UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER I – 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*	:	DECEMBER 2022 / JANUARY 2023 *DISEMBER 2022 / JANUARI 2023*

INSTRUCTION :
ARAHAN

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

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 11 pages including the cover
Kertas soalan ini mengandungi 11 muka surat termasuk kulit hadapan

UTM
UNIVERSITI TEKNOLOGI MALAYSIA

School of Professional and Continuing Education (SPACE)

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*

STRUCTURED QUESTIONS / *SOALAN STRUKTUR*

30 MARKS / *30 MARKAH*

Instruction: Answer all questions / *Arahan: Jawab semua soalan*

---

1. Cryptography means hidden writing. Define each terminology on cryptography below and give example for each terminology.
   Kriptografi bermaksud tulisan tersembunyi. Tentukan setiap istilah pada kriptografi di bawah dan berikan contoh untuk setiap istilah.

   a. Ciphertext / *Teks sifir*

   b. Cryptographer / *Kriptografi*

   c. Cryptanalyst / *Kriptoanalisis*

   d. Cryptosystem / *Sistem Kripto*

[8 M]

2. There are **FOUR** (4) cryptographic service. List and explain all services.
   *Terdapat **EMPAT (4)** perkhidmatan kriptografi. Senaraikan dan terangkan semua perkhidmatan.*

[8 M]

3. Explain and suggest a method or any software to avoid the situation of each malware below:
Terangkan dan cadangkan cara atau perisian untuk mengelakan setiap perisian perosak berikut

a. Logic bomb / *Bom Logik*

b. Trapdoor / *Perangkap pintu*

c. Worm / *Cecacing*

[6M]

4. Explain and give example for each threats in computer security.
Terangkan dan berikan contoh bagi setiap ancaman dalam keselamatan komputer.

a. Interruption / *Gangguan*

b. Interception / *Pemintasan*

c. Modification /*Pengubahsuaian*

d. Fabrication / *Fabrikasi*

[8 M]

SECTION B / *SEKSYEN B*

SUBJECTIVES QUESTIONS / *SOALAN SUBJEKTIF*

50 MARKS / *50 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 = "Programming" key = F [2 M]

   b. Message = "Fundamental" key= 5 [2 M]

c. Message = "Security" key= G [3 M]

2. List **THREE (3)** advantages of vernam cipher compare to Ceaser Cipher
*Senaraikan **TIGA (3)** kelebihan sifir vernam berbanding Ceaser sifir* [6 M]

3. List **THREE (3)** example that use the implementation of Cryptographic Hash Function.
*Senaraikan **TIGA (3)** contoh yang menggunakan pelaksanaan Fungsi Hash Kriptografi.*

[3 M]

4. Explain the differences between stream cipher and block cipher. You may visualize or use a table to described the differences.
   Terangkan perbezaan antara sifir strim dan sifir blok. Anda boleh memvisualisasikan atau menggunakan jadual untuk menerangkan perbezaan. [4 M]

5. Giving p=21 and g=9, find the following key base on following requirement:
   Dengan memberi p=21 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?

   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?

   c. Find shared key.
      Cari kunci yang dikongsi.

[10 M]

6. List **THREE (3)** advantages of Advanced Encrypt Standard (AES) Compare to Data Encryption Standard (DES).
*Senaraikan **TIGA (3)** kelebihan Advanced Encrypt Standards (AES) Bandingkan dengan Data Encryption Standard (DES).* [3 M]

7. Giving p=3 and q= 7, solve following task using Rivest Shamir Adleman (RSA) method.
Memberi 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.

e. Encrypt message = 11. [2 M]
Sulitkan mesej=11.

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

SECTION C/ *SEKSYEN C*

ESSAY QUESTIONS / *SOALAN ESEI*

20 MARKS / *20 MARKAH*

Instruction: Answer all questions.

Arahan: Jawab semua soalan.

---

1. Ahmad was assigned to be a data analyst for his company. He was responsible to secure his company from any damages. Ahmad should make sure his company data is protected in term of law and security.

   Ahmad ditugaskan menjadi penganalisis data bagi syarikatnya. Dia bertanggungjawab untuk melindungi syarikatnya daripada sebarang kerosakan. Ahmad harus memastikan data syarikatnya dilindungi dari segi undang-undang dan keselamatan

   a. Suggest security precaution that should be taken in each layer for OSI model internet protocol implemented.

      Cadangkan langkah berjaga-jaga keselamatan yang perlu diambil dalam setiap lapisan untuk protokol internet model OSI yang dilaksanakan. [7 M]

   b. Suggest a law action can be make for Ahmad to make sure his company data protected.

      Cadangkan tindakan undang-undang boleh dibuat untuk Ahmad bagi memastikan data syarikatnya dilindungi. [7 M]

c. Explain a method for Ahmad secure his data from physical and logical damages

Terangkan satu kaedah untuk Ahmad melindungi datanya daripada kerosakan fizikal dan logik [10 M]

- END OF QUESTIONS -

- SOALAN TAMAT -