UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (SPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER II – SESSION 2018 / 2019
PROGRAM KERJASAMA

COURSE CODE / *KOD KURSUS* : DDWC 3343 WC

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

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

DURATION / *TEMPOH* : 2 HOURS 30 MINUTES

DATE / *TARIKH* : APRIL 2019

INSTRUCTION/*ARAHAN* :

Answer **ALL** questions in the spaces provided in this question paper.

*Jawab **SEMUA** soalan di ruang yang disediakan dalam kertas soalan ini.*

(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*	:	.....
I.C NO. / *NO. K/PENGENALAN*	:	.....
YEAR / COURSE *TAHUN / KURSUS*	:	.....
COLLEGE *KOLEJ*	:	.....
LECTURER'S NAME *NAMA PENSYARAH*	:	.....

This examination paper consists of ...18... pages including the cover
Kertas soalan ini mengandungi .....18..... muka surat termasuk kulit hadapan

PUSAT PROGRAM 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 Peperiksaan melainkan dengan kebenaran Ketua Pengawas; atau

1.1.2 menggunakan makluman yang diperolehi 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 2.1.2 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 / *BAHAGIAN A*
24 MARKS / *24 MARKS*

MULTIPLE CHOICES / *ANEKA PILIHAN*

Choose the most appropriate answer. Answer in the table provided on page 8.
Pilih satu jawapan yang paling tepat. Jawab pada jadual yang disediakan pada mukasurat 8.

1. Computer security is generally considered to be the responsibility of _____.
Keselamatan komputer secara umumnya dianggap sebagai tanggungjawab _____.

   A. everyone in the organization. / *semua orang dalam organisasi*
   B. corporate management. / *pengurusan korporat.*
   C. the corporate security staff. / *kakitangan keselamatan korporat.*
   D. everyone with computer access. / *semua orang dengan capaian komputer.*

2. A system security engineer is evaluating methods to store user passwords in an information system, what may be the best method to store user passwords and meeting the confidentiality security objective?

   Jurutera keselamatan sistem sedang menilai kaedah untuk menyimpan kata laluan pengguna dalam sistem maklumat, apa yang boleh menjadi kaedah terbaik untuk menyimpan kata laluan pengguna dan memenuhi objektif keselamatan kerahsiaan?

   A. Password-protected file / *Fail yang dilindungi dengan kata laluan*
   B. File restricted to one individual / *Fail terhad kepada seorang individu*
   C. One-way encrypted file / *Fail yang dienkrip satu hala*
   D. Two-way encrypted file / *Fail yand dienkrip dua hala*

3. What is meant by the term **'cyber-crime'**?
*Apa yang dimaksudkan dengan istilah **'jenayah siber'**?*

   A. Any crime that uses computers to jeopardise or attempt to jeopardise national security
   Apa-apa jenayah yang menggunakan komputer untuk menggugat atau cubaan untuk menggugat keselamatan negara

   B. The use of computer networks to commit financial or identity fraud
   Penggunaan rangkaian komputer untuk melakukan perbuatan keji yang kewangan atau penipuan identiti

   C. The theft of digital information
   Kecurian maklumat digital

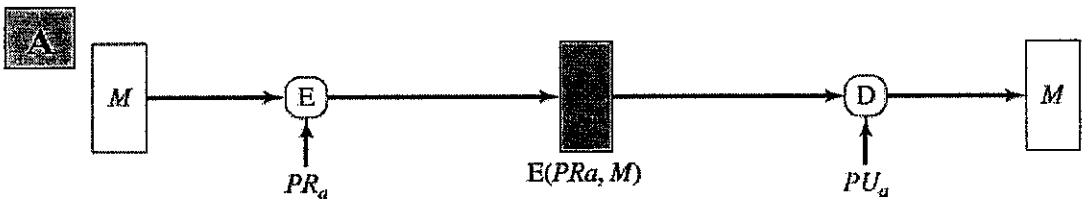
   D. Any crime that involves computers and networks
   Apa-apa jenayah yang melibatkan komputer dan rangkaian

4. Which of the followings is an example of simple substitution algorithm?
Manakah di antara berikut adalah contoh algoritma penggantian mudah?

A. Rivest, Shamir, Adleman (RSA)
B. Data Encryption Standard (DES)
C. Caesar cipher
D. Blowfish

5. Refer to the diagram below. Suppose A would like to send a message, **M**. **E** and **D** are the encryption and decryption algorithms. A's private key and A's public key are denoted $\mathbf{PR_a}$ and $\mathbf{PU_a}$ respectively.

*Rujuk kepada gambarajah di bawah. Katakan A ingin menghantar mesej, **M**. **E** dan **D** adalah algoritma enkripsi dan dekripsi. dekripsi Kunci peribadi, A dan kunci awam, A adalah ditandakan dengan $\mathbf{PR_a}$ dan $\mathbf{PU_a}$.*



The above diagram implements:
Gambarajah di atas melaksanakan:

A. Authentication only. / *Hanya Pengesahan*
B. Signature and Confidentiality. / *Tandatangan dan Kerahsiaan*
C. Authentication and Signature. / *Pengesahan dan Tandatangan*
D. Authentication, Signature and Confidentiality. / *Pengesahan, Tandatangan dan Kerahsiaan*

6. If Ramsey encrypts the message using Ozil's public key, this is to achieve _____ .
Jika Ramsey mengenkrip mesej dengan kunci umum Ozil, ini untuk mencapai _____.

A. confidentiality / *kerahsiaan*
B. availability / *ketersediaan*
C. authentication / *pengesahan*
D. integrity / *keutuhan*

7. The following are threats that could affect the confidentiality of message in the network **EXCEPT**
*Berikut merupakan ancaman yang menjejaskan kerahsiaan mesej dalam rangkaian **KECUALI***

A. cookie / *'cookie'*
B. traffic flow analysis / *analisis aliran trafik*
C. DNS attack / *serangan DNS*
D. misdelivery / *penghantaran silap*

8. Databases are very challenging from a security perspective. One of the more risky vulnerabilities is inference. How can inference be explained?
Pangkalan data adalah sangat mencabar dari perspektif Keselamatan. Salah satu kelemahan lebih berisiko adalah inferen. Bagaimana inferen dapat dijelaskan?

A. Corruption of data integrity by input data errors or erroneous processing.
Kerosakan keutuhan data disebabkan ralat pada data masuk atau pemprosesan yang salah.

B. Running processes at the same time, thus forming the risk of inconsistency.
Menjalankan proses-proses pada masa yang sama, maka risiko percanggahan terbentuk.

C. By passing security controls at the front end, in order to access information which is not authorized.
Memintas kawalan keselamatan pada bahagian hadapan untuk mengakses maklumat yang tidak dibenarkan.

D. Deducing sensitive information from available information.
Menyimpul maklumat sensitif daripada maklumat yang tersedia.

9. In Information Security a **"Trojan Horse"** refers to a _____.
*Dalam Keselamatan Maklumat **"Kuda Trojan"** merujuk kepada _____.*

A. a useful, or apparently useful, program or command procedure but with hidden (malicious) side-effects
aturcara atau arahan prosedur yang berguna, atau nampaknya berguna, tetapi kesan-kesan sampingan tersembunyi (berniat jahat)

B. a computer virus
satu virus komputer

C. program that sends large volumes of unwanted e-mail
aturcara yang menghantar sebilangan besar e-mel yang tidak diingini

D. a secret entry point into a program
satu pintu rahsia untuk masuk ke dalam program

10. What is the main purpose of access control?
Apakah tujuan utama kawalan capaian?

A. to authorize full access to authorized users
untuk membenarkan akses penuh kepada pengguna yang diberi kuasa

B. to limit the actions or operations that a legitimate user can perform
untuk menghadkan tindakan atau operasi yang pengguna sah boleh lakukan

C. to stop unauthorised users accessing resources
untuk menghalang pengguna yang tidak dibenarkan mencapai sumber

D. to protect computers from viral infections
untuk melindungi komputer daripada jangkitan virus

11. In Message Integrity, SHA-I hash algorithms create an **N**-bit message digest out of _____ message.
*Dalam keutuhan mesej, algoritma cincangan SHA-I menghasilkan suatu digest mesej **N**-bit daripada _____ mesej.*

A. 1024 Bit Blocks / *1024 bit blok*
B. 512 Bit Blocks / *512 bit blok*
C. 256 Bit Blocks / *256 bit blok*
D. 128 Bit Blocks / *128 bit blok*

12. In digital certificate, under what circumstance might a certification authority (CA) revoke a certificate?
Dalam sijil digital, dalam keadaan apakah autoriti pensijilan (CA) kemungkinan membatalkan sesuatu sijil?

A. The certificate owner has not utilized the certificate for an extended period.
Pemilik sijil tidak menggunakan sijil untuk satu tempoh.

B. The certificate owner public key has been compromised.
Kunci umum pemilik sijil telah dikompromi.

C. The certificate owner' private key has been compromised.
Kunci peribadi pemilik sijil telah terjejas.

D. The certificate owner has upgraded his/her web browser.
Pemilik sijil telah tingkatkan pelayar webnya.

13. Prior to installation of an intrusion prevention system (IPS), a network engineer would place a packet sniffer on the network, what is the purpose for using a packet sniffer?
Sebelum pemasangan sistem pencegahan pencerobohan (IPS), seorang jurutera rangkaian akan meletakkan sniffer paket pada rangkaian. Apakah tujuan menggunakan sniffer paket?

A. *It tracks network connections.*
Ia mengesan sambungan rangkaian.
B. It monitors network traffic.
Ia memantau trafik rangkaian.
C. It scans network segments for cabling faults.
Ia mengimbas segmen rangkaian untuk kesilapan perkabelan.
D. It detects illegal packets on the network.
Ia mengesan paket-paket yang menyalahi undang-undang di dalam rangkaian.

14. Physical security is accomplished through proper facility construction, fire and water protection, anti-theft mechanisms, intrusion detection systems, and security procedures that are adhered to and enforced. Which of the following is **NOT** a component that achieves this type of security?
*Keselamatan fizikal dicapai menerusi pembinaan kemudahan yang betul, perlindungan kebakaran dan air, mekanisme anti-kecurian, sistem pengesanan pencerobohan dan prosedur keselamatan yang dipatuhi dan dikuatkuasakan. Manakah di antara berikut **BUKAN** komponen yang mencapai keselamatan jenis ini?*

A. Technical control mechanisms.
Mekanisma kawalan teknikal.

B. Administrative control mechanisms.
Mekanisma kawalan pentadbiran.

C. Physical control mechanisms
Mekanisma kawalan fizikal.

D. Integrity control mechanisms
Mekanisma kawalan keutuhan.

15. A security policy provides a way to _____.
Polisi keselamatan menyediakan satu cara untuk _____.

A. establish a cost model for security activities
mengisytiharkan satu model kos untuk aktiviti keselamatan

B. allow management to define system recovery requirements
membenarkan pihak pengurusan mentakrif keperluan sistem baikpulih

C. identify and clarify security goals and objectives
mengenalpasti dan menjelaskan matlamat dan objektif keselamatan

D. enable management to define system access rules
membenarkan pengurusan menjelaskan peraturan sistem pencapaian

16. Copyright provides what form of protection?
Apakah bentuk perlindungan yang diberi oleh hak cipta?

A. Protects an author's right to distribute his/her works.
Melindungi hak seorang pengarang untuk mengedar karya beliau

B. Protects information that provides a competitive advantage.
Melindungi maklumat yang menyediakan satu kelebihan daya saing.

C. Protects the right of an author to prevent unauthorized use of his/her works.
Melindungi hak seorang pengarang untuk menghalang penggunaan tanpa kebenaran kerja-kerja beliau.

D. Protects the right of an author to prevent viewing of his/her works.
Melindungi hak seorang pengarang untuk menghalang melihat kerja-kerja beliau.

ANSWER SPACE FOR SECTION A /24 MARKS

RUANG JAWAPAN BAGI BAHAGIAN A /24 MARKAH

1		5		9		13	
2		6		10		14	
3		7		11		15	
4		8		12		16	

SECTION B / *BAHAGIAN B*
76 MARKS / *76 MARKAH*

ANSWER ALL QUESTIONS.ANSWER IN THE SPACES PROVIDED
JAWAB SEMUA SOALAN. JAWAB PADA RUANG YANG DISEDIAKAN.

Q1. a) For the cybercrimes below, indicate whether the crime is an attack on **data integrity, system integrity, data confidentiality, privacy** or **availability.** **[3 M]**
Untuk jenayah siber di bawah, nyatakan sama ada jenayah itu adalah serangan terhadap ***integriti data, integriti sistem, kerahsiaan data, privasi*** *atau* ***ketersediaan.***

i. Offering or making available of child pornography through a computer system.
Menawarkan atau sediakan pornografi kanak-kanak menerusi sistem komputer.

_____

ii. Infringements of copyright and related rights
Perlanggaran hak cipta dan yang berkaitan dengannya

_____

iii. Damaging, deletion, deterioration, alteration or suppression of data without right.
Merosakkan, penghapusan, memerosotkan, pindaan atau penindasan data tanpa hak.

_____

b) Determine the types of viruses to the definitions given: **[4 M]**
Tentukan jenis virus dengan definisi yang diberi:

i. Corrupts or replaces instructions in the boot sector, preventing the OS from loading properly thus stopping the computer from powering up.
Merosakkan atau menggantikan arahan dalam sektor but, menghalang OS daripada dimuatkan dengan sempurna lalu menghalang komputer ini daripada sandaran.

_____

ii. Infects program files
Menjangkiti fail aturcara

_____

iii. Replicates itself without limit to exhaust resource in the computer.
Mengulangi diri tanpa had untuk menggunakan sumber dalam komputer sepenuhnya,

_____

iv. Comes as an attachment to an e-mail or as the e-mail itself.
Datang sebagai lampiran kepada e-mel atau e-mel itu sendiri.

_____

Q2. a) Explain the difference between stream cipher and block ciphers. **[3 M]**

Terangkan perbezaan antara kod rahsia rentetan dan kod rahsia blok.

b) Given **p=17**, **q = 11**, and the decryption key, **d = 23**. Find **e** and encrypt the message, **EXAM**.
Note: Use integer value for A=1, B=2, C=3, D=4, ..., Z= 26 **[6 M]**

*Diberi **p=17**, **q = 11**, dan kunci dekripsi, **d = 23**. Cari **e** dan enkrip mesej, **EXAM**.*
Nota: Use integer value for A=1, B=2, C=3, D=4, ..., Z= 26.

c) Refer Figure 1 below. It shows steps involved in the S-box substitution and P-Box permutation in one DES cycle. It uses 8 S-boxes and a P-Box to produce 32-bits output. Input of each S-box is 6-bit and the output is 4-bit. Suppose the 48-bits data is **10001111 01010001 00011110 10100010 00111101 01000110** and the 48-bit key,K in hexadecimal value is **123456789ABCh**. Determine the 32-bit output of the P-box. Give your answer in hexadecimal representation.
(Note: Refer to **Appendix A** for S-box and P-box) **[8 M]**

*Rujuk Rajah 1 di bawah. Ia menunjukkan langkah-langkah yang terlibat dalam proses penyelitan kotak-S dan pemutasi kotak-P dalam satu kitaran DES. Ia menggunakan 8 kotak-S dan satu kotak-P untuk menghasilkan 32-bit output. Input untuk setiap satu kotak-S adalah 6-bit dan outputnya adalah 4-bit. Andaikan 48-bit data adalah **10001111 01010001 00011110 10100010 00111101 01000110** dan 48-bit kunci,K dalam heksadesimal adalah **123456789ABCh**. Tentukan output 32-bit bagi kotak-P. Berikan jawapan anda dalam nilai kelsadesiml.*

*(Nota: rujuk **Lampiran A** untuk kotak-S dan kotak-P)*

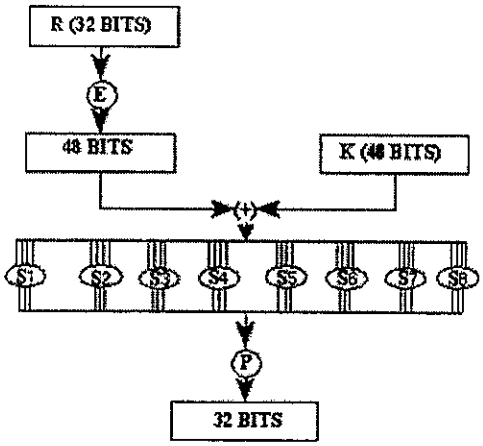


Figure 1 : S-Box Substitution and P-box Straight Permutation

Rajah 1: Penyelitan Kotak S- dan Permutasi lurus Kotak-P

Answer

Step1: Substitution with the Key

Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35	36	37	38	39	40	41	42	43	44	45	46	47	48
48-bit Data	1	0	0	0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	1	0	1	0	0	0	1	0	0	0	1	1	1	1	0	1	0	1	0	0	0	1	1	0
Key	0	0	0	1	0	0	1	0	0	0	1	1	0	1	0	0	0	1	0	1	0	1	1	0	0	1	1	1	1	0	0	0	1	0	0	1	1	0	1	0	1	0	1	1	1	1	0	0
⊕ =																																															

Step 2: S-Box Substitution

Box	S1	S2	S3	S4	S5	S6	S7	S8
Row								
Column								
Value in Decimal								
Value in Binary								

Result of S-Boxes Substitution / *Hasil Penggantian Kotak-S*

_____

Step 3 : Result of P-Box Substitution / *Hasil Pengantian Kotak-P*

Bit	1	2	3	4	5	6	7	8
Bit	9	10	11	12	13	14	15	16
Bit	17	18	19	20	21	22	23	24
Bit	25	26	27	28	29	30	31	32

⇨ Equivalent Hex Value/ *Nilai Hex Setara:*

_____

Q3. Answer the questions below regarding key generation in **Diffie-Hellman** and **RSA**.
*Jawab soalan berikut mengenai penjanaan kunci dalam **Diffie-Hellman** and **RSA***

a) One method of key management is the use of **Diffie-Hellman** algorithm. Suppose the Diffie-Hellman public values **p** and **g** are **7** and **4**, respectively. If user A choose private key $\mathbf{X_A} = 4$.
*Satu kaedah pengurusan kunci adalah penggunaan algoritma **Diffie-Hellman** Katakan nilai umum bagi Diffie-Hellman **p** dan **g** adalah masing-masing **7** dan **4**. Jika pengguna A memilih kunci peribadi $\boldsymbol{X_A} = 4$.*

i. What is A's public key $\mathbf{Y_A}$? **[2 M]**
Apakah kunci umum pengguna A, $\boldsymbol{Y_A}$?

ii. If user B has private key $\mathbf{X_B} = \mathbf{3}$, what is B's public key $\mathbf{Y_B}$? **[2 M]**
Jika pengguna B mempunyai kunci peribadi $\boldsymbol{X_B} = \boldsymbol{3}$, apakah kunci umum B, $\boldsymbol{Y_B}$?

iii. What is the shared key? **[1 M]**
Apakah kunci yang dikongsi?

b) Suppose that you are computing an RSA key pair. What are **p** and **q** and **φ(n)** for an **n = 51**? Find the RSA public key pair for this **p** and **q**. **[4 M]**
*Andaikan bahawa anda mengira satu pasangan kunci RSA. Apakah **p** dan **q** dan **φ(n)** untuk untuk n = 51? Cari kunci umum RSA dari pasangan **p** dan **q** ini.*

Q4. Figure 2 below shows the application of public-key encryption. It illustrates how Ali creates digital envelope when sending confidential message to Siti.

Rajah 2 di bawah menunjukkan penggunaan penyulitan kekunci awam. Ia menggambarkan bagaimana Ali mencipta sampul surat digital semasa menghantar mesej rahsia kepada Siti.

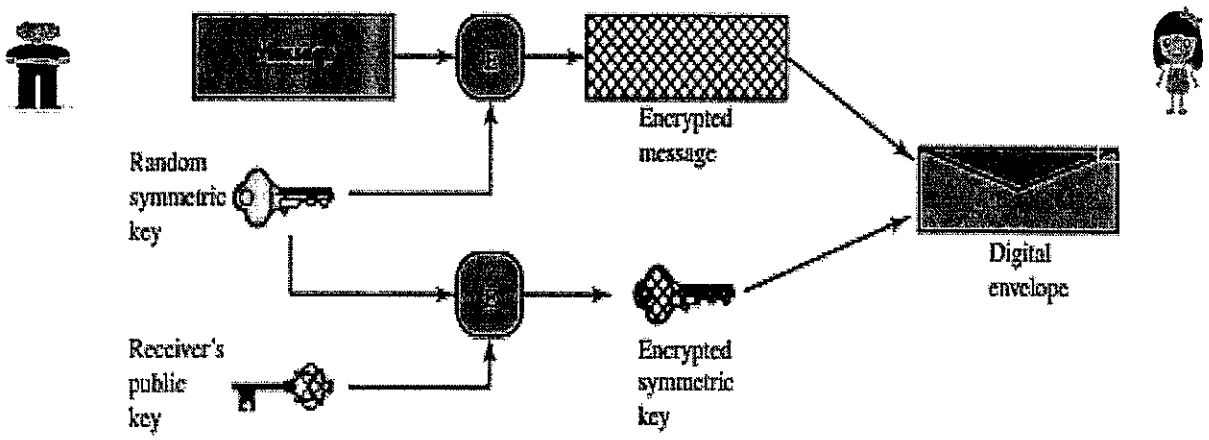


Figure 2. Creation of Digital Envelope
Rajah 2: Pembentukan Sampul Digital

a) What is the purpose of the digital envelop? **[2 M]**
Apakah kegunaan sampul surat digital?

b) Show the opening of the digital envelop by Siti. **[4 M]**
Tunjukkan bagaimana pembukaan sampul surat digital oleh Siti.

c) Modify Figure 2 above that will include a digital signature to authenticate the message in the digital envelop. **[4 M]**

Ubah Rajah 2 di atas yang akan memasukkan tandatangan digital untuk mengesahkan mesej di dalam sampul surat digital.

Q5. a) Describe briefly the **three (3)** main concerns with the use of passwords for authentication.
*Terangkan dengan ringkas **tiga (3)** kebimbangan utama dalam penggunaan katalaluan dalam pengesahan.* **[3 M]**

b) Explain what is meant by a social engineering attack on a password. **[2 M]**

Terangkan apa yang dimaksudkan dengan serangan kejuruteraan sosial terhadap katalaluan.

c) You subscribe to a number of free IT magazines. Among the questions you were asked in order to activate your subscriptions are: one magazine asked for your month of birth, a second asked for your year of birth, and a third asked for your mother's maiden name. What do you think is going on here? Do you think this is an example of social engineering attack on your personal data? **[4 M]**

Anda melanggan sejumlah majalah IT secara percuma. Antara soalan-soalan yang anda diminta untuk mengaktifkan langganan anda adalah: satu majalah meminta tentang bulan kelahiran anda, kedua meminta tahun kelahiran, dan ketiga meminta nama ibu anda. Apakah yang sedang berlaku di sini? Adakah anda fikir ini adalah satu contoh serangan kejuruteraan sosial terhadap maklumat peribadi anda?

Q6. a) Your company is trying to determine the type of IDS to implement. As an IT security manager of the company, write a brief comparison of host-based and network-based intrusion detection systems. Include one advantage and disadvantage of each. **[4 M]**

Syarikat anda sedang cuba untuk menentukan jenis IDS untuk dilaksanakan. Sebagai pengurus keselamatan IT di syarikat, tulis dengan ringkas satu perbandingan antara sistem pengesanan pencerobohan "host-based" dan "network-based". Sertakan satu kebaikan dan kelemahan bagi setiap satu jenis IDS.

b) For the following statements regarding firewalls, answer True / False. **[3 M]**
Untuk pernyataan mengenai tembok api berikut, jawab Benar / Salah.

i. Primary function of a firewall is to enforce security between user and the Internet. _____
Fungsi utama tembok api adalah untuk menguatkuasakan keselamatan antara pengguna dan Internet.

ii. Network layer firewall works as a packet filter. _____
Tembok api lapisan rangkaian bertugas sebagai penapis paket.

iii. A proxy firewall filters at data link layer. _____
Tembok api proksi menapis pada lapisan pautan data.

c) For the vulnerabilities that can affect **confidentiality** in a computer network listed in a table below, determine **one (1)** control that can be used to overcome the problem.
*Untuk kelemahan yang boleh menjejaskan kerahsian dalam sesuatu rangkaian yang disenaraikan dalam jadual di bawah, tentukan **satu (1)** langkah kawalan yang boleh digunakan untuk mengatasi masalah yang dihadapi.* **[3 M]**

Vulnerabilities / *Kelemahan*	Controls / *Kawalan*
Passive Wiretapping / *Curi Talian Pasif*	
Cookie / *'Cookie'*	
Protocol flaw / *Kecacatan protokol*	

Q7. a) The following are among the database system security requirements. For each requirement listed, give reason why they are needed for the security of the database. **[4 M]**

Berikut adalah antara keperluan keselamatan bagi sistem pangkalan data. Untuk setiap keperluan yang disenaraikan, berikan sebab mengapa ia diperlukan untuk keselamatan pangkalan data.

i. Physical database integrity / *Keutuhan fizikal pangkala data*: _____

_____

ii. Element integrity / *Keutuhan elemen*:_____

_____

b) List and briefly explain **three (3)** methods provided in most DBMS that can be used to maintain the integrity of the database elements. **[6 M]**

*Senarai dan terangkan dengan ringkas **tiga (3)** kaedah yang disediakan dalam kebanyakan DBMS yang boleh digunakan untuk mengekalkan keutuhan bagi elemen pangkalan data.*

c) Protection of the memory space is crucial especially in multiprogramming operating system. What is meant by protection of the memory? Give **two (2)** methods provided by the operating system to protect the memory. **[4 M]**

*Perlindungan ruang memori adalah penting terutamanya dalam sistem operasi berbilang aturcara. Apa yang dimaksudkan dengan perlindungan memori? Berikan **dua (2)** kaedah-kaedah yang disediakan oleh sistem pengendalian untuk melindungi kad memori.*

APPENDIX A

Table 1: S-Boxes of DES

Box	Row	Column 0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
S_1	0	14	4	13	1	2	15	11	8	3	10	6	12	5	9	0	7
	1	0	15	7	4	14	2	13	1	10	6	12	11	9	5	3	8
	2	4	1	14	8	13	6	2	11	15	12	9	7	3	10	5	0
	3	15	12	8	2	4	9	1	7	5	11	3	14	10	0	6	13
S_2	0	15	1	8	14	6	11	3	4	9	7	2	13	12	0	5	10
	1	3	13	4	7	15	2	8	14	12	0	1	10	6	9	11	5
	2	0	14	7	11	10	4	13	1	5	8	12	6	9	3	2	15
	3	13	8	10	1	3	15	4	2	11	6	7	12	0	5	14	9
S_3	0	10	0	9	14	6	3	15	5	1	13	12	7	11	4	2	8
	1	13	7	0	9	3	4	6	10	2	8	5	14	12	11	15	1
	2	13	6	4	9	8	15	3	0	11	1	2	12	5	10	14	7
	3	1	10	13	0	6	9	8	7	4	15	14	3	11	5	2	12
S_4	0	7	13	14	3	0	6	9	10	1	2	8	5	11	12	4	15
	1	13	8	11	5	6	15	0	3	4	7	2	12	1	10	14	9
	2	10	6	9	0	12	11	7	13	15	1	3	14	5	2	8	4
	3	3	15	0	6	10	1	13	8	9	4	5	11	12	7	2	14
S_5	0	2	12	4	1	7	10	11	6	8	5	3	15	13	0	14	9
	1	14	11	2	12	4	7	13	1	5	0	15	10	3	9	8	6
	2	4	2	1	11	10	13	7	8	15	9	12	5	6	3	0	14
	3	11	8	12	7	1	14	2	13	6	15	0	9	10	4	5	3
S_6	0	12	1	10	15	9	2	6	8	0	13	3	4	14	7	5	11
	1	10	15	4	2	7	12	9	5	6	1	13	14	0	11	3	8
	2	9	14	15	5	2	8	12	3	7	0	4	10	1	13	11	6
	3	4	3	2	12	9	5	15	10	11	14	1	7	6	0	8	13
S_7	0	4	11	2	14	15	0	8	13	3	12	9	7	5	10	6	1
	1	13	0	11	7	4	9	1	10	14	3	5	12	2	15	8	6
	2	1	4	11	13	12	3	7	14	10	15	6	8	0	5	9	2
	3	6	11	13	8	1	4	10	7	9	5	0	15	14	2	3	12
S_8	0	13	2	8	4	6	15	11	1	10	9	3	14	5	0	12	7
	1	1	15	13	8	10	3	7	4	12	5	6	11	0	14	9	2
	2	7	11	4	1	9	12	14	2	0	6	10	13	15	3	5	8
	3	2	1	14	7	4	10	8	13	15	12	9	0	3	5	6	11

Table 2: Permutation Box P

Bit	Goes to Position							
1-8	9	17	23	31	13	28	2	18
9-16	24	16	30	6	26	20	10	1
17-24	8	14	25	3	4	29	11	19
25-32	32	12	22	7	5	27	15	21

END OF QUESTIONS/ *SOALAN TAMAT*

Mukasurat ini sengaja dibiarkan kosong

[This page is purposely left blank]

Mukasurat ini sengaja dibiarkan kosong

[This page is purposely left blank]