UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (UTMSPACE)

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

COURSE CODE *KOD KURSUS*	:	DDWC 3343
COURSE NAME *NAMA KURSUS*	:	COMPUTER SECURITY / *KESELAMATAN KOMPUTER*
YEAR / PROGRAMME *TAHUN / PROGRAM*	:	3 DDWC
DURATION *TEMPOH*	:	2 HOURS 30 MINUTES
DATE *TARIKH*	:	NOVEMBER 2018

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 ...19... pages including the cover
Kertas soalan ini mengandungi .....19..... 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. Write your answer in the table provided on page 8.
Pilih satu jawapan yang paling tepat. Tulis jawapan pada jadual yang disediakan pada mukasurat 8.

1. 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 melibatkan 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.

2. 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 inferens. Bagaimana inferens dapat dijelaskan?

   A. Corruption of data integrity by input data errors or erroneous processing.
   Kerosakan integriti data disebabkan oleh ralat pada yang 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. Bypassing 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.

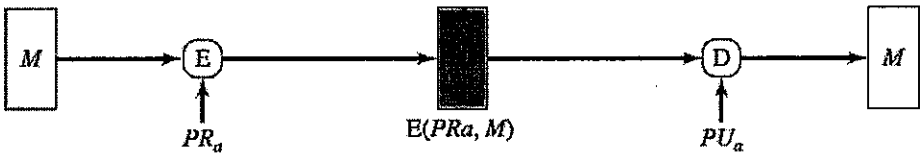
3. Social engineering is one of the most successful attack methods of cybercriminals. What is regarded as a form of social engineering?
Kejuruteraan sosial adalah salah satu kaedah serangan yang paling berjaya daripada jenayah siber. Apa yang dianggap sebagai satu bentuk kejuruteraan sosial?

A. Cryptoware / *Perisian Kripto*
B. Denial of Service (DOS) attack / *Serangan Penafian Perkhidmatan (DOS)*
C. Phishing / *Pemalsuan*
D. Spam / *Spam*

4. An organization is not willing to share any resources. Which deployment model in Cloud Computing represents the most secure one?
Organisasi ini tidak bersedia untuk berkongsi apa-apa sumber. Penggunaan model mana dalam Pengkomputeran Awan merupakan yang paling selamat?

A. Community cloud / *Awan Komuniti*
B. Hybrid cloud / *Awan Hibrid*
C. Private cloud / *Awan Peribadi*
D. Public cloud / *Awan Awam*

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* $\boldsymbol{PR_a}$ *dan* $\boldsymbol{PU_a}$.



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. 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

7. We use a cryptography method in which the plaintext AAAAAA becomes ciphertext FFFFFF. This method is probably _____.
Kita menggunakan kaedah kriptografi yang mana teks asal AAAAAA menjadi teks rahsia FFFFFF. Kaedah ini mungkin adalah _____.

A. monoalphabetic substitution cipher / *tulisan rahsia penggantian satu abjad*
B. polyalphabetic substitution cipher / *tulisan rahsia penggantian berbilang-abjad*
C. transposition cipher / *tulisan rahsia penyusunan*
D. none of the above / *tiada satu pun jawapan di atas*

8. The following are network vulnerabilities that could be used to gain information before attacking the network **EXCEPT**
Berikut merupakan kelemahan rangkaian yang boleh digunakan untuk mendapat malumat sebelum menyerang rangkaian ***KECUALI***

A. port scan / *pengimbas port*
B. traffic flow analysis / *analisis aliran trafik*
C. reconnaissance / *tinjauan*
D. social engineering / *kejuruteraan sosial*

9. When a communication link is subjected to monitoring, what is the advantage for using an end-to-end encryption solution over link encryption?
Apabila pautan komunikasi perlu pengawasan, apakah kebaikan menggunakan enkipsi hujung-ke-hujung berbanding enkripsi pautan?

A. Cleartext is only available to the sending and receiving entities.
Teks biasa hanya tersedia kepada pihak penghantar dan penerima.
B. Routing information is included in the message transmission protocol.
Maklumat penghalaan terangkum dalam protokol penghantaran mesej.
C. Routing information is encrypted by the originator.
Maklumat penghalaan dienkrip oleh pihak penghantar asal.
D. Each message has a unique encryption key.
Setiap satu mesej ada kunci enkripsi yang unik

10. If Ramsey encrypts the message using his private key, this is to achieve _____ .
Jika Ramsey mengenkrip mesej dengan kunci peribadinya, ini untuk mencapai _____.

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

11. 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*

12. Putting guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters. This is _____,
Menempatkan pengawal di pintu masuk, membuat salinan "backup" bagi perisian dan data penting, perancangan tapak fizikal yang mengurangkan risiko akibat bencana alam. Ini adalah _____.

A. software controls / *kawalan perisian*
B. physical controls / *kawalan fizikal*
C. hardware controls / *kawalan perkakasan*
D. both software and hardware controls / *kedua-dua kawalan perisian dan perkakasan*

13. After running the key-gen, system performance is extremely slow and numerous antivirus alerts are displayed. Which of the following **BEST** describes this type of malware?
*Pengguna memuat turun key-gen untuk memasang perisian cetak rompak. Selepas melarikan key-gen, prestasi sistem adalah sangat perlahan dan banyak amaran antivirus dipaparkan. Mana antara berikut yang **TERBAIK** yang menerangkan perisian berniat jahat ini?*

A. Logic bomb / *Bom logik*
B. Worm / *Cacing*
C. Trojan Horse / *Kuda Trojan*
D. Adware / *'Adware'*

14. 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*

15. 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.

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 /24MARKAH

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. Match the appropriate terms with the explanation given below: [6 M]
Padankan istilah yang sesuai dengan penerangan yang diberikan di bawah:

Data Integrity *Keutuhan Data*	Rabbit	Trojan Horse *Kekuda Trojan*	Man-in-the Middle attack *Serangan Orang di Tengah*
Digital Signature *Tandatangan Digit*	Virus Signature *Tandatangan Virus*	Covert Channel *Saluran Terselindung*	Data Confidentiality *Kerahsian Data*

a) Communications between two users is monitored and modified by an unauthorized party.
Komunikasi antara dua pengguna dipantau dan diubahsuai oleh pihak yang tidak dibenarkan.

_____

b) Patterns yield by the virus after it has executed and affected the program.
Corak yang dikeluarkan atau dijana oleh virus selepas ia melaksanakan dan menjejas aturcara.

_____

c) Software that enables a user to obtain secret information about another's computer activities by transmitting data covertly from their hard drive
Perisian yang membolehkan pengguna untuk mendapatkan maklumat rahsia mengenai aktiviti komputer lain dengan memindah data secara berselindung dari cakera keras komputer itu.

_____

d) This kind of virus replicates itself without limit to exhaust resources.
Virus jenis ini membiak tanpa batas bertujuan untuk menghabiskan sumber yang diserang.

_____

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

_____

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

_____

Q2. a) Explain the difference between stream ciphers and block ciphers. **[3 M]**
Terangkan perbezaan di antara 'stream cipher' dan 'block cipher'.

b) Give **one [1]** advantage and **one [1]** disadvantage of asymmetric cryptography over symmetric-key cryptography. **[4 M]**
*Berikan **satu [1]** kelebihan dan **satu [1]** kelemahan kriptografi asimetri berbanding kriptografi simetri.*

	Advantage / *Kelebihan*	Disadvantage / *Kelemahan*
asymmetric cryptography *kriptografi asimetri*		
symmetric-key cryptography *kriptografi simetri*		

c) Determine the type of cryptosystem (symmetric/ asymmetric) for the following encryption technique:
Tentukan jenis kriptosistem (simmetri / asimmetri) bagi teknik enkripsi berikut: **[3 M]**

i. DES _____

ii. RSA _____

iii. Vernam _____

d) In symmetric key cryptography, can Ozil use the same key to communicate with both Hendrikh and Ramsey? Explain your answer. **[2 M]**
Dalam kriptografi kunci simetrik, bolehkah Ozil menggunakan kunci yang sama untuk berkomunikasi dengan kedua-dua Hendrikh dan Ramsey? Terangkan jawapan anda.

Q3. a) Consider a cycle of DES. Each cycle involves: expansion permutation, XOR operation, S-boxes and straight permutation functions. Suppose given the Left Data Half, L_0 = **1100 1100 0000 0000 1100 1100 1111 1111** and Right Data Half, R_0 = **1111 0000 1010 1010 1111 0000 1010 1010**.

Anggap satu kitaran DES. Setiap kitaran melibatkan: fungsi permutasi pengembangan, operasi XOR, Kotak-S dan permutasi lurus. Andai diberi nilai setengah Data Kiri, L_0 = ***1100 1100 0000 0000 1100 1100 1111 1111*** *dan setengah Data Kanan,* R_0 = ***1111 0000 1010 1010 1111 0000 1010 1010.***

i) Expand R_0 to get $E[R_0]$, where E[*] is the expansion permutation function. **[4 M]**

Kembangkan R_0 *untuk mendapatkan* $E[R_0]$, di mana *E[*] adalah fungsi pemutasi kembangan.*

Note: Refer Tables in Appendix A / *Rujuk Jadual di Apendiks A*

$E[R_0]$, = _____

ii) What is the purpose of expansion permutation function? **[2 M]**
Apakah tujuan fungsi permutasi kembangan?

iii) Given the Key, K_0 = 0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101, perform XOR operation, that is $A = E[R_0] \oplus K_0$ **[3 M]**

Diberi kunci, K_0 = *0000 1011 0000 0010 0110 0111 1001 1011 0100 1001 1010 0101, lakukan operasi XOR, iaitu* $A = E[R_0] \oplus K_0$

Q4. a) 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.*

b) In RSA, given 2 prime numbers p=17 and q=11. Find **n** and **φ(n)**. If the public key e = 7, find the public key **d** such that $d = e^{-1} \bmod \phi(n)$ is the inverse of **e**. Using the key pairs obtained, **decrypt** the ciphertext "**ME**". Note: Let A =1, B=2,C=3,.....,Z=26. **[5 M]**

*Dalam RSA, diberikan 2 nombor perdana p = 17 dan q = 11. Cari **n** dan **φ(n)**. Jika kekunci umum e = 7, **d** di mana $d = e^{-1} \bmod ((n)$ adalah songsang **e**. Menggunakan pasangan kunci yang diperolehi, nyahsulitkan ciphertext "**ME**". Nota: Biarkan A = 1, B = 2, C = 3,..., Z = 26.*

Q5. a) A digital signature is one of the most important methods to ensure the authenticity of digital information. How is a digital signature created from the digital fingerprint (hash) of the information? **[2 M]**

Tandatangan digital adalah salah satu kaedah yang paling penting untuk memastikan kesahihan maklumat digital. Bagaimana tandatangan digital dihasilkan dari cap jari digital (cincangan) maklumat?

b) Refer to Figure 1 below. **A** is the sender of the message (plaintext) and **B** is the receiver.
*Rujuk Rajah 1 di bawah. **A** adalah menghantar mesej (teks biasa) dan **B** adalah penerima.*

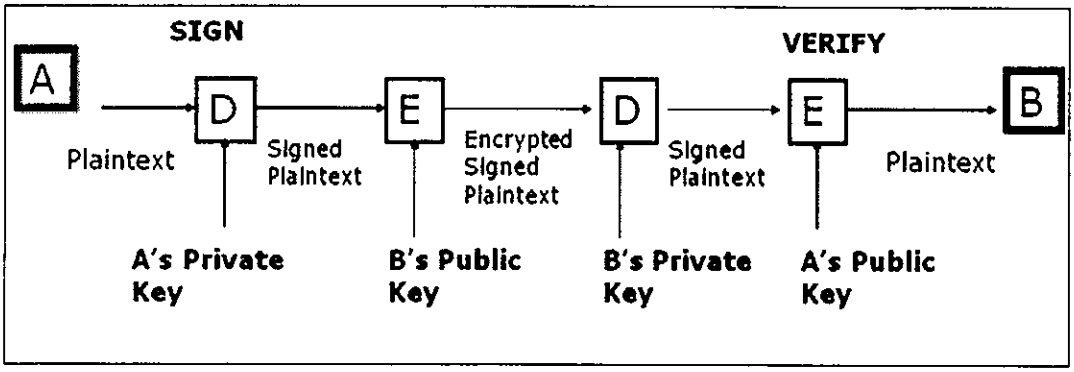


Figure 1 / *Rajah 1*

i) What is the purpose of using A's private key to decrypt the plaintext and then using A's public key to encrypt the signed message? What major security issue is addressed here? **[3 M]**
Apakah tujuan menggunakan kunci peribadi A untuk mendekrip mesej dan kemudian menggunakan kunci umum A to mengenkrip mesej yang telah ditanda-tangani? Apakah isu keselamatan utama yang cuba ditangani?

ii) What is the purpose of using B's public key to encrypt the signed plaintext and then using B's private key to decrypt the encrypted signed message? **[3 M]**
Apakah tujuan menggunakan kunci umum B untuk mengenkrip mesej yang telah dan menggunakan kunci peribadi B untuk mendekrip mesej yang telah ditanda tangani?

Q6. 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.

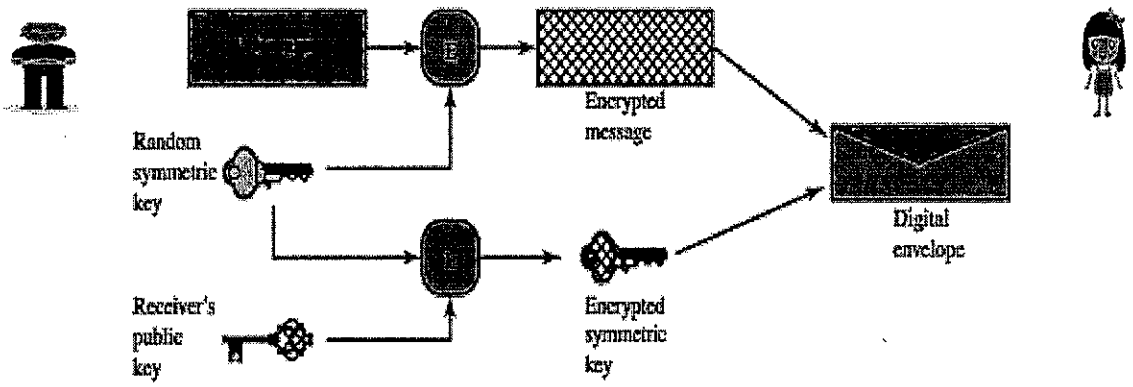


Figure 2. Creation of Digital Envelope

Rajah 2: Pembentukan Sampul Digital

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

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

Q7. a) Describe the **three (3)** main concerns with the use of passwords for authentication.
*Terangkan **tiga (3)** kebimbangan utama dalam penggunaan katalaluan dalam pengesahan,* **[3 M]**

b) Biometric authentication can be used to control access to employees and registered visitors, but there are some problems with biometrics. List **two [2]** reasons people might be reluctant to use biometrics for authentication. **[3 M]**
*Pengesahan biometrik boleh digunakan untuk kawalan capaian kepada pekerja dan pelawat yang berdaftar tetapi terdapat beberapa masalah dalam penggunaan biometrik ini. Senaraikan **dua [2]** sebab mengapa orang ramai enggan menggunakan biometrik untuk pengesahan.*

c) Your supervisor is very busy and asks you to log into the HR Server using her user-ID and password to retrieve some reports. What should you do? Choose below.

A: It's your boss, so it's OK to do this.
B: Ignore the request and hope she forgets.
C: Decline the request and remind your supervisor that it is against the company's policy.

Give reason to your answer. **[3 M]**

Penyelia anda tersangat sibuk dan menyuruh anda untuk 'log in' pelayan HR dengan menggunakan ID pengguna dan katalaluannya untuk mendapatkan laporan. Apakah yang anda harus lakukan? Pilih berikut.

A: Ia adalah ketua anda, maka ini adalah OK untuk melakukanya.
B: Abaikan permintaannya dan berharap ia akan lupa mengenai perkara ini.
C: Menolak permintaan dan mengingatkan penyelia anda bahawa ia dalah melanggari polisi syarikat.

Beri alasan kepada jawapan anda.

Q8. a) You work as an IT security manager in Data-Secure Inc., you are in charge of the security of data in your company. How do you sanitizing your confidential data? Give **three (3)** methods. **[3 M]**
*Anda bekerja sebagai pengurus keselamatan IT di Data-Secure Inc., anda bertanggung-jawab untuk keselamatan data di syarikat andda. Bagaimanakah anda membersihkan data sulit? Beri **tiga (3)** kaedah.*

b) Read the following scenario / *Baca senario berikut:*

Ramsey is a computer security consultant. He likes the challenge of finding and fixing securities vulnerabilities. He is wealthy and does not need to work, so he has ample time to test the security of the system.
In his spare time he aggressively attacks commercial product for vulnerabilities. He is proud of the tools and approach he has developed, and he is quite successful of finding flaws. He likes to probe accessible system on the Internet, and when he finds the vulnerable sites, he contacts the owners to offer his services repairing the problems. He is also a believer in high quality pastries and he will plant small programs to slow down the performance of the web sites of the pastry shops that do not use quality butter.

Ramsey adalah perunding keselamatan komputer. Dia suka cabaran dalam mencari dan memperbaiki kelemahan keselamatan. Dia seorang yang kaya dan tidak perlu bekerja, jadi dia mempunyai masa yang mencukupi untuk menguji keselamatan sesuatu sistem.
Pada masa lapang, dia secara agresif menyerang produk komersil bagi mencari kelemahan Dia gemar mencari sistem yang boleh diakses di Internet, dan apabila dia mendapati kelemahan di sesuatu laman itu, dia menghubungi pemilik untuk menawarkan perkhidmatan membaiki masalah. Dia juga seorang yang tegas dan percaya pada pastri yang berkualiti tinggi dan beliau akan meletakkan aturcara yang kecil untuk melambatkan prestasi laman web kedai pastri yang tidak menggunakan mentega berkualiti.

Would you hire Ramsey as a computer security consultant to protect your computer system in your company? Discuss. **[4 M]**
Adakah anda akan mengupah Ramsey sebagai perunding keselamatan komputer untuk melindungi sistem komputer syarikat anda? Bincangkan.

Q9. a) For the vulnerabilities that can affect the integrity of a computer network listed in a table below, determine **one (1)** control that can be used to overcome the problem faced.
*Untuk kelemahan yang boleh menjejaskan keutuhan sesuatu rangkaian yang disenaraikan dalam jadual di bawah, tentukan **satu (1)** langkah kawalan yang boleh digunakan untuk mengatasi masalah kelemahan yang dihadapi.* **[3 M]**

Vulnerabilities / *Kelemahan*	Controls / *Kawalan*
Active Wiretapping / *Curi Talian Aktif*	
Impersonation / *Penyamaran*	
DNS attack / *Serangan DNS*	

b) List and explain **two (2)** encryption methods used in a network application. **[4 M]**
*Senarai dan terangkan **dua(2)** kaedah enkripsi yang digunakan dalam aplikasi rangkaian.*

c) Firewall is an extremely useful security measure for an organization. However, it does not solve all of the security problems. List **three [3]** limitations of a firewall. **[3 M]**
*Tembok api adalah langkah keselamatan yang amat berguna bagi sebuah organisasi, Walau bagaimanapun ia tidak dapat menyelesaikan semua masalah keselamatan. Senaraikan **tiga [3]** kekangan tembok api.*

APPENDIX A

Table 1: Initial Permutation

Bit	Goes to Position							
1-8	40	8	48	16	56	24	64	32
9-16	39	7	47	15	55	23	63	31
17-24	38	6	46	14	54	22	62	30
25-32	37	5	45	13	53	21	61	29
33-40	36	4	44	12	52	20	60	28
41-48	35	3	43	11	51	19	59	27
49-56	34	2	42	10	50	18	58	26
57-64	33	1	41	9	49	17	57	25

Table 2: Expansion Permutation

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

Table 3: 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

Table 4: Key Permutation

Key Bit	1	2	3	4	5	6	7	8	9	10	11	12	13	14
Selected for Position	5	24	7	16	6	10	20	18	—	12	3	15	23	1
Key Bit	15	16	17	18	19	20	21	22	23	24	25	26	27	28
Selected for Position	9	19	2	—	14	22	11	—	13	4	—	17	21	8
Key Bit	29	30	31	32	33	34	35	36	37	38	39	40	41	42
Selected for Position	47	31	27	48	35	41	—	46	28	—	39	32	25	44
Key Bit	43	44	45	46	47	48	49	50	51	52	53	54	55	56
Selected for Position	—	37	34	43	29	36	38	45	33	26	42	—	30	40

Table 5: S-Boxes

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

END OF QUESTIONS/ *SOALAN TAMAT*

Mukasurat ini sengaja dibiarkan kosong

[This page is purposely left blank]