UTM
UNIVERSITI TEKNOLOGI MALAYSIA

Sekolah Pendidikan Profesional dan Pendidikan Berterusan (UTMSPACE)

FINAL EXAMINATION / *PEPERIKSAAN AKHIR*
SEMESTER I – 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 / 3 DDPZ
DURATION *TEMPOH*	:	2 HOURS 30 MINUTES
DATE *TARIKH*	:	OCTOBER / NOVEMBER 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 ...16... pages including the cover
Kertas soalan ini mengandungi .....16..... 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 15.
Pilih satu jawapan yang paling tepat. Tulis jawapan anda pada jadual yang disediakan pada mukasurat 15.

1. Which of the following methods are **most** effectively be used to prevent logical breach of security?
*Manakah antara kaedah berikut yang **paling** efektif untuk digunakan dalam menghalang pelanggaran logik keselamatan?*

   A. Operating system and other system software.
   Sistem pengoperasian dan perisian sistem yang lain.
   B. Computer architectural design
   Rekabentuk senibina komputer.
   C. Distributed systems design
   Rekabentuk sistem bertaburan.
   D. Network design
   Rekabentuk rangkaian.

2. 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 virus infections
   Untuk melindungi komputer daripada jangkitan virus

3. MD5 (Message Digest Algorithm 5) is a widely used cryptographic hash function and its application is for checking the _____ of the files.
MD5 (Message Digest Algorithm 5) adalah satu fungsi cincangan kriptografik yang digunakan dengan meluasnya dan applikasinya adalah untuk menyemak _____ fail.

   A. confidentiality / *kerahsiaan*
   B. availability / *ketersediaan*
   C. integrity / keutuhan
   D. access control / kawalan capaian

4. 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

5. 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*

6. Which of the following mechanism is used to achieve non-repudiation of a message delivery?
Manakah di antara mekanisma berikut digunakan untuk mencapai penafian penghantaran mesej?

A. Sender encrypts the message with the recipients public key and signs it with their own private key.
Pengirim mengenkripsi mesej dengan kekunci umum penerima dan menandatanganinya dengan kunci peribadi mereka sendiri.

B. Sender computes a digest of the message and sends it to a Trusted Third Party (TTP) who signs it and stores it for later reference.
Pengirim menjanakan menghadamkan mesej dan menghantarnya kepada pihak ketiga yang dipercayai (TTP) yang menandatangani mesej itu lalu menyimpan untuk rujukan kemudian.

C. Sender sends the message to a TTP who signs it together with a time stamp and sends it on to the recipient.
Pengirim menghantar mesej kepada TTP yang menandatanganinya bersama-sama dengan setem masa dan menghantarnya kepada penerima.

D. Sender gets a digitally signed acknowledgment from the recipient containing a copy or digest of the message.
Penghantar mendapat akuan yang ditandatangani secara digital dari penerima yang mengandungi salinan atau digest mesej.

7. Under what circumstance might a certification authority (CA) revoke a certificate?
Di bawah keadaan apakah mungkin autoriti pensijilan (CA) 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.

8. An item **not** found on a digital certificates is the _____.
*Butiran yang **tidak** terdapat dalam sijil digital adalah* _____.

A.	owner identity	*/ identity pemilik*
B.	issuing CA	*/ CA yang mengeluarkan sijil.*
C.	expiration date	*/ tarikh tamat tempuh*
D.	private key for the certificate holder	*/ kunci peribadi bagi pemegang sijil.*

9. 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*

10. 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 diikhtiraf 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 diikhtiraf.

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.

11. This kind of controls include locks on doors, guards at entry points, backup copies of important software and data, and physical site planning that reduces the risk of natural disasters.
Kawalan jenis ini termasuk memasang kunci pada pintu, menempatkan pengawal di pintu masuk, membuat salinan "backup" bagi perisian dan data yang penting, perancangan lokasi fizikal supaya dapat mengurangkan risiko akibat bencana alam.

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*

12. Alexis wishes to send a confidential and signed message to Wilshere using public key cryptography. Which is **CORRECT**?
*Alexis ingin menghantar mesej sulit dan ditandatangani kepada Wilshere dengan menggunakan kriptografi kunci umum. Manakah yang **BETUL**?*

A. Alexis signs with his public key, and encrypts with his private key
Alexis menanda tangani dengan kunci umumnya, dan enkrip dengan kunci rahsia.

B. Alexis signs with his public key and encrypts with Wilshere's public key
Alexis menanda tangani dengan kunci umumnya, dan enkrip dengan kunci umum Wilshere.

C. Alexis signs with his private key and encrypts with Wilshere's public key.
Alexis menanda tangani dengan kunci rahsianya dan enkrip dengan kunci umum Wilshere.

D. Alexis signs with Wilshere's public key and encrypts with his private key
Alexis menanda tangan dengan kunci umum Wilshere dan enkrip dengan kunci rahsianya.

13. To prevent faulty user program from destroying part of the resident portion of the operating system, _____ register is used to confine the users to one side of the boundary.
Untuk menghalang sebarang aturcara pengguna merosakkan bahagian residen sistem pengoperasian, daftar _____ digunakan untuk meletakkan pengguna pada satu bahagian sempadan.

A. fence */ pagar*
B. base */ dasar*
C. bounds */ sempadan*
D. relocation */ relokasi*

14. In the software engineering process, security requirements are best define in the _____.
Dalam proses kejuruteraan perisian, keperluan keselamatan sebaiknya ditakrifkan dalam _____.

A. the requirements phase / *fasa keperluan*
B. the system design phase / *fasa reka bentuk sistem*
C. the coding phase / *fasa pengkodan*
D. the testing phase / *fasa pengujian*

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.

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) Explain the following term in the context of computer security. [6 M]
Terangkan istilah berikut dalam konteks keselamatan komputer.

i) non-repudiation/ *tiada penyangkalan* _____

_____

ii) confidentiality / *kerahsiaan* _____

_____

iii) integrity / keutuhan _____

_____

b) The following are threats that could harm a computing system physically. For each of the following threats, suggest **one (1)** physical security control that can be used for protection.
*Berikut adalah antara ancaman yang boleh mengancam sesuatu sistem komputer secara fizikal. Untuk setiap ancaman berikut, cadangkan **satu(1)** langkah perlindungan keselamatan fizikal yang boleh digunakan untuk kawalan.*

i) Interception of Sensitive Data [2 M]
Pemintasan Data Sensitif

ii) Human vandals for example unauthorized access to your computer lab.
Vandalisme yang dilakukan oleh manusia seperti memasuki atau menggunakan makmal komputer tanpa kebenaran. [2 M]

Q2.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.

i) Explain what happen in this DES key transformation. [4 M]

ii) What is the size of the DES key after the key transformation step? [2 M]

b) Given bit pattern for the plaintext as: **ABCDABCDABCDABCDh.** Also given the first cycle key, $\mathbf{K_1}$ as **123412341234h**. Consider first cycle of DES, calculate $A = E[R_1]$ ***XOR*** K_1 [6 M]

Note: Refer to Table as in Appendix A.

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

i) Terangkan apa yang berlaku dalam transformasi kunci DES.

ii) Apakah saiz kunci DES selepas langkah transformasi kunci ini?

b) Diberi pola bit bagi teks-biasa sebagai: ***ABCDABCDABCDABCDh****. Juga diberi kunci kitaran pertama,* $\boldsymbol{K_1}$ *sebagai* ***123412341234h.*** *Andaikan kitaran pertama DES, kira* $A = E[R_1]$ ***XOR*** K_1

Nota: *Rujuk Jadual di Appendiks* A.

Q3.a) Explain the difference between stream ciphers and block ciphers. [4 M]
Terangkan perbezaan antara aliran 'cipher' dan blok 'cipher'.

b) In RSA, given 2 prime numbers p=17 and q=11. Find n and $\phi(n)$. . If the public key e = 7, find the public key **d** such that d = e^{-1} mod ϕ(n) is the inverse of **e**. Using the key pairs obtained, **decrypt** the ciphertext "**ME**". Refer Table 1 [on page 15] for the value of the alphabet [8 M]
*Dalam RSA, diberi dua nombor perdana p=17 dan q=11, cari **n** dan $\phi(n)$. Jika e=7, cari kunci umum **d** di mana d = e^{-1} mod ϕ(n) adalah songsangan bagi **e**. Menggunakan pasangan kunci yang didapati, **dekrip** teks rahsia "**ME**". Rujuk Jadual 1 [pada mukasurat 15] untuk nilai-nilai abjad*

c) Suppose we have a set of blocks encoded with the RSA algorithm and we do not have the private key. Assume **[n ,e]** where **n = pq.** is the public key. Suppose also someone tells us they know one of the plaintext blocks has a common factor with **n**. Does this help us in any way to know the keys? Justify your answer. [3 M]
*Katakan kita mempunyai satu set blok-blok yang dikodkan dengan algoritma RSA dan kita tidak mempunyai kunci peribadi. Menganggap **[n,e]** di mana **n = pq**, adalah kekunci umum. Katakan juga seseorang memberitahu kita dia tahu salah satu blok teks biasa mempunyai faktor yang sama dengan **n**. Adakah ini membantu kita dalam apa juga cara untuk mengetahui kunci kunci tersebut? Justifikasi jawapan anda.*

Q4. a) Compare and contrast MD-5 and SHA-1. [3 M]
Bandingkan dan sebaliknya MD-5 dan SHA-1.

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.

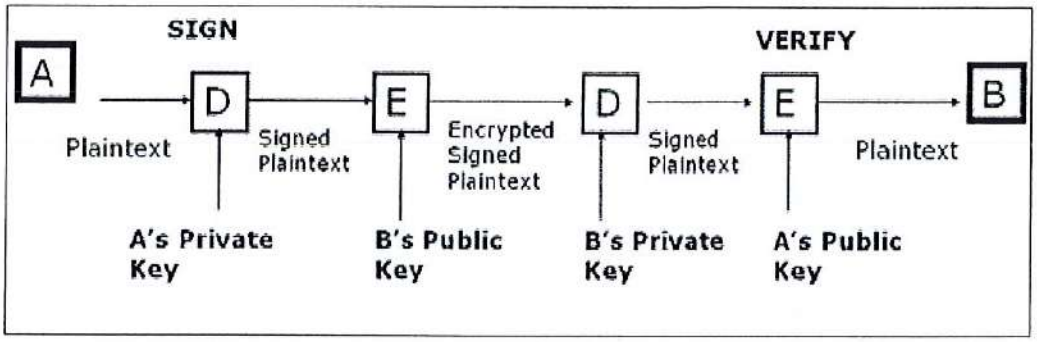

Figure 1 / *Rajah 1*

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? [4 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?

Q5. a) Describe the **three (3)** main concerns with the use of passwords for authentication. Explain what is meant by a social engineering attack on a password. [8 M]
Terangkan ***tiga (3)*** *kebimbangan utama dalam penggunaan katalaluan dalam pengesahan. Terangkan apa yang dimaksudkan dengan serangan kejuruteraan sosial terhadap katalaluan.*

b) List **two (2)** disadvantages of using physical separation in a computing environment. [2 M]
Senaraikan ***dua (2)*** *kelemahan menggunakan pengasingan fizikal dalam persekitaran pengkomputeran.*

c) List the basic steps used to secure the base operating system. [4 M]
Senaraikan langkah-langkah asas yang digunakan untuk mendapatkan sistem operasi asas yang selamat.

Q6. a) When you send messages using the latest version of WhatsApp you received message as shown in Fig 2. What is the meaning of the message?
Note: you need to explain what is end-to-end encryption and how does it work to ensure the security of the message. [5 M]

Apabila anda menghantar mesej menggunakan versi terkini WhatsApp anda menerima mesej seperti dalam Rajah 2. Jelaskan apakah maksud mesej tersebut?

***Nota:** Anda perlu menerangkaan enkripsi hujung-ke-hujung dan bagaimana ia berfungsi untuk memastikan keselamatan mesej.*

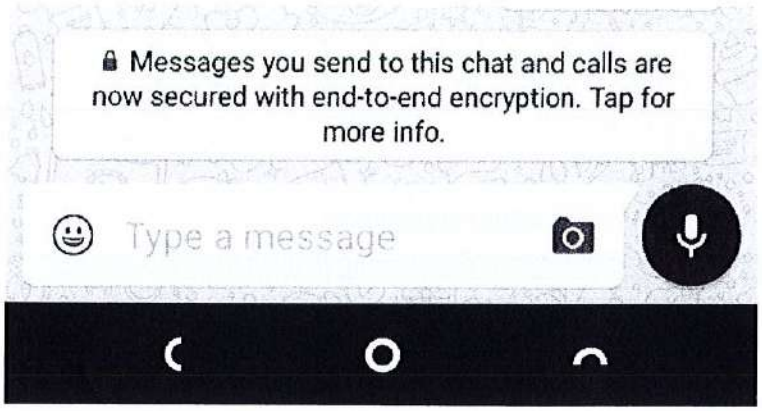

Figure 2 / *Rajah 2*

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, dicuss **two (2)** risks that you would face? [5 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?*

Q7. a) What is buffer overflow? Why is buffer overflow a vulnerability? What can we do to avoid buffer overflow attacks? [6 M]

Apakah limpahan penimbal? Mengapakah limpahan penimbal merupakan satu kelemahan? Apakah yang boleh kita buat untuk mengelak daripada serangan limpahan penimbal?

b) How could a hacker exploit the following program? [2 M]

Bagaimanakah seorang penceroboh dapat mengeksploit aturcara berikut?

```
int login()
{
char username[8];
char hashed_pw[8];
char password[8];
printf("login:"); gets(username);
lookup(username, hashed_pw); /* Put stored hash in hashed_pw */
printf("password:"); gets(password);
if (equal(hashed_pw, hash(password))) return OK;
else return INVALID_LOGIN;
}
```

ANSWER SPACE FOR SECTION A /24 MARKS

RUANG JAWAPAN BAGI BAHAGIAN A /24MARKAH

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

APPENDIX A

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

Mukasurat ini sengaja dibiarkan kosong

[This page is purposely left blank]

Mukasurat ini sengaja dibiarkan kosong

[This page is purposely left blank]