UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (UTMSPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER II – SESSION 2017 / 2018

PROGRAM KERJASAMA

COURSE CODE / *KOD KURSUS* : DDPC 3343

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

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

DURATION / *TEMPOH* : 2 HOURS 30 MINUTES

DATE / *TARIKH* : APRIL 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 ...17... pages including the cover
Kertas soalan ini mengandungi .....17..... 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 7.

Pilih satu jawapan yang paling tepat. Tulis jawapan anda pada jadual yang disediakan pada mukasurat 7.

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. Which of the following virus types changes its characteristics as it spreads?
   Manakah di antara jenis virus berikut yang merubah ciri-cirinya apabila ia merebak?

   A. Boot sector / *But sektor*
   B. Parasitic / *Parasit*
   C. Stealth / *Sembunyian*
   D. Polymorphic / *Polimorfik*

4. 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*

5. The act of obtaining information of a higher level of sensitivity by combining information from lower level of sensitivity is called _____.
Tindakan memperolehi maklumat daripada tahap sensitiviti yang tinggi dengan menggabungkan maklumat dari tahap kepekaan yang lebih rendah yang dipanggil _____ .

A. Aggregation / *Pengagregatan*
B. Data mining / *Perlombongan data*
C. Inference / *Inferens*
D. Polyinstantiation / ' Polyinstantiation '

6. The following are types of disclosure that can happened in database **EXCEPT**
Berikut adalah jenis-jenis pendedahan yang boleh berlaku dalam pangkalan data ***KECUALI***

A. exact data / *data sebenar*
B. existence / *kewujudan*
C. bounds / *sempadan*
D. precision / *kejituan*

7. 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*

8. 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'*

9. 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

10. Which of the following **DOES NOT** use a 'Cryptographical Technique' to protect data?
*Manakah antara berikut **TIDAK** menggunakan 'Teknik Kriptografi' untuk memelihara data?*

A. The use of digital signatures
Penggunaan tanda tangan digital

B. Data encryption
Enkripsi data

C. The use of stored encrypted password files
Penggunaan fail kata laluan yang dienkrip dan tersimpan

D. Using asymmetric keys at 'sender' and 'receiver' nodes
Menggunakan kunci asimetrik pada nod penghantar dan penerima

11 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.

12. 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

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. Which of the following is **NOT** a good property of a firewall?
*Manakah antara berikut **BUKAN** sifat yang baik untuk tembok api?*

A. Only authorized traffic must be allowed to pass through the firewall.
Hanya trafik yang diiktiraf dibenarkan untuk melalui tembok api itu.
B. The firewall itself, should be immune to penetration.
Tembok api itu patut lali dengan penembusan.
C. It should allow for easy modification by authorized user.
Ia patut membenarkan pengubah-suaian yang mudah oleh pengguna yang diiktiraf.
D. Traffic must only be allowed to pass from inside to outside the firewall
Mesti hanya trafik dari dalam ke luar tembok api dibenarkan lalu.

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

A. establish a cost model for security activities.
mengistiharkan 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 /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. 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***.

Cybercrimes / *Jenayah Siber*	**Type of Attack / *Jenis Serangan***
Offering or making available of child pornography through a computer system. *Menawarkan atau sediakan pornografi kanak-kanak menerusi sistem komputer.*	
Infringements of copyright and related rights *Perlanggaran hak cipta dan yang berkaitan dengannya*	
Damaging, deletion, deterioration, alteration or suppression of data without right. *Merosakkan, penghapusan, memerosotkan, pindaan atau penindasan data tanpa hak.*	

b) Classify each of the following as a violation of (A) confidentiality, (B) integrity, (C) availability, (D) non-repudiation, or (E) access control. Put your answer in the box provided. **[4 M]**

Sila kelaskan setiap berikut sebagai pelanggaran terhadap (A) kerahsiaan (B) keutuhan (C) ketersediaan, (D) tiada penyengkalan, atau (E) kawalan capaian. Tulis jawapan anda dalam kotak yang disediakan.

i) Alexis copies Wilshere's progtamming assignment. ☐
Alexis meniru tugasan pengaturcaraan Wilshere.

ii) Walcott crashes the operating system in Ramsey's computer, ☐
Walcott merosakkan sistem pengoperasian dalam komputer Ramsey.

iii) Rooney changes the amount on Jack's check from $1000 to $10000 ☐
Rooney menukar jumlah pada cek Jack dari $1000 kepada $10000.

iv) Özil is given the right to read and modify FileArsenal.doc. ☐
Özil diberi kebenaran untuk membaca dan mengubahsuai FileArsenal.doc

Q2. a) Explain the difference between stream cipher and block ciphers. **[4 M]**

Terangkan perbezaan antara kod rahsia rentetan dan kod rahsia blok.

b) There are a number of different possible attacks on a cryptosystem by a passive eavesdropper depending on what information is available to the eavesdropper. Suppose Eve is the eavesdropper. Describe the three (3) kinds of attack on a cryptosystem: ciphertext only, known plaintext, chosen plaintext. For each, give a scenario in which such an attack might be plausible for Eve to carry out. **[6 M]**

Terdapat beberapa serangan berbeza yang boleh dilakukan oleh pengintip pasif terhadap sebuah kriptosistem bergantung kepada apakah maklumat yang didapati oleh pengintip tersebut. Andaikan Eve adaalah pengintip itu. Huraikan tiga (3) serangan ke atas sebuah kriptosistem: teks rahsia sahaja, mengetahui teks biasa, teks biasa pilihan. Bagi setiap satu, berikan satu senario di mana serangan mungkin munasabah bagi Eve lakukan.

Q3. a) DES is a block encryption consisting of 16 cycles of transposition and substitution processes. One of the steps in these 16 cycles is DES key transformation. Explain steps in DES key transformation. **[4 M]**

DES adalah enkripsi blok yang merangkumi 16 kitaran proses transposisi dan penyelitan. Salah satu langkah dalam 16 kitaran ini adalah transformasi kunci DES. Terangkan langkah-langkah dalam transformasi kunci DES.

b) Refer to the following diagram. 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 input of the S-box is **100011110101000100011110101000100011110101000111O** and the 48-bit key, K in hexadecimal value is **123456789ABCh**. Determine the 32-bit output of the P-box. (Note: Refer to Appendix A for S-box and P-box) **[8 M]**

Rujuk Rajah 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 input 48-bit bagi kotak-S ini adalah ***100011110101000100011110101000100011110101000111O*** *dan kunci, K 48-bit dalam heksadesimal adalah* ***123456789ABCh****. Tentukan output 32-bit bagi kotak-P (Nota: rujuk Lampiran A untuk kotak-S dan kotak-P)*

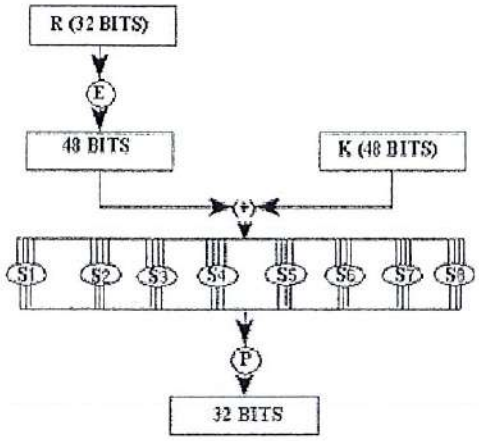

Figure 1 : S-Box Substitution and P-box Straight Permutation

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

Answer space for Question 3 b. / *Ruang jawapan bagi soalan 3 b*

Q4. a) Using values shown in Table 1, decrypt the following message using monoalphabetic substitution method with key = 4. Give the formula that you use in solving the problem. **[5 M]**

Menggunakan nilai pada Jadual 1, dekrip mesej berikut dengan menggunakan kaedah tulisan rahsia penggantian satu abjad dengan kunci = 4. Berikan formula yang anda guna dalam menyelesaikan masalah ini.

Message: **EVWIREP MW KVIEX**

Table 1 / *Jadual 1*

A	B	C	D	E	F	G	H	I	J	K	L	M	N
00	**01**	**02**	**03**	**04**	**05**	**06**	**07**	**08**	**09**	**10**	**11**	**12**	**13**
O	P	Q	R	S	T	U	V	W	X	Y	Z		
14	**15**	**16**	**17**	**18**	**19**	**20**	**21**	**22**	**23**	**24**	**25**		

Decrypted Mesaage/ *Message yang didekrip*: _____

Formula: _____

b) Describe steps involved in the generation of public and private keys in the *RSA* (Rivest Shamir and Adelman) public key cryptosystem. **[5 M]**

Huraikan langkah-langkah yang terlibat dalam penjanaan kunci umum dan peribadi dalam in kriptosistem umum RSA (Rivest Shamir dan Adelman).

c) My robot toy RSA key is N = 187, e = 107.If a ciphertext , C is 2. What is the plaintext? (Note: 187 = 11 * 17) **[4 M]**

*Kunci RSA bagi robot mainan saya adalah N = 187 e = 107. Jika ciphertext, C adalah 2. Apakah teks biasanya ? (Nota: 187 = 11 * 17)*

Q5. a) Explain the following terminologies: **[4 M]**
Terangkan istilah-istilah berikut:

i. Message Authentication / *Pengesahan Mesej*

ii. Message Non-repudiation / *Tiada Penafian Mesej*

b) Refer to Figure 2 below. What is the purpose of using the public key of the sender (A) in encrypting the signed message? What major security issue is addressed here?
Rujuk Rajah 2 di bawah. Apakah tujuan menggunakan kunci umum penghantar (A) untuk mengenkrip mesej yang telah ditanda-tangani? Apakah isu keselamatan yang utama yang cuba di atasi? **[4 M]**

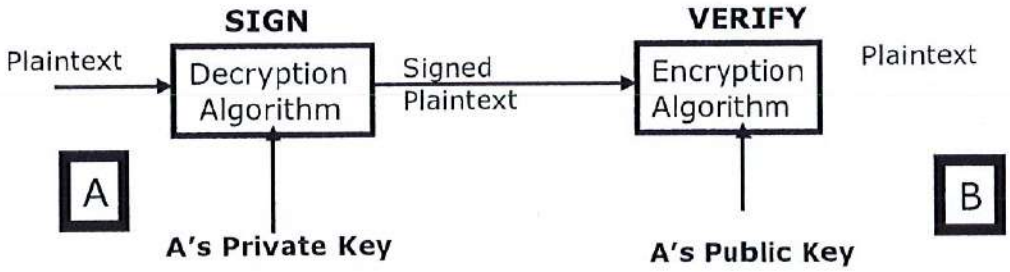

Figure 2 / *Rajah 2*

Q6. a) Describe the **three (3)** main concerns with the use of passwords for authentication.
Terangkan ***tiga (3)*** *kebimbangan utama dalam penggunaan katalaluan dalam pengesahan,* [6 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) 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.

Q7. a) Sometimes when you send messages using WhatsApp you received message as shown in Figure 2. What is the meaning of the message?
Note: Your answer should explain what is end-to-end encryption and how does it work to ensure the security of the message. [3 M]

Kadang-kadang apabila anda menghantar mesej menggunakan WhatsApp anda menerima mesej seperti dalam Rajah 2. Jelaskan apakah maksud mesej tersebut?

Nota: Jawapan anda harus menerangkan apa itu enkripsi hujung-ke-hujung dan bagaimana ia berfungsi untuk memastikan keselamatan mesej.

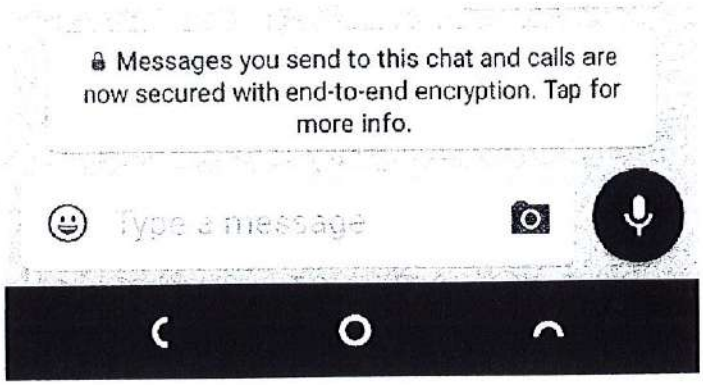

Figure 2 / *Rajah 2*

b) 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.*

Q8. a) What is element integrity in a database? [2 M]
Apakah keutuhan elemen dalam pangkalan data?

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.

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]