



**FINAL EXAMINATION / PEPERIKSAAN AKHIR  
SEMESTER I – SESSION 2023 / 2024 / SEMESTER I – SESI 2023 / 2024  
PROGRAM KERJASAMA**

**COURSE CODE** : DDWD 3343  
*KOD KURSUS*

**COURSE NAME** : COMPUTER SECURITY /  
*NAMA KURSUS* *KESELAMATAN KOMPUTER*

**YEAR / PROGRAMME** : 3 / DDWD  
*TAHUN / PROGRAM*

**DURATION** : 2 HOURS 30 MINUTES  
*TEMPOH* *2 JAM 30 MINIT*

**DATE** : DECEMBER 2023 / JANUARY 2024  
*TARIKH* *DISEMBER 2023 / JANUARI 2024*

**INSTRUCTION** : **ANSWER ALL QUESTIONS IN THE QUESTION PAPER.**  
*ARAHAN* **JAWAB SEMUA SOALAN DALAM KERTAS 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* )

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

This examination paper consists of 10 pages including the cover  
*Kertas soalan ini mengandungi 10 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. In program security, there are various way of virus attached to the program. List and explain **THREE (3)** way of virus effect the program. [6M]

*Dalam keselamatan program, terdapat pelbagai cara virus melekat pada program. Senaraikan dan terangkan **TIGA (3)** cara virus memberi kesan kepada program.*

2. There are **FOUR (4)** cryptographic service. List and explain all services. [8M]

*Terdapat **EMPAT (4)** perkhidmatan kriptografi. Senaraikan dan terangkan semua perkhidmatan.*



**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. Windows and Linux are the example of an Operating System (OS). What is OS and list **THREE (3)** OS available nowadays. [5 M]  
*Windows dan Linux adalah contoh Sistem Operasi (OS). Apakah itu OS dan senaraikan TIGA (3) OS yang tersedia pada masa kini.*
  
2. List and explain **THREE (3)** types of firewalls. [6 M]  
*Senaraikan dan jelaskan TIGA (3) jenis tembok api*
  
3. List **THREE (3)** example that use the implementation of Cryptographic Hash Function. [3 M]  
*Senaraikan TIGA (3) contoh yang menggunakan pelaksanaan Fungsi Hash Kriptografi.*

4. Explain the **TWO (2)** advantages using anti-virus. [2 M]

*Terangkan DUA(2) kelebihan menggunakan anti-virus.*

5. Explain the **TWO (2)** malware effect to our computer [2 M]

*Terangkan DUA(2) kesan perissian jahat pada komputer.*

6. Giving  $p=21$  and  $g=9$ , find the following key base on following requirement: [10 M]

*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.*

7. 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]

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

*Memberi  $p=3$  dan  $q=7$ , selesaikan tugas berikut menggunakan kaedah Rivest Shamir Adleman (RSA).*

- a. What is a differences between RSA and Diffie Hilamn Algorithm? [2 M]

*Apakah perbezaan antara RSA dan Algotirma Diffie Hilman?*

- b. Find the value of  $n$ . [2 M]

*Cari nilai  $n$ .*

- c. Find the value of  $\phi n$ . [3 M]

*Cari nilai  $\phi n$ .*

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

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

f. Encrypt message = 11. [2 M]  
*Sulitkan mesej=11.*

g. 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.* [6 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* [7 M]

**- END OF QUESTIONS -**  
**- SOALAN TAMAT -**