UTM UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (UTMSPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER II– 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 / 3 DDPZ
DURATION *TEMPOH*	:	2 HOURS 30 MINUTES
DATE *TARIKH*	:	MARCH / APRIL 2017

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 PENGAJIAN DIPLOMA
SPACE
UTM *International Campus*
PETIKAN DARIPADA PERATURAN AKADEMIK

ARAHAN AM

1. PENYELEWENGAN AKADEMIK (SALAH LAKU PEPERIKSAAN)

1.1 Pelajar tidak boleh melakukan mana-mana salah laku peperiksaan seperti berikut:-

(a) Memberi atau menerima atau memiliki sebarang maklumat dalam bentuk elektronik, cetak atau apa-apa jua bentuk lain yang ada kaitan dengan sesuatu kursus semasa peperiksaan bagi kursus tersebut dijalankan sama ada di dalam atau di luar Dewan/Bilik Peperiksaan melainkan dengan kebenaran Ketua Pengawas.

(b) Menggunakan maklumat yang diperolehi seperti di perkara 1(a) di atas bagi tujuan menjawab soalan peperiksaan.

(c) Menipu atau cuba untuk menipu atau berkelakuan mengikut cara yang boleh ditafsirkan sebagai menipu atau cuba untuk menipu semasa peperiksaan sedang berjalan.

(d) Lain-lain salah laku yang ditetapkan oleh Universiti.

2. HUKUMAN

2.1 Sekiranya pelajar didapati telah melakukan pelanggaran mana-mana peraturan peperiksaan ini, setelah dibicara oleh Jawatankuasa Akademik Fakulti dan disabitkan kesalahannya, Senat boleh mengambil tindakan dari mana-mana satu, atau kombinasi yang sesuai dari dua atau lebih hukuman-hukuman berikut :-

(a) Memberi markah SIFAR (0) bagi keseluruhan keputusan peperiksaan mata pelajaran yang berkenaan. (Termasuk kerja kursus).

(b) Memberi markah SIFAR (0) bagi semua mata pelajaran yang didaftarkan kepada semester tersebut.

(c) Pelajar yang didapati melakukan kesalahan kali kedua hendaklah 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 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 closest meaning of the phrase "**Internet Security**"?
*Apakah makna terdekat bagi frasa "**Keselamatan Internet**"?*

   A. Rules defined in firewall systems.
   Peraturan-peraturan yang ditetapkan dalam sistem tembok api.
   B. Rules defined in X.500.
   Peraturan-peraturan yang ditentukan dalam X.500.
   C. Measures to protect data during their transmission.
   Langkah-langkah untuk melindungi data semasa penghantaran mereka.
   D. Measures to protect data during their transmission over a collection of interconnect ed networks.
   Langkah-langkah untuk melindungi data semasa penghantaran mereka ke atas sekumpulan rangkaian saling.

2. A firewall is a _____.
Tembok api merupakan satu _____.

   A. wall built to prevent fires from damaging a corporate intranet
   dinding yang dibina untuk mengelakkan kebakaran dari merosakkan intranet korporat
   B. security device deployed at the boundary of a company to prevent unauthorized physical access
   alat keselamatan yang ditempatkan di sempadan sesebuah syarikat untuk mencegah pencapaian secara fizikal yang tidak dibenarkan
   C. security device deployed at the boundary of a corporate intranet to protect it from unauthorized access
   alat keselamatan yang ditempatkan di sempadan intranet korporat untuk melindunginya daripada capaian yang tidak dibenarkan
   D. device to prevent all accesses from the internet to the corporate intranet
   peranti untuk mengelakkan semua pencapaian daripada internet ke pihak intranet korporat

3. 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

4. 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 tembok api, 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 tembok api 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.
Tembok api tidak dapat menyekat serangan denial-of-service.

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

5. Link encryption _____.
Enkripsi pautan _____.

A. is more secure than end-to-end encryption
adalah lebih selamat dari enkripsi hujung-ke-hujung

B. is less secure than end-to-end encryption
kurang selamat daripada enkripsi hujung-ke-hujung

C. cannot be used in a large network
tidak boleh digunakan dalam satu rangkaian yang besar

D. is used only to detect errors
hanya digunakan untuk mengesan kesilapan

6. _____ of message means that the receiver is ensured that the message is coming from the intended sender, not an imposter.

_____ mesej bermakna bahawa penerima adalah memastikan bahawa mesej tersebut datang daripada pengirim yang dimaksudkan, bukan dari penyamar.

A. Confidentiality / *Kerahsiaan*
B. Integrity / *Integriti*
C. Authentication / *Pengesahan*
D. Availability / *Ketersediaan*

7. 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 / *'Polyinstantiation'*

8. 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*

9. 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*

10. One safeguard against theft or alteration of data is the use of _____ .

Satu langkah perlindungan dari kecurian atau pengubahsuaian data adalah dengan menggunakan _____ .

A. DES / *DES*
B. trapdoor / *pintu perangkap*
C. identical password / *katalaluan yang sama*
D. Trojan Horse / *Kuda Trojan*

11. 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*

12. When an attempt is to make a machine or network resource unavailable to its intended users, the attack is called _____.

Apabila cubaan untuk membuat sumber mesin atau rangkaian tiada kepada para penggunanya yang dimaksudkan, serangan itu dipanggil _____.

A. denial-of-service attack / *serangan 'denial-of-service'*
B. spoofed attack / *serangan 'spoofed'*
C. starvation attack / *serangan kebuluran*
D. man-in-the-middle attack / *serangan orang-di-tengah*

13. 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*

14. 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*

15 Unfair use of copyrighted item is called _____.
Penggunaan tidak adil terhadap bahan-bahan hak cipta dipanggil _____.

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

16. 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 penguruan 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.

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) Classify each of the following as a violation of (A) confidentiality, (B) integrity, (C) availability, (D) non-repudiation, (E) access control or (F) privacy [4 M]
Kelaskan setiap berikut sebagai pelanggaran terhadap (A) kerahsiaan (B) keutuhan (C) ketersediaan, (D) tiada penyengkalan, (E) kawalan capaian, atau (F) privasi

i) Ramsey crashes the operating system in Walcott's computer.
Ramsey merosakkan sistem pengoperasian pada komputer Walcott. _____

ii) Rooney changes the amount on Giroud's check from $1000 to $10000.
Rooney menukar jumlah pada cek Giroud dari $1000 kepada $10000. _____

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

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

b) The four (4) kinds of threats in the computer systems are interception, interruption, modification and fabrication. Describe and give examples for **two (2)** kind of threats.
*Empat (4) jenis ancaman di dalam sistem komputer adalah pemintasan, gangguan, pengubahsuaian dan pemalsuan. Terangkan dan berikan contoh bagi **dua (2)** jenis ancaman tersebut.* [6 M]

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

Q2. a) Give the most appropriate malicious code type to the following definition:
Berikan jenis kod 'jahat' yang paling sesuai dengan takrifan yang diberi: [3 M]

i) A program that appears to have a useful function but also contains hidden and unintended function that presents a security risk.
Satu program yang pada hakikatnya mempunyai tujuan yang berguna tetapi juga mempunyai fungsi yang tersorok yang mengakibatkan risiko keselamatan.

_____

ii) A program which triggers an unauthorized, usually malicious act when some predefined condition occurs.
Satu program yang akan mengakibatkan membuat perkara yang tidak dibenarkan dan jahat apabila satu keadaan yang ditetapkan berlaku.

_____

iii) A program that replicates itself without limit to exhaust resource.
Program yang membiak tanpa had bertujuan untuk menghabiskan sumber komputer.

_____

b) Why is encryption not an effective control against virus? [2 M]
Mengapakan enkripsi merupakan satu kawalan yang tidak berkesan untuk mengawal virus?

c) Describe covert channel and explain why it is a threat in data security. [4 M]
Terangkan saluran terselindung dan terangkan mengapa ia merupakan satu ancaman dalam keselamatan data.

Q3. Suppose Ramsey wants his friends to encrypt email messages before sending them to him. Computers represent text as long numbers (01 for "A", 02 for "B" and so on). The RSA Encryption Scheme is used to encrypt and then decrypt in the electronic communications. Ramsey public and private key pairs are (n,e) and (n,d) are (33,3) and (33,7).

Andaikan Ramsey mahu kawan-kawannya untuk mengenkripsi mesej e-mel sebelum menghantarnya kepada-nya. Komputer mewakilkan teks sebagai nombor lama (01 bagi "A", 02 bagi "B" dan sebagainya). Skim enkripsi RSA digunakan untuk menyulitkan dan kemudian nyahsulitkan dalam komunikasi elektronik. Pasangan kunci umum dan peribadi Ramsey (n, e) dan (n, d) adalah (33,3) dan (33,7).

a) Giroud wants to send the message **M = 13** to Ramsey. Using Ramsey's public and private keys, calculate the ciphertext **C,** and the value for plaintext, **P** when Ramsey recovers the original message. **[6 M]**

Giroud ingin menghantar mesej **M = 13** kepada Ramsey. Menggunakan kunci umum dan kunci peribadi Ramsey, kira ciphertext **C**, dan nilai untuk teks asal, **P** apabila Ramsey mendapat semula mesej asal.

b) Alexis wants to set up his own public and private keys. He chooses **p = 23** and **q = 19** with **e = 283**. Find **d** so that ed has a remainder of 1 when divided by (p − 1)(q − 1). **[4 M]**

Alexis mahu sediakan sendiri kekunci umum dan peribadi. Beliau memilih **p = 23** dan **q = 19** dengan **e = 283**. Cari **d** supaya ed mempunyai baki 1, apabila dibahagi dengan (p − 1)(q − 1).

c) In the RSA public-key encryption scheme, each user has a public key, **e**, and a private key, **d**. Suppose Alex 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. **[3 M]**

*Dalam skim enkripsi kunci umum RSA, setiap pengguna mempunyai kunci umum, **e** dan kunci peribadi, **d**. Andaikan Alex 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.*

Q4. DES is a block encryption consisting of 16 cycles of transposition and substitution processes. Given bit pattern for the plaintext as: **ABCDABCDABCDABCDh.** Also given the first cycle key, $\mathbf{K_1}$ as **123412341234h**. Consider first cycle of DES and answer the following questions:
Note: Refer to Table as in Appendix A.

DES adalah enkripsi blok yang merangkumi 16 kitaran proses transposisi dan penyelitan. Diberi pola bit bagi teks-biasa sebagai: ***ABCDABCDABCDABCDh****. Juga diberi kunci kitaran pertama,* $\boldsymbol{K_1}$ *sebagai* ***123412341234h.*** *Andaikan kitaran pertama DES dan jawab soalan berikut:*
Perhatian: Rujuk Jadual di Appendiks A.

a) Derive L_1 and R_1 **[4 M]**
Perolehi L_1 dan R_1

b) 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.*

c) Calculate $A = E[R_1]$ ***XOR*** K_1 **[4 M]**
Kira $A = E[R_1]$ ***XOR*** K_1

Q5. a) The principle of non-repudiation is one of the major computer security issues.
Prinsip tiada-penyangkalan adalah satu isu utama keselamatan komputer.

What is non-repudiation? Explain.
Apa itu tiada-penyangkalan? Terangkan. **[2 M]**

b) Suppose A wants to send message to B. A would like to insert a signature in the transaction. By using public key cryptosystem , show how can:
i) A implement the signature.
ii) B verify that the message comes from A and not any other person.

Andaikan A ingin menghantar mesej kepada B. A ingin meletakkan tandatangan pada mesej tersebut. Dengan menggunakan kritosistem kunsi umum, tunjukkan bagaimana:
i) A mengimplemen tandatangan ini.
ii) B membuktikan yang mesej ini datang dari A dan bukan dari orang lain. **[6 M]**

Q6. a) Explain the following in terms of providing security for a database:
Terangkan perkara-perkara berikut dari segi menyediakan keselamatan pangkalan data:

i. authorization / *kebenaran* **[3 M]**

ii. integrity / *integriti* **[3 M]**

iii. encryption / *penyulitan* **[3 M]**

b) When using databases, we expect a DBMS to provide access in a reliable way. Concerns for reliability and integrity are general security issues in the DBMS and they can be viewed from **three (3)** perspectives: database integrity, element integrity and element accuracy. Briefly explain the **three (3)** dimensions mentioned above.
*Apabila menggunakan pangkalan data, kita harapkan DBMS dapat menyediakan capaian yang boleh dipercayai. Perhatian terhadap kebolehpercayaan dan keutuhan adalah isu yang lazim di dalam DBMS dan ia boleh dilihat dari **tiga (3)** perspektif: keutuhan pangkalan data, keutuhan elemen dan ketepatan elemen. Dengan ringkas, terangkan **tiga (3)** dimensi yang disebut di atas.* **[6 M]**

Q7. a) 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*

b) You receive the following email from the Help Desk:

Anda menerima email berikut dari 'Help Desk':

> *Dear UTMail User,*
>
> *Beginning next week, we will be deleting all inactive email accounts in order to create space for more users. You are required to send the following information in order to continue using your email account. If we do not receive this information from you by the end of the week, your email account will be closed.*
>
> **Name (first and last):*
> **Email Login:*
> **Password:*
> **Date of birth:*
> **Alternate email:*
>
> *Please contact the Webmail Team with any questions. Thank you for your immediate attention.*

What should you do? Explain. **[3 M]**

Apakah yang patut anda lakukan? Jelaskan.

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