# PENGGUNAAN KAEDAH MATRIKS DALAM ENKRIPSI DAN DEKRIPSI MESEJ

AHMAD SHAFIQ BIN AHMAD TERJUDIN



DISERTASI INI DIKEMUKAKAN UNTUK MEMENUHI SEBAHAGIAN
DARIPADA SYARAT MEMPEROLEHI IJAZAH SARJANA MUDA SAINS
DENGAN KEPUJIAN

PROGRAM MATEMATIK DENGAN KOMPUTER GRAFIK
SEKOLAH SAINS DAN TEKNOLOGI
UNIVERSITI MALAYSIA SABAH

APRIL 2008

PUMS99:1

# UNIVERSITI MALAYSIA SABAH

BORANG PENGESAHAN STATUS TESIS@

JUDUL: PENGGUNAAN KAEDAH MATRIKS DALAM ENKRIPSI DAN DEKRIPSI MESEJ

IJAZAH: SARJANA MUDA SAINS DENGAN KEPUJIAN (MATEMATIK DENGAN KOMPUTER GRAFIK)

SAYA AHMAD SHAFIQ BIN AHMAD TERJUDIN SESI PENGAJIAN: 2007/2008

mengaku membenarkan tesis (LPSM) ini disimpan di Perpustakaan Universiti Malaysia Sabah dengan syarat-syarat kegunaan seperti berikut:-

1. Tesis adalah hakmilik Universiti Malaysia Sabah.
2. Perpustakaan Universiti Malaysia Sabah dibenarkan membuat salinan untuk tujuan pengajian sahaja.
3. Perpustakaan dibenarkan membuat salinan tesis ini sebagai bahan pertukaran antara institusi pengajian tinggi.
4. Sila tandakan ( / )

| | | |
|---|---|---|
| [ ] | SULIT | (Mengandungi maklumat yang berdajah keselamatan atau Kepentingan Malaysia seperti yang termaktub di dalam AKTA RAHSIA RASMI 1972) |
| [ ] | TERHAD | (Mengandungi maklumat Terhad yang telah ditentukan oleh organisasi/badan di mana penyelidikan dijalankan) |
| [ / ] | TIDAK TERHAD | |

Disahkan Oleh

(TANDATANGAN PENULIS)

(TANDATANGAN PUSTAKAWAN)

Alamat tetap: Lot 8164, Lorong Hillview, Desa Perwira, 31350, Ipoh, Perak Darul Ridzuan.

Puan Suzelawati binti Zenian (Penyelia)

Tarikh: 30 / April / 2008

Tarikh: 30 / April / 2008

CATATAN:- @Tesis dimaksudkan sebagai tesis bagi Ijazah Doktor Falsafah dan Sarjana secara penyelidikan atau disertasi bagi pengajian secara kerja kursus dan Laporan Projek Sarjana Muda (LPSM)

## PENGAKUAN

Saya akui karya ini adalah hasil kerja saya sendiri kecuali nukilan dan ringkasan yang setiap satunya telah dijelaskan sumbernya.

**30 April 2008**

AHMAD SHAFIQ BIN AHMAD TERJUDIN

HS2004-2083

**DIPERAKUKAN OLEH**

Tandatangan

1. **PENYELIA**

   ( Pn. Suzelawati Bt. Zenian ) _____

2. **PEMERIKSA 1**

   ( Prof. Madya Dr. Jumat B. Sulaiman ) _____

3. **PEMERIKSA 2**

   ( En. Victor Tiong Kung Ming ) _____

4. **DEKAN**

   ( Supt./Ks. Prof Madya Dr. Shariff A.K.S. Omang ) _____

# PENGHARGAAN

Setinggi-tinggi penghargaan saya ucapkan kepada Puan Suzelawati Zenian diatas kesudian beliau menjadi penyelia saya dan memberikan tunjuk ajar dalam menghasilkan disertasi ini. Terima kasih kerana membantu saya dalam memberikan panduan dan meluangkan masa untuk memberikan penerangan dalam menghasilkan disertasi ini.

Saya juga ingin mengucapkan terima kasih kepada perkhidmatan Perpustakaan Universiti Malaysia Sabah serta kakitangan yang bertugas ke atas khidmat yang diberikan oleh mereka.

Tidak lupa juga, saya ucapkan setinggi-tinggi penghargaan dan terima kasih kepada ibu bapa saya, pensyarah-pensyarah dan rakan-rakan yang telah banyak membantu serta memberikan sokongan dalam penghasilan disertasi ini. Terima kasih juga diucapkan kepada individu-individu yang terlibat secara langsung atau tidak langsung dalam menghasilkan disertasi ini. Terima kasih diucapkan sekali lagi kepada semua yang terlibat.

Sekian, terima kasih.

# ABSTRAK

Kriptografi adalah satu kaedah melindungi maklumat dengan mengubah suatu maklumat asal menjadi satu maklumat yang tidak dapat difahami kecuali oleh pengirim dan penerima yang sah sahaja. Ia mempunyai peranan penting dalam memastikan pertukaran dan perkongsian maklumat adalah selamat dan dilindungi dari diceroboh. Kajian disertasi ini menjurus kepada kajian terhadap sistem kripto yang mengaplikasikan kaedah matriks dalam proses enkripsi dan dekripsi sesuatu mesej. Untuk mencapai objektif kajian, sistem kriptografi yang dikaji adalah kaedah kerahsiaan *Hill*. Kaedah ini merupakan salah satu kaedah dalam sistem kriptografi klasik dan menggunakan tranformasi matriks dalam proses enkripsi, dekripsi dan pembentukan kunci bagi memastikan kerahsiaan sesuatu maklumat adalah terjamin. Operasi-operasi matriks yang digunakan adalah pendaraban matriks, transposisi matriks dan pengiraan matriks songsang dengan menggunakan kaedah eselon baris terturun. Pengiraan juga melibatkan penggunaan aritmetik modulo untuk menghadkan julat perwakilan nilai angka bagi setiap aksara. Enkripsi merupakan proses penyulitan mesej asal kepada mesej rahsia dan dekripsi pula merupakan proses pentafsiran mesej rahsia kepada mesej asal. Proses bermula dengan pembahagian aksara-aksara dalam sesuatu mesej kepada beberapa kumpulan. Seterusnya, aksara-aksara setiap kumpulan akan diwakilkan dengan nilai angka. Bagi proses enkripsi, matriks kunci didarabkan dengan setiap matriks kumpulan dan hasil pendaraban yang diperolehi akan dikurangkan kepada nilai modulo. Nilai-nilai ini kemudiannya akan ditukarkan kembali kepada aksara. Proses yang sama juga digunakan bagi proses dekripsi tetapi matriks yang akan digunakan adalah songsangan matriks kunci dalam bentuk modulo. Kajian juga mengaplikasikan penggunaan pengaturcaraan C dalam membina atur cara yang akan memaparkan mesej rahsia bagi proses enkripsi dan memaparkan mesej asal bagi proses dekripsi. Perisian matematik, *MAPLE 10* digunakan bagi pengiraan songsangan matriks kunci dalam bentuk modulo. Melalui kajian ini, maka dengan jelas telah ditunjukkan bagaimana penggunaan kaedah matriks dalam proses enkripsi dan dekripsi sesuatu mesej.

# APPLICATION OF MATRIX METHOD IN MESSAGE ENCRYPTION AND DECRYPTION

## ABSTRACT

Cryptography is a method of protecting data by making it meaningless to anyone who does not have authorized access to it. It has an important role to ensure information transfer and sharing is secured and protected against threat. This research is focusing on cryptosystem that used matrix method for encryption and decryption process of information. To achieve the research objective, cryptography system that will be studied is the Hill cipher method. Hill cipher is one of the methods in classical cryptography system and uses matrix transformation in encryption process, decryption process and generating key to ensure the secrecy of information is secured. Matrix operations that have been used are matrix multiplication, matrix transposition and calculation of inverse matrix by using row reduced echelon method. Calculation also involves the usage of modular arithmetics to limit the numeric values for each corresponding characters. Encryption is a process of encoding an original message to secret message while decryption is a process of decoding a secret message to original message. This process begins by dividing each character in a message into some number of groups. Then, characters in each group will be replaced by the corresponding numeric value. For encryption process, key matrix is multiplied with each group matrix and the multiplication result will be reduced into modular value. Each value then replaced with the corresponding characters. The same process also used for decryption process but the matrix that been used is inverse of the key matrix in modular form. This research also implements the used of C programming in constructing program that display secret message for encryption process and display original message for decryption process. Mathematical software, *MAPLE 10* is used to calculate the inverse of the key matrix in modular form. This research shows clearly the application of matrix methods in message encryption and decryption.

# ISI KANDUNGAN

Muka Surat

# SENARAI JADUAL

# SENARAI RAJAH

# SENARAI SIMBOL

| | |
|---|---|
| $\forall$ | untuk sebarang |
| $\exists$ | wujud |
| $\in$ | unsur kepada |
| $\ni$ | sedemikian hingga |
| $e$ | 2.718281... |
| $gcd(a, b)$ | pembahagi sepunya terbesar |
| $\mathbb{Z}_n$ | aritmetik modulo $n$ |
| mod $n$ | modulo $n$ |
| $\rightarrow$ | jika maka |
| $\leftrightarrow$ | jika hanya jika |
| $\geq$ | lebih besar atau sama dengan |
| $\leq$ | kurang atau sama dengan |
| $=$ | sama dengan |
| $\neq$ | tidak sama dengan |
| $\equiv$ | kongruen |
| $a_{ij}$ | unsur baris ke-$i$ dan lajur ke-$j$ |
| $m \times n$ | peringkat bagi matriks ( $baris \times lajur$ ) |
| $\sum$ | hasil tambah |
| $x^{-1}$ | songsang bagi $x$ |
| $I$ | identiti |
| $\lvert A \rvert$ | penentu bagi $A$ |
| $n\|a$ | $a$ membahagi $n$ |

## SENARAI ISTILAH

| | |
|---|---|
| *Array* | Tatasusunan |
| *Affine Cipher* | Kerahsiaan Affine |
| *Automated Teller Machines (ATM)* | Mesin Juruwang Automatik |
| *Character* | Aksara |
| *Cipher* | Kaedah penulisan rahsia (*kerahsiaan*) |
| *Decryption* | Dekripsi |
| *Display* | Paparan |
| *Digital Foot-Print* | Tapak-Kaki Digital |
| *Digital Signature* | Tandatangan Digital |
| *Encryption* | Enkripsi |
| *Hackers* | Penggodam |
| *Hill Cipher* | Kerahsiaan Hill |
| *Interface* | Pengantaramukaan |
| *Object-Oriented* | Berorientasikan Objek |
| *Password* | Kata Laluan |
| *PC - Banking* | Perbankan Komputer Peribadi |
| *Private-Key* | Kunci Persendirian |
| *Public-Key* | Kunci Awam |
| *Preprocessor* | Prapemproses |
| *Program* | Atur Cara |
| *Programmer* | Pengaturcara |
| *Programming* | Pengaturcaraan |
| *Row Reduced Echelon (RRE)* | Eselon Baris Terturun (EBT) |
| *Shift Cipher* | Kerahsiaan Pemindahan |
| *Software* | Perisian |
| *Standard Header* | Pengepala Piawai |
| *Standard Identifier* | Pencam Piawai |
| *Standard Library* | Pustaka Piawai |
| *Substitution Cipher* | Kerahsiaan Penggantian |
| *Vignere Cipher* | Kerahsiaan Vignere |

# BAB 1

# PENDAHULUAN

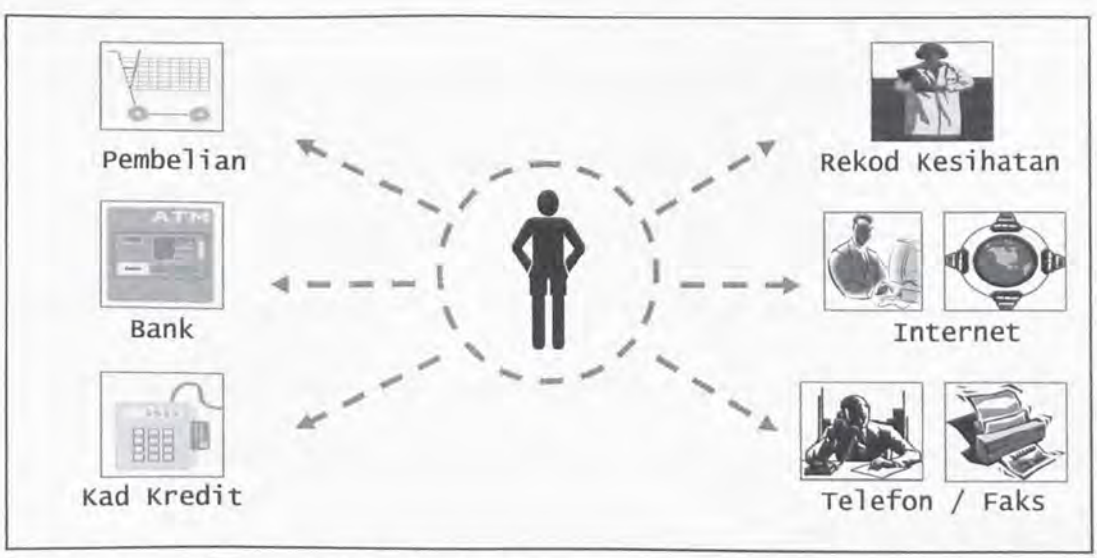
## 1.1 Pengenalan

Perkembangan teknologi global yang semakin pesat pastinya memerlukan suatu mekanisma yang dapat bergerak seiring dengan perkembangan teknologi itu sendiri. Tanpa hala tuju yang sama, sudah pasti kelemahan dalam sesuatu mekanisma yang terdahulu tidak dapat diatasi.

Dalam konteks teknologi maklumat khususnya, kita sedia maklum bahawa teknologi maklumat merupakan salah satu cabang teknologi yang mempunyai kadar perkembangan yang sangat pantas. Dalam cabang teknologi ini, dunia dari sudut capaian maklumat menjadi semakin kecil atau dalam kata lain "Dunia tanpa sempadan" atau "Maklumat di hujung jari". Dalam era ini, sudah pastinya maklumat boleh didapati dengan sangat mudah. Pertukaran maklumat antara penerima dan penghantar maklumat akan berlaku di mana-mana sahaja. Oleh itu, satu mekanisma diperlukan untuk melindungi maklumat yang dihantar oleh penghantar kepada penerima supaya pertukaran maklumat yang berlaku hanya melibatkan individu

tertentu sahaja tanpa diketahui oleh individu yang tidak terlibat. Apabila masyarakat semakin maju seiring dengan perkembangan teknologi itu sendiri, maka keperluan kepada mekanisma atau kaedah yang dapat melindungi maklumat dari diceroboh adalah semakin meningkat.

Pada era ini, kebanyakan komunikasi yang berlaku meninggalkan kesan yang direkod atau dikenali sebagai kesan tapak kaki digital. Sebagai contoh, komunikasi melalui talian telefon, termasuklah faks dan mesej e-mail, menghasilkan rekod nombor yang dihubungi dan masa panggilan dilakukan. Transaksi kewangan, maklumat perubatan dan juga pembelian barang-barang misalnya boleh dikesan melalui resit kad kredit ataupun rekod insurans. Setiap kali seseorang itu menggunakan telefon atau kad kredit, syarikat telefon atau institusi kewangan akan menyimpan rekod nombor yang dihubungi atau jumlah transaksi, tempat dan tarikh ia dilakukan. Pada masa hadapan, dengan jaringan telefon yang menjadi digital, tidak mustahil perbualan yang berlaku juga akan direkod dan disimpan. Secara tidak langsung, sudah semestinya ia akan mengakibatkan kehilangan hak peribadi.




**Rajah 1.1** Kesan tapak kaki digital.

Dengan dunia yang menjadi semakin kecil dalam konteks capaian maklumat, maka permintaan untuk kemudahan informasi dan elektronik berkembang dengan pesat, dan dengan permintaan yang semakin meningkat tersebut maka kebergantungan kepada sistem elektronik juga semakin meningkat. Teknik yang diperlukan untuk melindungi maklumat ini tergolong dalam bidang kriptografi. Kriptografi adalah alat yang boleh memastikan hak peribadi seseorang dilindungi sepenuhnya.

### 1.1.1 Kriptografi

Perkataan kriptografi berasal dari perktaan Greek iaitu "*kriptos*" yang bermaksud rahsia dan "*graphos*" yang bermaksud menulis (Whitman & Mattord, 2003). Kriptografi adalah satu kajian untuk merekacipta suatu sistem yang dapat mengubah suatu maklumat asal menjadi satu maklumat yang tidak dapat difahami kecuali oleh pengirim dan penerima sahaja. Sistem yang menggunakan kaedah kriptografi dinamakan sebagai sistem kriptografik (Buchanan, 2000).

Kriptografi sebenarnya telah lama wujud dan telah digunakan semasa era kebangkitan Rom lagi (Lampiran B). Contohnya sistem kod rahsia yang digunakan oleh Julius Caeser untuk menghantar mesej semasa berlakunya peperangan Gallic supaya mesej yang dihantar tidak diketahui musuh. Dalam kaedah enkripsi Caeser ini yang diberi sempena nama Julius Caeser, setiap huruf dalam perkataan asal akan ditukar dengan tiga huruf seterusnya. Contohnya, huruf *ABC* yang melalui proses enkripsi Caeser akan menjadi *DEF* (Trappe & Washington, 2002). Selain itu, dalam perang dunia pertama dan kedua, penggunaan kod rahsia juga dipraktikkan.

Contohnya ialah sistem-sistem seperti kod *ENIGMA* yang digunakan oleh tentera Jerman dan *PURPLE* yang digunakan oleh tentera Jepun (Joyner, 2000).

Kriptografi adalah mekanisma yang paling kuat dalam mengawal pelbagai ancaman keselamatan kerana data yang melalui proses enkripsi tidak akan dapat dibaca dan diubahsuai (Obimbo & Salami, 2007). Kriptogafi moden banyak melibatkan kaedah-kaedah dalam matematik dan sains komputer. Pada asasnya bidang ini terbahagi kepada tiga nama iaitu kriptografi, kriptologi, dan kriptalisis. Secara teknikal, kriptologi adalah kajian tentang sistem untuk komunikasi rahsia. Proses untuk merekacipta sistem komunikasi rahsia dipanggil kriptografi. Manakala kriptalisis pula melibatkan kajian tentang cara atau langkah untuk memecahkan komunikasi rahsia tersebut (Sedgewick, 1990).

Kaedah-kaedah atau cara untuk melakukan proses enkripsi bukan sesuatu yang unik. Malah, terdapat berbagai-bagai kaedah yang digunakan dalam bidang ini. Salah satu andaian yang paling penting dalam kriptografi moden adalah Prinsip Kerckhoffs yang menyatakan dalam memastikan suatu sistem kripto adalah selamat dari ancaman musuh, kita perlulah mengandaikan bahawa musuh mengetahui kaedah yang digunakan. Prinsip ini dinyatakan oleh Auguste Kerckhoffs pada tahun 1883 dalam karangan klasik beliau yang bertajuk *La Cryptographic Militaire* (Trappe & Washington, 2002). Maka, keselamatan sesuatu sistem perlulah berpandukan kepada kunci bagi proses enkripsi atau dekripsi dan bukannya semata-mata kepada algoritma yang digunakan.

Jika dilihat pada masa kini, yang mana kebergantungan kepada internet semakin menjadi pilihan dalam pelbagai urusan seharian, kita dapat lihat bagaimana penggunaan kata laluan yang berperanan sebagai kunci merupakan salah satu mekanisma penting dalam memastikan keselamatan maklumat peribadi daripada diceroboh atau dicuri oleh pihak yang tidak bertanggungjawab. Perubahan dalam teknologi juga telah memberikan impak yang besar ke atas perkembangan ekonomi secara global khususnya kepada institusi kewangan dan perdagangan. Lantaran itu, wujudnya saluran alternatif perkhidmatan kewangan melalui perbankan elektronik seperti mesin-juruwang automatik, perbankan telefon, perbankan komputer peribadi dan perbankan internet sebagai alat pemudah cara (Noriza & Haslinda, 2006).

Dalam memastikan sesuatu urusniaga elektronik adalah selamat, kriptografi memainkan peranan penting dalam melindungi sistem perbankan dunia dan syarikat-syarikat yang mengamalkan perdagangan elektronik atau "E-dagang". Kebanyakkan bank dan institusi kewangan menjalankan perniagaan melalui jaringan terbuka seperti internet (Stallings, 2003). Contohnya dalam urusniaga yang melibatkan kad kredit, kita dapat lihat bagaimana pemindahan wang dan jual beli berlaku dengan banyak sekali secara elektronik melalui internet. Contohnya dalam perkhidmatan yang digunakan oleh syarikat-syarikat terkemuka seperti "*Air Asia*" dan "*Maybank*". Sistem pembelian tiket secara atas talian yang digunakan oleh syarikat penerbangan *Air Asia* misalnya melibatkan sepenuhnya pembayaran dengan menggunakan kad kredit melalui laman webnya. Syarikat *Maybank* pula, telah memperkenalkan urusan kewangan atas talian melalui aplikasi "*Maybank2u*" yang memudahkan pengguna melakukan urusan kewangan secara atas talian (Noriza & Haslinda, 2006). Bagaimanakah syarikat-syarikat ini menjamin keselamatan maklumat-maklumat yang

dihantar oleh pengguna secara atas talian? Jawapannya adalah kriptografi, yang mana semua maklumat akan dilindungi dengan suatu mekanisma yang mana hanya pihak yang berurusan sahaja akan dapat mengetahui maklumat-maklumat yang dikongsi.

Dengan sistem kriptografi, data yang dihantar yang melibatkan urusniaga kewangan adalah selamat dan terjamin. Tetapi harus diingat bahawa sistem yang sedia ada perlulah dipertingkatkan bagi memperkuatkannya daripada diceroboh. Kriptografi sebenarnya memainkan peranan yang sangat penting pada masa kini dan akan datang kerana maklumat yang dihantar juga melibatkan maklumat peribadi atau sulit yang sudah semestinya perlu dilindungi dari diceroboh oleh individu ketiga atau musuh yang tidak terlibat dalam rangkaian maklumat tersebut.

### 1.1.2 Takrifan Proses Enkripsi Dan Dekripsi

Kriptografi melibatkan dua proses utama, iaitu enkripsi dan dekripsi. Kedua-dua proses ini memainkan peranan penting dalam melindungi maklumat dan saling berkait antara satu sama lain. Setiap sistem kripto mempunyai kaedah enkripsi dan dekripsi yang tersendiri dan berbeza antara satu sama lain. Berikut adalah takrifan umum bagi proses enkripsi dan dekripsi.

**a. Enkripsi**

- Enkripsi adalah proses mengubah mesej atau maklumat ke dalam bentuk yang tidak dapat difahami (Stallings, 2003).

**b. Dekripsi**

- Dekripsi adalah proses untuk mentafsir mesej yang telah melalui proses enkripsi (mesej rahsia) ke dalam bentuk yang dapat difahami (mesej asal). Tanpa proses dekripsi, mesej yang telah melalui proses enkripsi tidak akan dapat difahami (Stallings, 2003).

### 1.1.3 Kegunaan Kriptografi

Kriptografi mempunyai banyak kegunaan terutamanya dalam melindungi maklumat dari ancaman penceroboh dan musuh. Berikut adalah beberapa aplikasi kriptografi (Trappe & Washington, 2002):

**a. Tandatangan digital**

Digunakan apabila kita mahu menandatangani maklumat elektronik. Tidak seperti tandatangan biasa yang boleh ditiru dan dibuang dari maklumat asal. Tandatangan digital tidak akan dapat dipisahkan dari mesej asal dan individu yang telah menandatangani tidak akan dapat menyangkal tandatangan yang telah dibuat.

**b. Pengesahan identiti**

Apabila mendaftar masuk ke dalam mesin atau mengaktifkan laluan komunikasi, pengguna perlu mengesahkan identiti dengan memasukkan nama pengguna dan kata

laluan. Penggunaan kriptogafi adalah dalam menjana dan menjamin keselamatan kata laluan yang digunakan dalam mengesahkan identiti pengguna.

**c. E-dagang**

Memastikan keselamatan sesuatu maklumat dalam mengendalikan perdagangan elektronik melalui internet khususnya adalah sangat penting. Penggunaan kad kredit misalnya adalah amat berguna dalam perdagangan elektronik. Kriptografi akan melindungi maklumat yang dipindahkan dari ancaman musuh atau penjenayah siber. Disamping itu ia juga melindungi hak peribadi pengguna.

### 1.1.4 Keselamatan Kata Laluan

Apabila seseorang mendaftar masuk ke dalam komputer dan memasukkan kata laluan, komputer akan memeriksa kata laluan yang dimasukkan dan akan memberikan kebenaran masuk sekiranya kata laluan yang dimasukkan adalah benar.

Bagi memastikan kata laluan yang dimasukkan tidak diketahui oleh orang lain, kata laluan tersebut perlulah dienkripsikan dahulu sebelum disimpan dalam fail *kata laluan* komputer. Katakan $f(x)$ adalah fungsi satu arah. Ini bermakna, adalah mudah untuk mengira $f(x)$, tetapi adalah sangat sukar untuk menyelesaikan $y = f(x)$ untuk sebarang $x$. Kata laluan $x$ seterusnya boleh disimpan sebagai $f(x)$, bersama dengan nama pengguna. Apabila pengguna mendaftar masuk dan memasukkan kata laluan $x$, komputer akan mengira $f(x)$ dan memeriksa samada nilai $f(x)$ adalah berpadanan

dengan nilai $f(x)$ pengguna. Penyimpanan nilai $f(x)$ dalam fail *kata laluan* akan dilakukan oleh komputer semasa pengguna menjana nama pengguna dan kata laluan.

Sekiranya penceroboh memperolehi fail *kata laluan*, penceroboh hanya akan memperolehi nilai $f(x)$ dan bukannya nilai $x$ (kata laluan pengguna). Ini kerana komputer akan hanya menyimpan nilai $f(x)$ dan bukannya nilai $x$. Walaupun penceroboh mengetahui nama pengguna, tetapi kata laluan yang berpadanan dengan nama pengguna tidak akan dapat dikira (Trappe & Washington, 2002).

## 1.2 Objektif Kajian

Daripada bahagian pengenalan yang telah menerangkan beberapa konsep dan kegunaan kriptografi, objektif utama kajian disertasi ini adalah:

a. Mengkaji jenis-jenis sistem kripto.

- Jenis-jenis sistem kripto akan dikaji bagi mendapatkan pemahaman secara umum mengenai jenis-jenis sistem kripto dan contoh sistem-sistem kripto lain di bawah jenis-jenis sistem kripto ini.

b. Mengkaji penggunaan kaedah matriks dalam enkripsi dan dekripsi mesej.

- Proses enkripsi dan dekripsi mesej yang menggunakan kaedah matriks akan dikaji bagi mengetahui penggunaan kaedah-kaedah matriks yang terlibat dalam proses tersebut.

c. Menggunakan pengaturcaraan C untuk membuat atur cara yang dapat menjalankan proses enkripsi dan dekripsi mesej.

- Atur cara yang menjalankan proses enkripsi dan dekripsi akan dibina. Atur cara ini akan memaparkan mesej asal apabila proses dekripsi dipilih dan memaparkan mesej rahsia apabila proses enkripsi dipilih.

## 1.3 Skop Kajian

Dalam kajian disertasi ini, skop yang dikaji adalah menjurus kepada proses enkripsi dan dekripsi dengan menggunakan kaedah matriks khususnya dalam kaedah kerahsiaan Hill. Kaedah-kaedah matriks yang akan digunakan adalah pendaraban matriks, matriks songsang dan eselon baris terturun. Saiz matriks yang terlibat adalah bergantung kepada saiz matriks kunci yang dipilih dan bagi kajian disertasi ini saiz matriks akan dihadkan kepada matriks berperingkat $5\times5$ dan $5\times1$ kerana setiap mesej akan dibahagikan kepada beberapa kumpulan yang setiapnya terdiri daripada lima huruf bagi setiap kumpulan. Pengiraan yang menggunakan operasi matriks akan melibatkan aritmetik modulo dan dihadkan kepada modulo 95 kerana sebanyak 95 aksara yang berlainan akan digunakan dalam proses enkripsi dan dekripsi. Kajian juga menjurus kepada kaedah yang melibatkan penukaran aksara di dalam suatu perkataan kepada nilai-nilai angka atau sebaliknya. Pengaturcaraan C akan digunakan dalam menghasilkan atur cara yang dapat melakukan proses enkripsi serta dekripsi bagi mendapatkan mesej asal dari mesej rahsia atau sebaliknya. Perisian matematik Maple digunakan bagi menyelesaikan pengiraan matriks songsang dalam bentuk modulo.

# BAB 2

# ULASAN PERPUSTAKAAN

## 2.1 Sejarah Kriptografi

Kriptografi telah bemula sejak dari zaman dahulu lagi (Lampiran B). Salah satu sistem kripto yang paling awal adalah pada zaman kebangkitan Rom yang digunakan oleh Julius Caesar untuk mengubah susunan huruf dalam perkataan supaya perkataan yang dihantar tidak diketahui musuh semasa peperangan (Trappe & Washington, 2002).

Semasa perang dunia pertama dan kedua pula, penggunaan kod-kod rahsia adalah sangat meluas. Contohnya adalah *PURPLE*, iaitu sistem diplomatik Jepun dan *ENIGMA*, iaitu mesin kriptografik tentera Jerman (Joyner, 2000). Kriptografi merupakan satu bidang yang memerlukan kajian yang berterusan kerana sistem yang dihasilkan pastinya akan cuba dipecahkan dan sering terdedah kepada ancaman.

Pada tahun 1949 iaitu melalui penerbitan kertas kerja oleh Shannon yang bertajuk *Communication Theory of Secrecy Systems* lebih menjurus kepada era kunci-

# RUJUKAN


Bergin, T. J. & Gibson, R. G. 1996. *History of Programming C Languages*. ACM Press & Addison-Wesley, New York.

Bronson, R. 1991. *Matrix Method: An Introduction*. Ed. ke-2. Academic Press, California.

Buchanan J. A. 2000. *Introduction to Cryptography*. Springer-Verlag, New York.

Fook, L. 1996. *Matrik dan Penentu*. Ed. ke-2. Pusat Pendidikan Jarak Jauh Universiti Sains Malaysia, Pulau Pinang & Dewan Bahasa dan Pustaka, Kuala Lumpur.

Gong, L. & Wheeler, D. J. 1990. A Matrix Key-Distribution Scheme. *Journal of Cryptology* **2**, ms. 51-59. http://www.springerlink.com/content/735p8702mg0g0147/fulltext.pdf

Habsah Abdullah, Halimah Hasan, Halinah Atan, Maslin Masrom & Noraniah Mohd Yassin (ptrj). 2000. *C untuk pengatucara*. Universiti Teknologi Malaysia, Skudai.

Howell, J. & Sussenbach, R. 2003. *C Programming Student Workbook*. http://www.itcourseware.com/Webpdfs/webc.pdf

Joyner, D. 2000. *Coding Theory and Cryptograhy: From enigma and Geheimschreiber to Quantum Theory*. Springer-Verlag, New York.

Koblitz, N. 1999. *Algebraic Aspects of Cryptography*. Ed. ke-2. Springer-Verlag, Berlin.

Kolman, B. & Hill, D. R. 2001. *Introductory Linear Algebra: Applied First Course*. Ed. ke-8. Pearson Prentice Hall, New Jersey.

Noriza Mohd. Jamal & Haslinda Kono Jamil. 2006. Tahap Penggunaan dan Halangan Perbankan Internet (Maybank2u) Di Kalangan Pelanggan. *Jurnal Kemanusiaan* **8**, ms. 25-33. http://www.fppsm.utm.my/jurnal/JK8DO6/JK8_NORIZAJAMAL.pdf

Obimbo, C. & Salami, B. 2007. A Parallel Algorithm for determining the inverse of a matrix for use in blockcipher in encryption/decryption. *Journal of Supercomputer* **39**, ms. 113-130. http://www.springerlink.com/content/w2581578w7p16546/fulltext.pdf

Sedgewick, R. 1990. *Algorithm in C*. Addison-Wesley, New York.

Stallings, W. 2003. *Cryptography and Network Security: principle and practice*. Prentice-Hall, New Jersey.

Standish, T. A. 1994. *Data Structure, Algorithms & Software Principle in C*. Addison-Wesley, New York.

Stinson, D. R. 1995. *Cryptography: theory and practice*. CRC Press, Florida.

Trappe, W. & Washington, L. C. 2002. *Introduction to Cryptography with Coding Theory*. Prentice-Hall, New Jersey.

Sastry, V. U. K, Kumar, S. U & Babu, A. V. 2006. A Large Block Cipher Using Modular Arithmetic Inverse of a Key Matrix and Mixing of the Key Matrix and the Plaintext. *Journal of Computer Science* **2** (9), ms. 698-703. http://www.scipub.org/fulltext/jcs/jcs29698-703.pdf

Whitman, M. E. & Mattord, H. J. 2003. *Principle of Information Security*. Thomson Course Technology, Massachusetts.

Yeh, Y. S, Wu, T. C, Chang, C. C & Yang, W. C. 1991. New Cryptosystem Using Matrix Transformation. *Proceedings 25th Annual 1991 IEEE International*

*Carnahan Conference*, 10 Januari1991 – 10 Mac 1991, Taipei, Taiwan, ms. 131-138. http://ieeexplore.ieee.org/iel2/575/5225/00202204.pdf?tp=&is number=&arnumber=202204

Yoong, W. K. 1985. *Matriks*. Dewan Bahasa dan Pustaka, Kuala Lumpur.