5

UTM UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (UTMSPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER 1 – SESSION 2016 / 2017
PROGRAM KERJASAMA

COURSE CODE *KOD KURSUS*	:	DDPC 3343
COURSE NAME *NAMA KURSUS*	:	COMPUTER SECURITY / *KESELAMATAN KOMPUTER*
YEAR / PROGRAMME *TAHUN / PROGRAM*	:	3 / DDPC / DDPZ
DURATION *TEMPOH*	:	2 HOURS 30 MINUTES / 2 *JAM 30 MINIT*
DATE *TARIKH*	:	OCTOBER 2016

INSTRUCTION/*ARAHAN* :

1. Answer **All** question in the space provided in this question paper.
   *Jawab **Semua** soalan diruang 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 NAME *NAMA 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

+SECTION A / *BAHAGIAN A*
24 MARKS / *24 MARKAH*

MULTIPLE CHOICE QUESTIONS / *SOALAN ANEKA PILIHAN*

Choose the most appropriate answer. Write your answer in the table on page 17.
Pilih jawapan yang paling sesuai. Tulis jawapan anda di jadual pada mukasurat 17.

1. What is the **best** description of a stream cipher?
*Manakah penerangan yang paling **baik** untuk 'cipher' aliran?*

   A. The message is divided into blocks and mathematical functions are performed on each block.
   Mesej dibahagi kepada dua blok dan fungsi matematik dilakukan pada setiap blok.

   B. The sender must encrypt the message with his/her private key so the receiver can decrypt it with her/his public key.
   Penghantar mesti enkrip mesej dengan kunci peribadi jadi penerima boleh mendekrip mesej itu dengan kunci umumnya.

   C. The cipher uses a key to create a keystream and XOR's the result with the message.
   Cipher menggunakan kunci untuk mewujudkan aliran utama dan kemudian XOR kan hasil dengan mesej.

   D. The cipher executes 16 rounds of computation on each bit.
   Cipher melaksanakan 16 pusingan komputasi untuk setiap bit.

2. If Walcott wants to send an encrypted message to Jack, the plaintext is encrypted using the public key of _____ .
Jika Walcott ingin menghantar mesej yang telah dienkrip kepada Jack, teks biasa akan dienkrip menggunakan kunci umum _____ .

   A. Walcott
   B. Jack
   C. the cryptographic system / *sistem kritografik*
   D. both Walcott and Jack. / *kedua-dua Walcott dan Jack*

3. A digital certificate binds a user with the _____ .
Sijil berdigit mengikat pengguna dengan _____ .

   A. user's private key / *kunci peribadi pengguna*
   B. user's public key / *kunci umum pengguna*
   C. user's passport / *paspot pengguna*
   D. user's driving license / *lesen memandu pengguna*

4. *The following statements are correct* ***except***
Kenyataan berikut adalah benar ***kecuali***

A. SHA-S is a message digest algorithm.
SHA-S adalah satu algoritma 'message digest'.

B. The X.509 standard defines the structure of the digital certificate.
Piawaian X.509 menakrif struktur bagi sijil digital.

C. Integrity of the entire database is the responsibility of the DBMS software.
Keutuhan bagi keseluruhan pangkalan data adalah tanggung jawab perisian DBMS.

D. An example of passive attack is altering message content.
Satu contoh bagi serangan pasif ialah mengubah kandungan mesej.

5. During a denial-of-service (DOS) attack, a network administrator blocks the source IP with the firewall, but the attack continues. What is the most likely cause of the problem?
Semasa serangan denial-of-service (DOS), pentadbir rangkaian memblok IP sumber dengan firewall, tetapi serangan itu masih berterusan. Apakah punca masalah yang paling mungkin?

A. The denial-of-service worm has already infected the firewall locally
Cecacing 'denial-of-service' sudah menjangkiti firewall tempatan

B. The attack is coming from multiple distributed hosts
Serangan datang dari berbilang tuan rumah yang teragih

C. A firewall can't block denial-of-service attacks
Firewall tidak dapat menyekat serangan denial-of-service.

D. Antivirus software needs to be installed.
Perisian antivirus perlu dipasang.

6. A virus that attempts to avoid detection by periodically modifying portions of itself would be _____.
Virus yang cuba mengelak daripada dikesan dengan menukar sebahagian dirinya dari masa ke semasa adalah _____.

A. a stealth virus / *virus rahsia*
B. a delayed propagation virus / *virus penyebaran lewat*
C. a polymorphic virus / *virus polimorpik*
D. a boot sector virus / *virus sektor boot*

7. Consider the following code fragment:
Pertimbangkan keratan kod berikut:

```
legitimate code
if data is Friday the 13th;
  crash_computer();
legitimate code
```

What type of malware is this?
Apakah jenis-jenis perisian berniat jahat ini?

A. Trojan Horse / *Kuda Trojan*
B. Logic Bomb / *Bom Logik*
C. Salami Attack / *Serangan Salami*
D. Trapdoor / *Pintu Perangkap*

8. 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 sah pengguna boleh melakukan

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

D. to protect computers from viral infections
untuk melindungi komputer daripada jangkitan virus
katalaluan, enkripsi, dan pengenalan diri

D. identification, encryption, and authorization
pengenalan diri, enkripsi, dan kebenaran

9. In database, an act of obtaining information of a higher level of sensitivity by combining information from lower level of sensitivity is called _____.
Dalam pangkalan data, perbuatan mendapatkan maklumat tahap sensitif yang tinggi dengan menggabungkan maklumat dari tahap sensitiviti lebih rendah dipanggil _____ .

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

10. The following are type of disclosure that can happened in database **except**
Berikut adalah jenis pendedahan yang boleh berlaku dalam pangkalan data ***melainkan***

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

11. 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 sah pengguna boleh melakukan

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

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

12 Which of the following statements regarding session hijacking is **incorrect**:
Manakah di antara kenyataan berikut mengenai rampasan sesi ***tidak betul:***

A. In session hijacking, to spoof IP addresses is possible.
Dalam sesi rampasan, untuk ditipu alamat IP boleh berlaku.

B. Involves an attacker inserting him/herself in between two conversing devices.
Melibatkan penyerang menyelitkan diri mereka antara dua peranti yang sedang berkomunikasi.

C. Allows the attacker to pretend he/she is one of the actual endpoints in the transaction.
Membolehkan penyerang untuk berpura-pura dia adalah salah satu daripada penghujung yang sebenar dalam transaksi

D. Session hijacking cannot be safeguarded, not even through mutual authentication using protocols such as IPsec.
Session hijacking tidak boleh dilindungi, walau pun melalui pengesahan bersama yang menggunakan protokol seperti IPsec.

13. What are the three(3) primary methods for authenticating users to a computer system or network system?
Apakah tiga(3) kaedah utama untuk mengesahkan pengguna untuk sistem komputer atau sistem rangkaian?

A. passwords, tokens, and biometrics.
katalaluan, token dan biometrik.

B. authorization, identification, and tokens.
kebenaran, pengenalan diri dan token.

C. passwords, encryption, and identification.
katalaluan, enkripsi, dan pengenalan diri.

D. identification, encryption, and authorization.
pengenalan diri, enkripsi, dan kebenaran.

14. This is a document that states in writing how a company plans to protect the company's physical and IT assets.
Ini adalah satu dokumen yang menyatakan secara bertulis bagaimana syarikat merancang untuk melindungi aset fizikal dan aset ITnya.

A. Data Encryption Standard / *Piawaian Enkripsi Data*
B. Security policy / *Polisi Keselamatan*
C. Public key certificate / *Sijil Kunci Umum*
D. Access control list / *Senarai Kawalan Capaian*

15. In a "work for hire" situation, who is considered as the author of the work?
Dalam situasi "kerja bergaji" , siapakah tuanpunya hasil sesuatu kerja?

A. employer / *majikan*
B. employee / *pekerja*
C. the owner of the patent / *tuanpunya paten*
D. employer and employee / *majikan & pekerja*

16. Unfair use of copyrighted item is called _____ .
Penggunaan tidak adil terhadap bahan-bahan "copyrighted" dipanggil _____.

A. patents / *paten*
B. public domain / *domaian umum*
C. trade secret / *rahsia perdagangan*
D. piracy / *cetak rompak*

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

ANSWER ALL QUESTIONS. WRITE YOUR ANSWER IN THE SPACES PROVIDED.
JAWAB SEMUA SOALAN. TULIS JAWAPAN ANDA 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	Type of Attack
Offering or making available of child pornography through a computer system. *Menawar 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, pengubahan atau penindasan data tanpa hak.*	

b) The **four(4)** kinds of threats in the computer systems are interception, interruption, modification and fabrication. Describe and give examples for each kind of threats.
Empat (4) *jenis ancaman di dalam sistem komputer adalah pemintasan, gangguan, pengubahsuaian dan pemalsuan. Terangkan dan berikan contoh bagi setiap jenis ancaman tersebut.* **[8 M]**

Kinds / *Jenis*	Description and examples / *Penerangan dan Contoh*

Q2. a) Describe the difference between symmetric and asymmetric cryptosystem.
Huraikan perbezaan di antara kriptosistem simetrik dan asimetrik. **[3 M]**

b) In symmetric-key cryptography, how do two persons can establish secret between themselves?
Dalam kriptografi kunci simetrik, bagaimanakah dua orang boleh mencapai kerahsiaan antara mereka? **[2 M]**

c) In the RSA public-key encryption scheme, each user has a public key, **e**, and a private key, **d**. Suppose Bob leaks his private key. Rather than generating a new modulus (**n**), he decides to generate a new public and a new private key. Is this safe? Give justification to your answer. **[4 M]**
Dalam skim enkripsi kunci umum RSA, setiap pengguna mempunyai kunci umum, **e** *dan kunci peribadi,* **d**. *Andaikan Bob membocorkan kunci peribadinya. Dia tidak menjana modulus baru* ***(n)****, tetapi memutuskan untuk menjana kunci umum,* **e** *dan kunci peribadi,* **d** *yang baru. Adakah ini selamat? Beri justifikasi kepada jawapan anda.*

Q3. a) Given **p**=5;**q**=11,**e**=3; **M**=9. Find **d** and perform encryption and decryption using RSA. **[8 M]**
*Diberi **p** = 5; **q** = 11, **e** = 3; **M** = 9. Cari **d** dan lakukan enkripsi dan dekripsi dengan menggunakan RSA.*

b) In a public-key system using RSA, you intercept the ciphertext **C** = 10 sent to a user whose public key is **e**=5, **n**=35. What is the plaintext **M**? **[4 M]**
*Dalam sistem kunci umum yang menggunakan RSA, anda memintas ciphertext **C** = 10 yang dihantar kepada pengguna yang kekunci umum adalah **e** = 5, **n**=35. Apakah teks biasa nya, **M**?*

Q4. a) DES is a block encryption consisting of 16 cycles of transposition and substitution processes. Given

ii) Expand R_1 to get $E[R_1]$, where E[*] is the expansion function. **[4 M]**

Kembangkan R_1 *untuk mendapatkan* $E[R_1]$, di mana E[*] *adalah fungsi kembangan.*

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 by listing **two(2)** advantages and disadvantages of each. **[6 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" dengan menyenaraikan **dua(2)** kebaikan dan kelemahan bagi setiap satu jenis IDS ini.*

b) Explain the strengths and weakness of each of the following firewall deploying scenarios in the defending servers desktop machines and laptops against network threats.

i. A firewall at the network perimeter

ii. Firewalls on every end host machines. **[6 M]**

Terangkan kekuatan dan kelemahan setiap tembok api berikut menggunakan senario dalam mempertahankan mesin pelayan desktop dan laptop daripada ancaman rangkaian.

i. *Tembok api pada perimeter rangkaian*

ii. *Tembok api pada tiap-tiap hujung hos mesin*

Q7. a) As an IT security manager in your office how do you sanitizing your confidential data? Give **three (3)** methods. **[3 M]**

*Sebagai pengurus keselamatan IT di pejabat anda, bagaimana anda membersihkan data sulit? Beri **tiga (3)** kaedah.*

b) A friend sends an electronic Hallmark greeting card (e-card) to your work email. You need to click on the attachment to see the card. What should you do? If you decide to click the attachment to see the card, discuss **two (2)** risks that you would face? **[3 M]**

*Seorang sahabat menghantar kad ucapan Hallmark elektronik (e-card) kepada e-mel kerja anda. Anda perlu klik pada lampiran untuk melihat kad. Apa yang perlu anda lakukan? Jika anda memutuskan untuk klik lampiran untuk melihat kad, bincangkan **dua (2)** risiko yang akan dihadapi?*

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

Wishere 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. He probes 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 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.

Wishere adalah perunding keselamatan komputer. Dia suka cabaran untuk mencari dan memperbaiki kelemahan keselamatan. Dia kaya dan tidak perlu ke tempat kerja, jadi dia mempunyai masa yang mencukupi untuk menguji keselamatan sesuatu sistem. Dia cari sistem yang boleh diakses di internet, dan apabila dia mendapati kelemahan sistem dia menghubungi pemilik untuk menawarkan perkhidmatan membaiki masalah. Dia adalah 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 Wilshere as a computer security consultant to protect your computer system in your company? Discuss. **[4 M]**

Adakah anda mengupah Wilshere sebagai perunding keselamatan komputer untuk melindungi sistem komputer syarikat anda? Bincangkan.

ANSWER SPACE FOR SECTION A /24 MARKS

RUANG JAWAPAN BAGI BAHAGIAN A /24MARKAH

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

APPENDIX

Initial Permutation

Bit	Goes to Position							
18	40	8	48	16	56	24	64	32
916	39	7	47	15	55	23	63	31
1724	38	6	46	14	54	22	62	30
2532	37	5	45	13	53	21	61	29
3340	36	4	44	12	52	20	60	28
4148	35	3	43	11	51	19	59	27
4956	34	2	42	10	50	18	58	26
5764	33	1	41	9	49	17	57	25

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	18	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

Permutation Box P

Bit	Goes to Position							
18	9	17	23	31	13	28	2	18
916	24	16	30	6	26	20	10	1
1724	8	14	25	3	4	29	11	19
2532	32	12	22	7	5	27	15	21

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

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]