UNIVERSITI PUTRA MALAYSIA

SISTEM KRIPTO LUC UNTUK PENGESAHAN APLIKASI TELNET

SITI JAUYAH BTE SIBO @ HJ MOHAMED OSMAN

FSKTM 1999 4

SISTEM KRIPTO LUC UNTUK PENGESAHAN APLIKASI *TELNET*

Oleh

SITI JAUYAH BTE SIBO @ HJ MOHAMED OSMAN

Tesis ini dikemukakan sebagai memenuhi keperluan bagi mendapatkan
Ijazah Master Sains di Fakulti
Sains Komputer dan Teknologi Maklumat
Universiti Putra Malaysia

Ogos 1999

PENGHARGAAN

Dengan nama Allah Yang Maha Pemurah Lagi Maha Mengasihani. Dipanjatkan kesyukuran ke hadrat Illahi, selawat dan salam ke atas junjungan besar Nabi Muhammad s.a.w. serta para sahabat baginda.

Setinggi-tinggi penghargaan dan terima kasih yang tidak terhingga dirakamkan kepada Jawatankuasa Penyeliaan yang dipengerusikan oleh Dr. Ramlan Mahmod dan ahli-ahli yang terdiri daripada Dr. Mohamad Rushdan Md Said dan Dr. Hajjah Fatimah Dato' Ahmad di atas segala tunjuk ajar, galakan, cadangan, komen, nasihat dan pertimbangan di sepanjang kajian ini.

Rakaman terima kasih juga kepada semua yang terlibat secara langsung dan tidak langsung terutamanya Major Sabri, Lt. Saidin, En. Azuddin, En. Mahizzan, Dr. Hishamuddin Zainuddin, Pn. Rohaya, Pn. Norhayati Abdullah, Pn. Zaiton Muda, Cik Ummu, Cik Adawiyah, En. Nordin, Im dan semua rakan-rakan dan kakitangan Fakulti Sains Komputer dan Teknologi Maklumat.

Terima kasih yang tidak terhingga untuk suami di atas segala tunjuk ajar, bantuan, dorongan serta semangat yang diberikan. Terima kasih juga untuk anak-anak yang memahami dan Rob serta Izam yang banyak membantu.

Akhir sekali rakaman terima kasih kepada Jabatan Perkhidmatan Awam yang telah memberi tajaan dan cuti belajar bagi menyempurnakan pengajian saya.

KANDUNGAN

Muka Surat

SENARAI JADUAL

SENARAI RAJAH

SENARAI SINGKATAN

CA	-	*Certification Authority*
CPU	-	*Central Processing Unit*
DES	-	*Data Encryption Standard*
GNU	-	*GNU's Not Unix*
IBM	-	*International Business Machines*
LUC	-	Sistem Kripto berasaskan fungsi Lucas
MB	-	*Mega Byte*
MIT	-	Massachusetts Institute of Technology
MIRACL	-	*Multi-precision Integer Arithmetic in C Language*
MHz	-	Mega Hertz
NATO	-	*North Atlantic Treaty Organization*
RAM	-	*Random Access Memory*
RSA	-	Rivest Shamir dan Adleman
SHA	-	*Secure Hash Algorithm*
VLSI	-	*Very Large Scale Integration*

Abstrak tesis yang dikemukakan kepada Senat Universiti Putra Malaysia sebagai memenuhi keperluan untuk Ijazah Master Sains.

SISTEM KRIPTO LUC UNTUK PENGESAHAN APLIKASI *TELNET*

Oleh

SITI JAUYAH BT SIBO @ HJ MOHAMED OSMAN

Ogos 1999

Pengerusi: **Ramlan Mahmod, Ph.D**

Fakulti: **Sains Komputer dan Teknologi Maklumat**

Tesis ini membincangkan perbandingan antara dua sistem kripto kunci awam iaitu sistem kripto Rivest-Shamir-Adleman, RSA dan sistem kripto berasaskan fungsi Lucas, LUC. Perbandingan dibuat untuk aspek-aspek pelaksanaan dan keselamatan. Bagi aspek pelaksanaan, proses penjanaan kunci kriptografi, penyulitan, penyahsulitan, tandatangan digital dan pengesahbetulan tandatangan digital dikaji. Bagi aspek keselamatan pula, kriptanalisis yang telah diterbitkan daripada segi protokol pelaksanaan dan ketakbolehramalan penjana nombor rawak RSA dan LUC dikaji.

Jujukan nombor rawak yang dihasilkan oleh penjana sistem kripto RSA dan LUC telah dikaji dan dibandingkan dengan menggunakan kaedah jelmaan *Fourier*. Hasil eksperimen menggunakan sehingga enam digit modulus menunjukkan kedua-dua penjana nombor rawak RSA dan LUC mempunyai ciri

yang hampir sama. Dengan itu kedua-dua sistem kripto tersebut mempunyai tahap kekriptografian yang agak setara.

Sistem kripto LUC dipilih sebagai algoritma kriptografi untuk membangunkan prototaip sistem pengesahan aplikasi *telnet* dalam persekitaran sistem pengoperasian Linux. Prototaip yang dibangunkan menyediakan sistem pengesahan dua hala. Semasa sidang pengesahan, tantangan nombor rawak yang dijana oleh pengesah betul dikaitkan dengan pengecam pihak pendakwa. Pihak pendakwa akan menjana tandatangan digital ke atas tantangan sebagai kiriman balas sidang berkenaan. Untuk mengesah betul tandatangan digital, pihak pengesah betul akan menggunakan kunci awam yang berkaitan dengan pengecaman pihak pendakwa. Jika kunci awam tersebut berjaya mengesah betul tandatangan digital pada tantangan tersebut, maka pihak pendakwa adalah sah.

Abstract of thesis presented to the Senate of Universiti Putra Malaysia in fulfilment of the requirements for the degree of Master of Science.

LUC CRYPTOSYSTEM FOR TELNET APPLICATION AUTHENTICATION

By

SITI JAUYAH BT SIBO @ HJ MOHAMED OSMAN

August 1999

Chairman: **Ramlan Mahmod, Ph.D**

Faculty: **Computer Science and Information Technology**

This thesis discusses the comparison between two public key cryptosystems i.e. Rivest-Shamir-Adleman, RSA cryptosystem and cryptosystem based on Lucas function, LUC. Comparisons are made with respect to the implementation and security aspects. On the implementation aspect, key generation, encryption, decryption, digital signature creation and signature verification are studied. The security aspect covers the study of published cryptanalysis on the implementation protocol and of the unpredictability of the RSA and LUC random number generator.

Sequence numbers generated by the RSA and LUC generators have been analysed and compared using the fourier transform method. Experiments involving

up to six digits modulus show that both RSA and LUC random number generators have the same characteristic and hence cryptographically equal.

LUC cryptosystem has been chosen as the cryptographic algorithm for the telnet application authentication system prototype in Linux operating system environment. The developed prototype provides mutual authentication. During an authentication exchange, a random number generated by the verifier as a challenge is associated with the claimants identifier. The claimant then generates a signature on that challenge, which is freshly generated for that particular event. In order to verify a signature, the verifier uses the claimant's public key. If that public key can be used to successfully verify the claimant's signature on that challenge, then the claimant is authentic.

BAB I

PENGENALAN

Pendahuluan

Perkembangan penggunaan rangkaian yang semakin meluas pada hari ini, menjurus kepada peri mustahaknya untuk mengesahkan identiti pengguna-pengguna sistem dengan tepat. Sistem yang tidak berkemampuan untuk membezakan di antara permintaan untuk perkhidmatan oleh pengguna sah dan percubaan capaian yang tidak dibenarkan adalah tergugat kepada beberapa serangan. Istilah pengguna bagi sistem pengesahan adalah meliputi pengguna manusia, sistem pengkomputeran dan proses-proses yang dilaksanakan pada sistem berkenaan.

Terdapat beberapa kaedah yang boleh digunakan untuk mengesah betul pengguna. Empat kategori kaedah yang biasa digunakan adalah berdasarkan kepada *sesuatu yang diketahui*, seperti menggunakan kata laluan; *sesuatu yang dimiliki,* seperti menggunakan token; *sifat-sifat fizikal*, seperti menggunakan cap jari atau pengecaman suara; dan *tindakan luar kawalan*, seperti menggunakan tandatangan (Davies dan Price, 1989; Jackson dan Hruska, 1992). Kategori *sifat-sifat fizikal* dan *tindakan luar kawalan* biasanya digabungkan sebagai biometrik. Kaedah biometrik adalah khusus untuk mengesah betul pengguna manusia.

Model pengesahan menggunakan kaedah kata laluan adalah yang paling lazim dan sehingga kini masih digunakan. Pengguna memberikan kata laluan kepada hos untuk disah betul. Kebiasaannya hos akan melakukan fungsi sehala (Diffie dan Hellman, 1976) terhadap kata laluan dan membandingkan hasil tersebut dengan nilai yang berkaitan dengan pengguna berkenaan, yang tersimpan di dalam hos. Jika kedua-dua nilai ini adalah setara maka hos akan sah betul identiti pengguna berkenaan. Beberapa faktor mempengaruhi tahap keselamatan sistem pengesahan menggunakan kaedah kata laluan seperti komposisi, panjang, jangka masa digunakan dan cara penyimpanan. Kelebihan utama menggunakan kaedah kata laluan dalam pengesahan ialah membolehkan ianya dilaksanakan sepenuhnya oleh perisian. Model pengesahan menggunakan kaedah kata laluan ini memadai untuk sistem tersendiri dalam persekitaran yang selamat dengan kata laluan yang dihantar akan bergerak pada jarak yang berdekatan, daripada terminal pengguna terus kepada hos.

Identiti pengguna boleh juga dibuktikan dengan memiliki sesuatu objek unik yang dikenali sebagai token. Sebagai contoh dalam kehidupan harian adalah penggunaan lesen memandu atau kad pengenalan. Dalam pengesahan berautomasi, token dikod dengan maklumat pengguna yang akan digunakan oleh protokol pengesahan dalam mengesah betul identiti pengguna. Kebiasaannya token ini mengandungi ingatan semikonduktor yang berupaya melaksanakan protokol pengesahan. Kekuatan sistem pengesahan menggunakan kaedah token adalah bergantung kepada kepayahan pihak musuh untuk memalsukan token (Jackson dan Hruska, 1992).

Sesetengah anggota badan manusia mempunyai ciri yang unik yang dapat membezakan di antara satu individu dengan yang lain. Pengesahan biometrik adalah pengukuran sifat biologi yang unik yang digunakan untuk mengesahkan identiti seseorang secara automatik. Biometri yang biasa digunakan adalah pengecaman cap jari, mata dan suara. Mekanisme pengesahan biometrik mempunyai dua fasa, iaitu kemasukan dan pengesahan. Sebelum menggunakan sistem, setiap pengguna perlu melalui proses kemasukan dengan pengurus sistem akan mengesahkan setiap pengguna yang mendaftar. Proses ini menyimpan sifat biologi yang akan digunakan untuk mengecam identiti pengguna berkenaan. Algoritma perbandingan digunakan untuk menentukan individu yang disah benar adalah individu yang setara semasa fasa kemasukan.

Kaedah kata laluan, token dan biometrik adalah sasaran kepada beberapa serangan. Sebagai contoh, kata laluan yang digunakan oleh seseorang boleh diteka; token pula boleh dicuri atau dipalsukan. Salah satu langkah yang boleh digunakan untuk meningkatkan tahap keselamatan sistem pengesahan adalah dengan menggunakan kombinasi teknik-teknik pengesahan. Sistem pengesahan bertoken misalnya, memerlukan pengguna memasukkan kata laluan untuk membolehkan token berfungsi. Dengan cara ini, token yang dicuri atau dipalsukan tidak dapat digunakan selagi kata laluan bagi token tersebut tidak diperolehi.

Pengesahan yang selamat adalah teknik yang membenarkan entiti-entiti menyediakan bukti yang mereka mengetahui sesuatu rahsia tanpa mempamerkan rahsia berkenaan. Dengan kaedah ini pihak kedua tidak mengetahui rahsia dan

mengelakkan penggunaan rahsia berkenaan untuk menyamar sebagai entiti tersebut.

Latar Belakang Masalah

Keselamatan sistem komputer pada masa lampau adalah lebih mudah dikawal kerana sistem komputer pada masa itu lazimnya dipasang di dalam pusat pemprosesan komputer. Oleh kerana terminal-terminal yang digunakan untuk mencapai komputer juga terletak di dalam bangunan yang sama, hanya pengguna-pengguna yang boleh memasuki bangunan tersebut sahaja boleh menggunakan terminal tersebut. Dengan perkembangan pesat teknologi rangkaian kawasan luas (WAN) seperti Internet, tahap kawalan capaian fizikal sedemikian tidak lagi selamat.

Pengguna-pengguna komputer pada dekad ini menggunakan kemudahan daripada pelbagai mesin, melalui log masuk jauh *rlogin* atau *telnet*. Seterusnya mereka menggunakan perkhidmatan yang disediakan oleh mesin jauh seperti capaian kepada fail-fail dan pencetak. Persekitaran sedemikian memerlukan teknik pengesahan yang lebih canggih dan selamat. Kaedah-kaedah pengesahan yang lazim digunakan tidak lagi selamat kerana rangkaian bukan sahaja menjadikan pengesahan pengguna bertambah sukar malah memudahkan pihak yang tidak diizinkan untuk melakukan pengintipan dawai ke atas data pengesahan yang melalui rangkaian semasa sidang pengesahan di antara pengguna dan hos komputer jauh. Maklumat ini boleh digunakan oleh penyerang untuk menyamar sebagai

pengguna yang tulen. Perisian untuk mengawasi laluan rangkaian telah banyak berada di pasaran, bagi tujuan pengurusan perjalanan dan juga mengesan masalah rangkaian. Malangnya, perisian ini juga boleh digunakan oleh pihak yang tidak bertanggungjawab untuk merekod kata laluan dan data penting lain yang dihantar melalui rangkaian.

Salah satu mekanisme untuk meningkatkan tahap keselamatan sistem pengesahan adalah menggunakan teknik kriptografi. Beberapa sistem pengesahan menggunakan teknik kriptografi kunci rahsia telah dibangunkan. Masalah bagi sistem pengesahan menggunakan teknik kriptografi kunci rahsia yang melibatkan banyak prinsipal yang dihubungkan di dalam sistem teragih, iaitu keperluan setiap prinsipal untuk mempunyai kunci rahsia yang unik dengan setiap prinsipal yang akan berkomunikasi dengannya. Untuk mengatasi masalah ini, sistem-sistem sedemikian memperkenalkan satu agen yang boleh dipercayai iaitu satu pelayan khusus dikenali sebagai pelayan pengesahan (Burrows *et al.*, 1990) sebagai penyebar kunci sidang yang akan digunakan oleh prinsipal-prinsipal yang terlibat dalam pengesahan. Tahap keselamatan yang tinggi perlu dikenakan ke atas pelayan pengesahan kerana pencerobohan kepada pelayan tersebut membolehkan kunci sidang terancam dan seterusnya boleh digunakan untuk menyamar sebagai prinsipal yang tulen.

Kriptografi kunci awam, pertama kali dibentangkan dalam (Diffie dan Hellman, 1976), telah mengelakkan keperluan berkongsi kunci rahsia di antara prinsipal-prinsipal yang akan berkomunikasi. Konsep tandatangan digital dapat

digunakan untuk mempastikan sesuatu entiti adalah benar seperti yang didakwa. Menggunakan teknik ini masalah untuk mengesah betul pengguna kepada sesuatu sistem dapat diatasi. Setiap pengguna yang ingin memasuki sistem perlu memberikan tandatangan digital yang unik, yang tidak dapat ditiru oleh orang lain. Dengan menggunakan kunci awam yang khusus untuk pengguna berkenaan, sistem dapat mengesah betul sama ada tandatangan digital tersebut benar dijana oleh pengguna berkenaan.

Perisian-perisian sistem pengesahan berdasarkan kepada kriptografi kunci awam agak kurang di pasaran. Kebanyakan perisian yang dibangunkan di Amerika Syarikat adalah tertakluk kepada kekangan eksport yang dikenakan oleh Kerajaan Amerika. Ini bermakna perisian yang berada di negara kita mempunyai tahap keselamatan yang rendah berbanding dengan perisian yang setara yang digunakan di Amerika Syarikat. Sudah tiba masanya negara kita membangunkan sendiri perisian-perisian keselamatan untuk keperluan negara.

Objektif Kajian

1) Menganalisis perbandingan di antara sistem kripto RSA dan LUC daripada aspek pelaksanaan dan keselamatan.
2) Membangunkan satu prototaip sistem pengesahan untuk aplikasi *telnet* yang menggunakan algoritma kunci awam.

Skop Kajian

Memandangkan keselamatan di dalam rangkaian komputer bergantung kepada berbagai faktor maka kajian ini hanya dihadkan kepada perkara-perkara seperti berikut:-

1) Kajian akan memberi penumpuan kepada mekanisme pengesahan menggunakan teknik kriptografi, khususnya tandatangan digital. Pengesahan diri sebelum diberi kebenaran untuk mencapai sesuatu hos komputer di dalam aplikasi *telnet* akan dilaksanakan dalam persekitaran sistem pengoperasian *Linux*. Pelayan aplikasi *telnet* dan pelayan pengesahan terletak di dalam hos yang sama.
2) Tandatangan digital yang akan digunakan adalah berasaskan sistem kripto kunci awam iaitu RSA atau LUC.
3) Kajian akan mempertimbangkan pelaksanaan daripada aspek perisian sahaja.

Sumbangan Kajian

1) Analisis yang telah dijalankan menunjukkan bahawa sistem kripto LUC mempunyai perbezaan yang tidak begitu ketara berbanding dengan sistem kripto RSA dan boleh dijadikan sebagai alternatif dengan keupayaan yang boleh diterima pakai.

2) Prototaip sistem pengesahan untuk aplikasi *telnet* yang telah dibangunkan akan menjadi perintis kepada pembangunan perisian keselamatan domestik bagi mengatasi masalah penggunaan perisian yang setara di pasaran dengan kekangan keselamatan.

Struktur Organisasi Tesis

Tesis ini dibahagikan kepada enam bab. Bab I membincangkan pengenalan kepada sistem pengesahan. Latar belakang masalah, skop kajian, objektif kajian, sumbangan kajian dan struktur organisasi tesis juga diberikan dalam bab ini. Bab II di dalam tesis ini memuatkan ulasan karya. Ulasan karya dimulakan dengan pengenalan kepada kriptografi. Bab II juga memberikan contoh kriptografi klasik. Seterusnya kriptografi moden menyentuh secara ringkas sistem kripto kunci rahsia. Kriptografi kunci awam, konsep tandatangan digital, definisi pengesahan, protokol-protokol pengesahan dan kajian yang berkaitan turut disertakan.

Bab III pula menerangkan rangka kerja analisis sistem kripto kunci awam manakala bab IV memuatkan reka bentuk prototaip sistem pengesahan. Hasil analisis perbandingan di antara sistem kripto kunci awam RSA dan LUC dan prototaip sistem pengesahan dibincangkan dalam Bab V. Bab terakhir, iaitu Bab VI memberikan kesimpulan bagi kajian dan cadangan untuk penyelidikan di masa hadapan.

BAB II

ULASAN KARYA

Pendahuluan

Kriptografi sebagaimana yang telah disentuh di dalam Bab I merupakan elemen penting dalam meningkatkan tahap keselamatan di dalam rangkaian. Pengenalan kepada kriptografi akan memulakan bab kedua. Ini termasuklah konsep asas dan algoritma yang digunakan di dalam bidang ini. Contoh kriptografi klasik akan diberikan seterusnya. Kriptografi moden pula menyentuh secara ringkas kriptografi kunci rahsia.

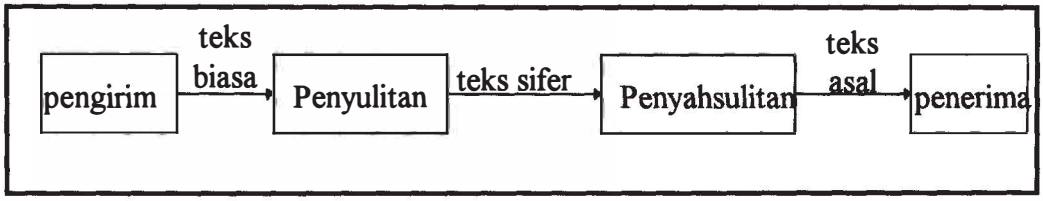
Kriptografi kunci awam akan diberikan penumpuan yang lebih kerana konsep di dalam kriptografi kunci awam, iaitu konsep tandatangan digital akan digunakan di dalam pembangunan prototaip sistem pengesahan. Bab kedua ini seterusnya memuatkan penerangan mengenai sistem pengesahan. Ini diikuti pula dengan ringkasan untuk keseluruhan bab kedua.

Pengenalan kepada Kriptografi

Konsep Asas

Bidang kriptologi terbahagi kepada dua cabang iaitu kriptografi dan kriptanalisis. Kriptografi adalah sains dan seni dalam menjadikan sesuatu perhubungan tidak difahami oleh semua pihak kecuali penerima yang dikehendaki. Kriptanalisis pula adalah kajian untuk mendapatkan semula teks asal tanpa mengetahui kunci penyahsulitan (Schneier, 1996). Kriptanalisis boleh juga digunakan sebagai cara untuk menemui kelemahan sesuatu sistem kripto. Juru kriptografi mencari kaedah-kaedah bagi mempastikan kerahsiaan dan kesahihan sesuatu mesej manakala juru kriptanalisis pula mencari jalan untuk memecah penyulitan yang telah dilakukan oleh juru kriptografi.

Proses menukar mesej daripada bentuk yang difahami ke bentuk yang tidak difahami dikenali sebagai penyulitan. Proses sebaliknya pula, menukar daripada bentuk yang tidak difahami ke bentuk asal yang difahami adalah penyahsulitan. Mesej asal yang lazimnya ditulis sebagai M, dipanggil teks asal, dan hasil penyulitan dikenali pula sebagai teks sifer atau kriptogram yang lazimnya ditulis sebagai C. Teks asal boleh jadi sebagai rentetan bit, fail teks, satu peta bit, satu rentetan suara yang telah didigitkan, imej video digital atau apa jua kerana sistem komputer hanya mengenali M sebagai data perduaan. Sistem yang digunakan untuk penyulitan dan penyahsulitan dikenali sebagai sistem kripto. Rajah 1 menunjukkan komponen asas sistem kripto.



Rajah 1: Asas Sistem Kripto

Pasang telinga atau pengintipan dawai adalah pintasan maklumat oleh pihak ketiga atau pihak yang tidak diberi kebenaran dengan cara mengawasi talian komunikasi (Rhee, 1994). Serangan pasif adalah keadaan apabila pihak musuh hanya memerhatikan maklumat atau rekod yang dihantar melalui talian komunikasi manakala serangan aktif pula adalah keadaan jika pihak musuh mengubahsuai maklumat atau menyelitkan data palsu ke dalam talian komunikasi.

Dua matlamat utama kriptografi adalah untuk (Massey, 1996):-

1) Kerahsiaan atau kebersendirian.

   Penafian capaian kepada maklumat oleh individu yang tidak diberi kebenaran.

2) Pengesahan.

   Pengesahan pula dikategorikan kepada pengesahan mesej dan pengesahan identiti pengirim. Pengesahan mesej memberi jaminan bahawa sesuatu mesej yang berada di dalam perjalanan telah tidak diubahsuai sama ada secara sengaja atau tidak sengaja dan dengan ini keutuhan mesej adalah terjamin (Diffie, 1988).

Sesuatu teknik dikatakan boleh menyediakan kerahsiaan jika tujuannya adalah untuk menentukan "*siapa yang dibenarkan untuk menerima mesej*" (Massey, 1996).

Algoritma Penyulitan

Algoritma penyulitan (kadangkala dikenali sebagai sifer) adalah satu set peraturan yang melaksanakan penjelmaan teks asal kepada teks sifer (Jackson dan Hruska, 1992). Kesemua algoritma penyulitan adalah berdasarkan kepada dua prinsip asas iaitu transposisi dan penggantian (Denning, 1983). Sifer transposisi melakukan proses penyusunan semula unsur-unsur teks asal mengikut skim tertentu. Sifer penggantian pula melakukan proses pemetaan setiap elemen teks asal kepada elemen lain.

Proses penyulitan dan penyahsulitan dikawal oleh kunci kriptografi. Sistem kripto terbahagi kepada dua iaitu sistem kripto kunci rahsia atau simetri dan sistem kripto kunci awam atau asimetri. Keselamatan sistem kripto kunci rahsia bergantung kepada pengirim dan penerima memiliki suatu rahsia sepunya yang tidak diketahui oleh orang lain. Keselamatan sistem kripto kunci awam pula bergantung kepada pengirim dan penerima memiliki suatu maklumat yang dipercayai oleh keduanya yang juga diketahui oleh orang lain (Massey, 1996).

Kriptanalisis

Kriptanalisis merupakan kajian mengenai kaedah untuk memecah atau menyerang sistem kripto. Sesuatu sistem kripto dikatakan boleh dipecah atau diserang jika sekiranya dapat ditentukan teks asal atau kunci yang digunakan daripada teks sifer, atau boleh ditentukan kunci yang digunakan daripada pasangan teks asal-sifer (Denning, 1983). Terdapat empat jenis serangan kriptanalitik (Denning, 1983; Schneier, 1996) :-

1) Serangan hanya teks sifer.

   Dalam serangan ini juru kriptanalisis mempunyai beberapa teks sifer yang telah disulitkan dengan menggunakan algoritma penyulitan yang sama. Tugas juru kriptanalisis adalah untuk memperolehi seberapa banyak yang mungkin teks asal atau merumuskan kunci yang digunakan.

2) Serangan teks asal yang diketahui.

   Juru kriptanalisis mempunyai beberapa teks sifer dan padanan teks asal. Tugas juru kriptanalisis adalah untuk merumuskan kunci yang digunakan atau algoritma untuk menyahsulit sebarang teks sifer menggunakan kunci berkenaan.

3) Serangan teks asal pilihan.

   Juru kriptanalisis mempunyai beberapa pasangan teks sifer dan teks asal yang sepadanan serta boleh memilih mesej untuk disulitkan. Tugas juru kriptanalisis adalah untuk merumuskan kunci yang digunakan atau algoritma untuk menyahsulit teks sifer yang baru.