TWO (2)** malware effect to our computer [4 M]
*Terangkan **DUA (2)** kesan perisian jahat pada komputer.*

c. Suggest **TWO (2)** methods to avoid malware. [2 M]
*Cadangkan **DUA (2)** cara untuk mengelakan daripada 'malware'.*

5. Given p=23 and g=9, find the following key base on following requirement:
Diberi p=23 dan g=9, cari asas kunci berikut pada keperluan berikut:

a. If user A has private key $X_A = 7$, what is the public key Y_A?
Jika pengguna A mempunyai kunci persendirian $X_A = 7$, apakah kunci awam Y_A? [4 M]

b. If user B has private key $X_B = 3$, what is the public key Y_B?
Jika pengguna B mempunyai kunci persendirian $X_B = 3$, apakah kunci awam Y_B [4 M]

c. Find shared key.
Cari kunci yang dikongsi. [2 M]

6. Given p=3 and q= 7, solve following task using Rivest Shamir Adleman (RSA) method.
Diberi p=3 dan q= 7, selesaikan tugasan berikut menggunakan kaedah Rivest Shamir Adleman (RSA).

a. Find the value of n. [2 M]
Cari nilai n.

b. Find the value of φn. [3 M]
Cari nilai φn.

c. Find the public key (e). [3 M]
Cari kunci public.

d. Find private key (d). [5 M]
Cari kunci rahsia. (d).

e. Encrypt message = 13. [2 M]
Sulitkan mesej=13.

f. Decrypt your cipher text in question (e). [2 M]
Nyahsulitkan teks sifir di soalan (e).

g. List **THREE (3)** differences between Rivest Shamir Adlement Algorithm (RSA) compare to Diffie Hilman Algorithm (DHA). [3 M]
*Senaraikan **TIGA (3)** perbezaan antara Rivest Shamir Adlement Algorithm (RSA) berbanding Algoritma Diffie Hilman (DHA).*

SECTION C/ *SEKSYEN C*
ESSAY QUESTIONS / *SOALAN ESEI*
20 MARKS / *20 MARKAH*

Instruction: Answer all questions.
Arahan: Jawab semua soalan.

1. Lucas was assigned to be a network specialist for his company. He was responsible to secure his company from any network threat. Lucas should make sure his company network are safe to maintain data integrity.
Lucas telah ditugaskan untuk menjadi pakar rangkaian untuk syarikatnya. Dia bertanggungjawab untuk melindungi syarikatnya daripada sebarang ancaman rangkaian. Lucas harus memastikan rangkaian syarikatnya selamat untuk mengekalkan integriti data.

   a. What are the possibilities of threat that can harm data integrity in network?
   Apakah kemungkinan ancaman yang boleh membahayakan integriti data dalam rangkaian?
   [10 M]

b. Suggest precautions for Lucas to take as a network specialist for security requirement to ensure that his company's network security is secure and that data is only accessible to authorized user.

Cadangkan langkah berjaga-jaga untuk Lucas ambil sebagai pakar rangkaian sebagai keperluan keselamatan untuk memastikan rangkaian syarikatnya selamat dan data hanya boleh diakses oleh pengguna yang dibenarkan. [10 M]

- END OF QUESTIONS -

- SOALAN TAMAT -