Aplikasi Kriptografi untuk Proteksi dan Keamanan Sistem Informasi

Rizkydaya Aditya Putra — NIM : 13506037
Jurusan Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
Email : if16037@students.if.itb.ac.id

Abstract *– Makalah ini membahas tentang pengaplikasian salah satu subbab dalam mata kuliah matematika diskrit yaitu kriptografi. Kriptografi dalam bahasa Yunani berarti tersembunyi. Dalam masa modern ini, kriptografi dianggap sebagai cabang baik dari matematika dan ilmu computer serta berhubungan erat dangan teori infromasi.Kriptografi saat ini banyak digunakan dalam masyarakat maju, sebagai contoh dalam system keamanan kartu ATM, sandi lewat pada computer, perdagangan elektronik, dan lain-lain yang mana semuanya bergantung kepada kriptografi. Oleh karena itu, dalam zaman modern ini, masih diperlukan pengetahuan dan pengenalan lebih mendalam tantang aplikasi dari kriptografi modern terutama di bidang keamanan sistem informasi.*

Kata Kunci*:kriptografi, kriptanalisis, kriptologi, ekripsi, dekripsi*, *chipertext, plaintext, kunci publik, kunci simetris.*

1. PENDAHULUAN

1.1 Latar Belakang

Kriptografi dalam mungkin masih menjadi suatu istilah yang asing bagi sebagian orang di berbagai Negara. Namun sebenarnya kriptografi amat mudah dijumpai meskipunmungkin hanya sebagian kecil dari masyarakat di dunia yang mampumerasakan langsung kegunaan dari kriptografi tersebut.

Dalam makalah ini akan dijelaskan apa itu kriptografi, teori-teori yang berhubungan dengan kriptografi bidang protaksi, pengaplikasiannya dalam kehidupan masyarakat, dan prinsip apa yang digunakan sehingga kriptografi mampu diaplikasikan dalam suatu barang elektronik terutama dalam bidang keamanan dan proteksi.

Tujuan dari dibuatnya makalah ini adalah untuk memberi penjelasan tentang berbagai aplikasi dari kriptografi dalam kehidupan modern. Selain itu, untuk memenuhi tugas makalah mata kuliah IF2153 Matematika Diskrit yang diberikan di prodi Teknik Informatika ITB.

2. ISI

2.1. Terminologi

Hingga zaman modern seperti saat ini, kriptografi semata-mata dianggap sebagai enkripsi, yaitu proses mengubah informasi yang tidak biasa dan tidak dapat dibaca menjadi suatu informasi yang jelas dan dapat dibaca. Sedangkan dekripsi adalah proses sebaliknya. Chipertext tersebut adalah suatu pasangan algoritma yang melakukan enkripsi dan membalikan dekripsi. Informasi detail dari chipertext dikontrol oleh algoritma tersebut, sengan kata lain dengan suatu kunci. Hal tersebut merupakan parameter rahasia untuk membaca pesan rahasia tersebut, dan biasanya hanya pengirim dan yang dikirim yang mengetahui kunci tersebut. Kunci tersebut amatlah penting karena tanpa kunci itu, pesan tersebut akan mudah terbongkar dan menjadi tidak berarti lagi. Berdasarkan sejarahnya, chipertext kadang kala digunakan langsung untuk mengenkripsi atau deskripsi tanpa prosedur tambahan seperti pengesahan dan pengecekan kepribadian.

Dalam bahasa sehari-hari, kode biasanya digunakan untuk mengartikan suatu metode enkripsi atau penyembunyian suatu makna. Tetapi, dalam kriptografi, kode memiliki arti spesifik lebih; berarti suatu pergantian dari suatu unit dari suatu informasi dengan kata kode (sebagai contoh, `apple pie` diganti dengan `attack at dawn`). Kode tidak digunakan lagi dalam kriptografi yang sesungguhnya-kecuali tidak sengaja seperti proses desain suatu unit (contoh 'Bronco Flight' atau Operation Overlord)-sejak chipertext yang dipilih lebih praktis dan lebih aman dari biasanya, serta lebih mudah disesuaikan dengan computer.

Beberapa penggunaan kriptografi dan kriptologi dapat saling bertukar tempat dalam bahasa Inggris, ketika penggunaan kriptografi yang lain mengarah ke penggunaan dan praktek dari teknik kriptografik, dan kriptologi lebih mengarah ke subjek sebagai studi lapangan.

Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.

2.2. Sejarah Kriptografi

gambar 1: media kriptografi yang digunakan oleh bangsa Yunani kuno

Kriptografi memiliki sejarah yang panjang dan mengagumkan. Penulisan rahasia ini dapat dilacak kembali ke 3000 tahun SM saat digunakan oleh bangsa Mesir. Mereka menggunakan hieroglyphcs untuk menyembunyikan tulisan dari mereka yang tidak diharapkan. Hieroglyphcs diturunkan dari bahasa Yunani hieroglyphica yang berarti ukiran rahasia. Hieroglyphs berevolusi menjadi hieratic, yaitu stylized script yang lebih mudah untuk digunakan. Sekitar 400 SM, kriptografi militer digunakan oleh bangsa Spartan dalam bentuk sepotong papyrus atau perkamen dibungkus dengan batang kayu. Sistem ini disebut Scytale.

Sekitar 50 SM, Julius Caesar, kaisar Roma, menggunakan cipher substitusi untuk mengirim pesan ke Marcus Tullius Cicero. Pada cipher ini, huruf-huruf apfabet disubstitusi dengan huruf-huruf yang lain pada alfabet yang sama. Karena hanya satu alfabet yang digunakan, cipher ini merupakan substitusi monoalfabetik. Cipher semacam ini mencakup penggeseran alfabet dengan 3 huruf dan mensubstitusikan huruf tersebut. Substitusi ini kadang dikenal dengan C3 (untuk Caesar menggeser 3 tempat). Secar umum sistem cipher Caesar dapat ditulis sbb.:

$$Zi = Cn(Pi)$$

Dimana Zi adalah karakter-karekter ciphertext, Cn adalah transformasi substitusi alfabetik, n adalah jumlah huruf yang digeser, dan Pi adalah karakter-karakter plaintext.

Disk mempunyai peranan penting dalam kriptografi sekitar 500 th yang lalu. Di Italia sekitar tahun 1460, Leon Battista Alberti mengembangkan disk cipher untuk enkripsi. Sistemnya terdiri dari dua disk konsentris. Setiap disk memiliki alfabet di sekelilingnya, dan dengan memutar satu disk berhubungan dengan yang lainnya, huruf pada satu alfabet dapat ditransformasi ke huruf pada alfabet yang lain.

Bangsa Arab menemukan cryptanalysis karena kemahirannya dalam bidang matematika, statistik, dan lingiustik. Karena setiap orang muslim harus menambah pengetahuannya, mereka mempelajari peradaban terdahulu dan mendekodekan tulisan-tulisannya ke huruf-huruf Arab. Pada tahun 815, Caliph al-Mamun mendirikan House of Wisdom di Baghdad yang merupakan titik pusat dari usaha-usaha translasi. Pada abad ke-9, filsuf Arab al-Kindi menulis risalat (ditemukan kembali th 1987) yang diberi judul "A Manuscript on Deciphering Cryptographic Messages".

Pada 1790, Thomas Jefferson mengembangkan alat enkripsi dengan menggunakan tumpukan yang terdiri dari 26 disk yang dapat diputar secara individual. Pesan dirakit dengan memutar setiap disk ke huruf yang tepat dibawah batang berjajar yang menjalankan panjang tumpukan disk. Kemudian, batang berjajar diputar dengan sudut tertentu, A, dan huruf-huruf dibawah batang adalah pesan yang terenkripsi. Penerima akan menjajarkan karakter-karakter cipher dibawah batang berjajar, memutar batang kembali dengan sudut A dan membaca pesan plaintext.

Sistem disk digunakan secara luas selama perang sipil US. Federal Signal Officer mendapatkan hak paten pada sistem disk mirip dengan yang ditemukan oleh Leon Battista Alberti di Italia, dan dia menggunakannya untuk mengkode dan mendekodekan sinyal-sinyal bendera diantara unit-unit.

Sistem Unix menggunakan cipher substitusi yang disebut ROT 13 yang menggeser alfabet sebanyak 13 tempat. Penggeseran 13 tempat yang lain membawa alfabet kembali ke posisi semula, dengan demikian mendekodekan pesan. Mesin kriptografi mekanik yang disebut Hagelin Machine dibuat pada tahun 1920 oleh Boris Hagelin di Scockholm, Swedia. Di US, mesin Hagelin dikenal sebagai M-209.

Gambar 2 : mesin Enigma, digunakan olek militer Jerman pada akhir 1920 dan pada akhir dari Perang Dunia II, menggunakan chipertext elektro mekanik yang kompleks untuk menjaga kerahasiaan komunikasi yang sensitif.

Pada tahun 20-an, Herbert O. Yardley bertugas pada organisasi rahasia US MI-8 yang dikenal sebagai "Black Chamber". MI-8 menjebol kode-kode sejumlah negara. Selama konferensi Angkatan Laut Washington tahun 1921-1922, US membatasi negosiasi dengan Jepang karena MI-8 telah memberikan rencana negosiasi Jepang yang telap disadap kepada sekretaris negara US. Departemen negara menutup MI-8 pada tahun 1929 sehingga Yardley merasa kecewa. Sebagai wujud kekecewaanya, Yardley menerbitkan buku The American Black Chamber, yang menggambarkan kepada dunia rahasia dari MI-8. Sebagai konsekuensinya, pihak Jepang menginstal kode-kode baru. Karena kepeloporannya dalam bidang ini, Yardley dikenal sebagai "Bapak Kriptografi Amerika".

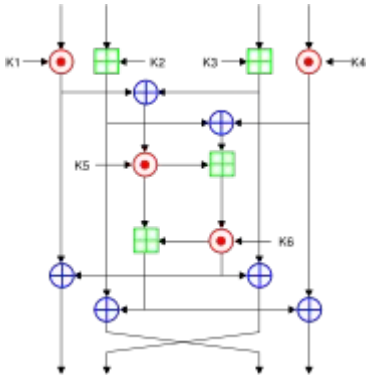
gambar 3 : mesin pembaca chipertext Lorenz milik Jerman, digunakan saat PD II

2.2. Kriptografi Modern

Bidang kripografi modern dapat dibagi menjadi beberapa area studi. Di makalah ini akan dibahas beberapa yang pokok saja.

2.2.1. Kriptografi Kunci-Simetris

Kriptografi kunci-simetrik mengarah kepada metode enkripsi yang mana baik pengirim maupun yang dikirim saling memiliki kunci yang sama(walaupun kebanyakan kunci yang ada sedikit berbeda namun masih berhubungan dalam hal kemudahan perhitungan). Berikut ini merupakan jenis enkripsi yang diketahui sampai tahun 1976.



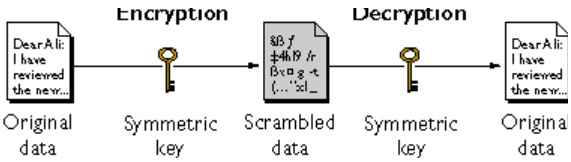
gambar 4 : bagan siklus dari chipertext IDEA yang telah dipatenkan

Secret-key cryptography kadang disebut sebagai symmetric cryptography merupakan bentuk kryptografi yang lebih tradisional, dimana sebuah kunci tunggal dapat digunakan untuk mengenkrip dan mendekrip pesan. Secret-key cryptography tidak hanya berkaitan dengan enkirpsi tetapi juga berkaitan dengan otentikasi. Salah satu teknik semacam ini disebut *message authentication codes*.

Data Encryption Standart (DES) dan *Advanced Encryption Standart* (AES) adaalh salah satu desain sandi balok yang sudah didesain standar kriptografi oleh pemerintah AS. Meskipun terdapat bantahan dari standar resminya, DES masih cukup terkenal dan digunakan sebagai aplikasi yang sudah luas penggunaannya, dari enkripsi ATM sampai privasi email dan akses keamanan. Banyak sandi balok lain yang telah didesaindan diluncurkan ke publik dengan mempertimbangkan kualitas dalam berbagai variasi. Tetapi banyak pula yang sudah terbongkar.

Sandi gelombang berlawanan dengan sandi balok, membuat material gelombang panjang yang berubah-ubah yang dikombinasikan dengan kode tulisan bit demi bit atau karakter demi karakter,.

Masalah utama yang dihadapi secret-key cryptosystems adalah membuat pengirim dan penerima menyetujui kunci rahasia tanpa ada orang lain yang mengetahuinya. Ini membutuhkan metode dimana dua pihak dapat berkomunikasi tanpa takut akan disadap. Kelebihan secret-key cryptography dari public-key cryptography adalah lebih cepat.. Teknik yang paling umum dalam secret-key cryptography adalah *block ciphers*, *stream ciphers*, dan message authentication codes.



Gambar 5 :Enkripsi kunci rahasia

2.2.2. Kriptografi Kunci-Publik/Asimetris

Seperti yang telah disebutkan dalam artikel sebelumnya, algoritma sandi dapat dikelompokkan menjadi 3 kategori yaitu : sistem sandi simetris, sistem sandi asimetris dan sistem sandi hashing. Masing-masing sistem sandi ini memiliki cara yang berbeda dalam metode penyandiannya.

Sistem sandi asimetris atau dikenal juga sebagai sistem sandi kunci publik adalah sistem sandi yang metode menyandi dan membuka sandinya menggunakan kunci yang berbeda. Tidak seperti sistem sandi simetris, sistem sandi ini relatif masih baru. Algoritma sandi jenis ini yang telah terkenal diantaranya RSA (Rivest-Shamir-Adleman), ElGamal, dan Diffie-Hellman.

Sistem ini memiliki sepasang kunci yang disebut kunci publik yaitu kunci yang didistribusikan secara umum dan kunci privat yaitu kunci yang dirahasiakan yang hanya dimiliki oleh pihak yang berhak. Umumnya kunci publik digunakan untuk menyandi dan kunci privat digunakan untuk membuka sandi.

Sistem sandi asimetrik bekerja lebih lambat dari sistem sandi simetris, sehingga sistem sandi ini lebih sering digunakan untuk menyandi data dengan ukuran bit yang kecil. Sistem sandi ini sering pula digunakan untuk mendistribusikan kunci sistem sandi simetris.

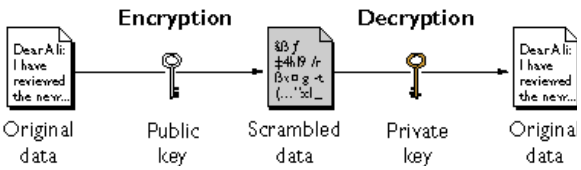
Penggunaan lain sistem sandi asimetris adalah dalam tandatangan digital. Tandatangan digital seperti halnya tandatangan biasa digunakan untuk membuktikan keaslian dari suatu dokumen yang dikirimkan. Kunci privat digunakan untuk menandatangani, sedangkan kunci publik digunakan untuk membuktikan keaslian tandatangan itu.

Untuk lebih memudahkan pengertian tandatangan digital dapat diilustrasikan sebagai berikut :

> *Untuk menandai pesannya, si Pengirim menyandi pesan tersebut dengan kunci privat-nya. Setiap orang yang memiliki pasangan kunci publik-nya dapat membuka pesan tersandi itu dan mengetahui dengan pasti si Pengirim adalah orang yang tepat.*

Cara ini tidak melindungi kerahasiaan datanya, mengingat setiap orang dapat saja memiliki pasangan kunci publik dari si Pengirim. Tujuan dari tandatangan digital hanyalah membuktikan bahwa pesan tersebut memang dari si Pengirim.

Karena kunci publik didistribusikan secara umum, kita mempunyai permasalahan yang berbeda dengan sistem sandi simetris. Permasalahan utamanya adalah apakah kunci publik-nya berada ditangan yang tepat ? Untuk mengatasi masalah tersebut maka Infrastruktur Kunci Publik (PKI) mencoba memberikan pemecahannya. Namun karena masih dalam tahap pengembangan, PKI tidak memberikan jaminan. Masih membutuhkan waktu lama untuk dapat menerima solusi PKI ini. System kriptografi kunci-simetri secara tipikal menggunakan enkripsi dan dekripsi yang sama meskipun pesan ini memiliki kunci berbeda satu sama lain. Secara signifikan, ketidakuntungan dari siem ini adalah manajemen kunci yang diperlukan untuk keamanan. Setiap pasang komunikasi yang berjarak jauh harus memiliki kunci yang berbeda. Setiap kunci yang bertambah akan menambahkan jarak dari anggota jaringan yang mana akan membutuhkan menajemen kunci yang lebih teliti lagi agar terjamin keamanannya. Hal yang membuat sulit adalah kesulitan dalam menempatkan kunci rahasia diantara kelompok yang berkomunikasi. Algoritma kunci-publik ini biasanya berdasarkan kompleksitas komputasional dari masalah yang "sulit", biasanya dari teori angka. Sebagai contoh, kekerasan dari RSA biasanya berhubungan dengan masalah faktorisasi integer, ketika Diffie-Hellman dan DSA berkaitan dengan masalah logaritma doskrit. Lebih jauh lagi, kriptografi kurva cekung telah berkembang dari msalah keamanan yang ada. Karena kesulitan dari masalah tersebut, algoritma kunci-publik termasuk operasi modular seperti perkalian dan eksponensial, yang mana hal tersebut secara komputasi lebih mahal daripada teknik lain yang digunakan oleh chipertext, terutama yang menggunakan kunci spesifik. Hasilnya, system criptografi kunci-publik merupakan kriptosistem hibrid secara umum, yang mana algoritma kunci-simetrik kualitas tinggi digunakan sebagai pesan tersebut. Persamaannya, skema tanda tangan hibrid lebih sering digunakan, yang mana fungsi kriptografi diperhitungkan dan hasilnya akan berlaku secara digital.



Gambar 6 : Enkripsi kunci public

2.2.3. Data Encryption Standart (DES)
DES, akronim dari Data Encryption Standard, adalah nama dari Federal Information Processing Standard (FIPS) 46-3, yang menggambarkan data encryption algorithm (DEA). DEA juga didefinisikan dalam ANSI standard X3.92. DEA merupakan perbaikan dari algoritma Lucifer yang dikembangkan oleh IBM pada awal tahun 70an. Meskipun algoritmanya pada intinya dirancang oleh IBM, NSA dan NBS (sekarang NIST (National Institute of Standards and Technology)) memainkan peranan penting pada tahap akhir pengembangan. DEA, sering disebut DES, telah dipelajari secara ekstensif sejak publikasinya dan merupakan algoritma simetris yang paling dikenal dan paling banyak digunakan. DEA memiliki ukuran blok 64-bit dan menggunakan kunci 56-bit kunci selama eksekusi (8 bit paritas dihilangkan dari kunci 64 bit). DEA adalah symmetric cryptosystem, khususnya cipher Feistel 16-rounddan pada mulanya dirancang untuk implementasi hardware. Saat digunakan untuk komunikasi, baik pengirim maupun penerima harus mengetahui kunci rahasia yang sama, yang dapat digunakan untuk mengenkrip dan mendekrip pesan, atau untuk menggenerate dan memverifikasi message authentication code (MAC). DEA juga dapat digunakan untuk enkripsi single user, seperti untuk menyimpan file pada harddisk dalam bentuk terenkripsi. Dalam lingkungan multiuser, distribusi kunci rahasia akan sulit. Public-key cryptography menyediakan solusi yang ideal untuk masalah ini. NIST telah mensertifikasi kembali DES (FIPS 46-1, 46-2, 46-3) setiap 5 tahun. FIPS 46-3 mensahkan kembali penggunaan DES sampai Oktober 1999, namun single DES hanya diijinkan untuk legacy systems. FIPS 46-3 mencakup definisi dari triple-DES (TDEA, menurut X9.52); TDEA adalah "pilihan algoritma simetris yang disetujui oleh FIPS." Dalam beberapa tahun, DES dan triple-DES akan digantikan dengan Advanced Encryption Standard.

2.2.4. Advanced Encryption Standart (AES)
AES adalah Advanced Encryption Standard. AES adalah block cipher yang akan menggantikan DES tetapi diantisipasi bahwa Triple DES tetap akan menjadi algoritma yang disetujui untuk penggunaan pemerintah USA. Pada Januari 1997 inisiatif AES diumumkan dan pada September 1997 publik diundang untuk mengajukan proposal block cipher yang cocok sebagai kandidat untuk AES. Pada tahun 1999 NIST mengumumkan lima kandidat finalis yaitu MARS, RC6, Rijndael, Serpent, dan Twofish. Algoritma AES dipilih pada Oktober 2001 dan standarnya dipublish pada November 2002. AES mendukung ukuran kunci 128 bit, 192 bit, dan 256 bit, berbeda dengan kunci 56-bit yang ditawarkan DES. Algoritma AES dihasilkan dari proses bertahun-tahun yang dipimpin NIST dengan bimbingan dan review dari komunitas internasional pakar kriptografi. Algoritma Rijndael, yang dikembangkan oleh Joan Daemen dan Vincent Rijmen, dipilih sebagai standar.

2.2.5. Kriptanalisis

Tujuan dari kriptanalisis ini adalah untuk menemukan beberapa kelemahan atau ketidakamanan dalam skema kriptografi, untuk itu dilakukan izin untuk subversi atau penghindaran. Kriptanalisis mungkin dianggap remeh bagi beberapa penyerang, dikarenakan system yang mudah ditumbangkan. Dalam praktik modernnya, algoritma kriptografi dan protocol harus dicek ulang secara teliti dan dites untuk memberikan jaminan system keamanan.

Jika kriptanalisis murni menggunakan kelemahan dalam algoritma, kriptosystem yang lain berdasarkan penggunaan actual dari algoritma dalam alat yang real dan disebut sebagai serangan sisi samping. Jika seorang kriptoanalis memiliki akses untuk memasukkan waktu yang diperlukan untuk enkripsi pesan kesalahan dari masukan sandi lewat atau karakter PIN, ia akan dapat melakuakan serangan waktu untuk membongkar chipertext yang tahan terhadap analis sekalipun. Seorang penyerang mungkin juga belajar pola dan ukuran pesan untuk mendapatkan informasi yang berharga.

2.2.6. RSA

RSA cryptosystem adalah public-key cryptosystem yang menawarkan baik enkripsi dan tanda tangan digital (otentikasi). Ronald Rivest, Adi Shamir, dan Leonard Adleman mengembangkan sistem RSA system pada tahun 1977.

Algoritma RSA bekerja seperti berikut: ambil dua bilangan prima besar, p dan q, dan hitung hasil kalinya $n = pq$; n disebut dengan modulus. Pilih sebuah bilangan, e, yang lebih kecil dari n dan merupakan bilangan prima secara relative dari $(p-1)(q-1)$, yang artinya e dan $(p-1)(q-1)$ tidak memiliki faktor bersama kecuali 1. temukan bilangan lain d sehingga $(ed - 1)$ dapat dibagi dengan $(p-1)(q-1)$. Nilai-nilai e dan d masing-masing disebut eksponen publik dan privat. Kunci publik adalah pasangan (n, e); kunci privat adalah (n, d). Faktor p dan q dapat dihancurkan atau disimpan dengan kunci privat. Sulit untuk mendapatkan kunci privat d dari kunci publik (n, e). Jika seseorang dapat memfaktorkan n menjadi p dan q, maka ia bisa mendapatkan kunci privat d. Sehingga keamanan sistem RSA berdasar pada asumsi bahwa pemfaktoran sulit dilakukan. Dibawah ini adalah bagaimana sistem RSA dapat digunakan untuk enkripsi dan tanda tangan digital (dalam prakteknya, penggunaan aktualnya sedikit berbeda):

Enkripsi:

Anggap Alice ingin mengirim pesan m kepada Bob. Alice membuat ciphertext c dengan mengeksponenkan: $c = me \bmod n$, dimana e dan n adalah kunci public Bob. Alice mengirim c kepada Bob. Untuk mendekripnya, Bob juga mengeksponenkan: $m = cd \bmod n$; hubungan antara e dan d meyakinkan bahwa Bob mendapatkan m dengan benar. Karena hanya Bob yang mengetahui d, hanya Bob yang dapat mendekrip pesan ini.

Tanda tangan digital:

Anggap Alice ingin mengirim pesan m kepada Bob sehingga Bob yakin bahwa pesannya otentik, tidak dimodifikasi, dan dari Alice.

Alice membuat tanda tangan digital s dengan mengeksponenkan: $s = md \bmod n$, dimana d dan n adalah kunci privat Alice. Alice mengirim m dan s kepada Bob. Untuk memverifikasi tandatangan, Bob mengeksponenkan dan mengecek bahwa pesan m didapatkan: $m = se \bmod n$, dimana e dan n adalah kunci publik Alice.

2.2.7 Fungsi Hash

One-way function adalah fungsi matematika yang secara signifikan mudah untuk dihitung pada satu arah (arah maju) daripada dengan arah sebaliknya (inverse). Dimungkinkan, sebagai contoh, untuk menghitung fungsi dengan arah maju pada beberapa detik namun untuk menghitung dapat memakan waktu berbulan-bulan atau bertahun-tahun, jika semua dimungkinkan. *Trapdoor oneway function* adalah fungsi satu arah dimana arah inversnya mudah diberikan sebuah informasi (trapdoor), tetapi sulit untuk melakukan hal sebaliknya.

Public-key cryptosystems berdasar pada (dianggap) trapdoor one-way functions. Kunci publik memberikan informasi tentang instans tertentu dari fungsi, kunci privat memberikan informasi tentang trapdoor. Siapapun yang mengetahui trapdoor dapat menghitung fungsi dengan mudah dalam dua arah, tetapi siapapun yang tidak memiliki trapdoor hanya dapat menjalankan fungsidengan mudah pada arah maju. Arah maju digunakan untuk enkripsi dan verifikasi tandatangan, arah invers digunakan untuk dekripsi dan pembuatan tandatangan.

Fungsi hash adalah fungsi yang memproduksi output dengan panjang tetap dari input yang berukuran variabel. Output dari fungsi hash disebut dengan message digest. Fungsi hash memiliki karakteristik fungsi satu arah karena file asli tidak dapat dibuat dari message digest.

2.3. Kriptografi Dalam Kehidupan Modern

Banyak sekali kegunaan kriptografi yang terdapat dalam kehidupan sehari-hari.

2.3.1.Transaksi Melalui Anjungan Tunai Mandiri (ATM)

Anjungan Tunai Mandiri atau *Automatic Teller Machine* (ATM) digunakan nasabah bank untuk melakukan transaski perbankan. Utamanya, kegunaan ATM adalah untuk menarik uang secara tunai (*cash withdrawal*), namun saat ini ATM juga digunakan untuk transfer uang (pemindahbukuan), mengecek saldo, membayar tagihan kartu ponsel, membeli tiket kereta api, dan sebagainya.

Transaksi lewat ATM memerlukan kartu magnetik (disebut juga kartu ATM) yang terbuat dari plastik dan kode PIN (*Personal Information Number*) yang berasosiasi dengan kartu tersebut.

PIN terdiri dari 4 angka yang harus dijaga kerahasiannya oleh pemilik kartu ATM, sebab orang lain yang mengetahui PIN dapat menggunakan kartu ATM yang dicuri atau hilang untuk melakukan penarikan uang.

PIN digunakan untuk memverifikasi kartu yang dimasukkan oleh nasabah di ATM. Proses verifikasi dilakukan di komputer pusat (*host*) bank, oleh karena itu harus ada komunikasi dua arah antara ATM dan komputer *host*. ATM mengirim PIN dan informasi tambahan pada kartu ke komputer *host*, *host* melakukan verifikasi dengan cara membandingkan PIN yang di-*entry*-kan oleh nasabah dengan PIN yang disimpan di dalam basisdata komputer *host*, lalu mengirimkan pesan tanggapan ke ATM yang menyatakan apakah transaksi dapat dilanjutkan atau ditolak.

Selama transmisi dari ATM ke komputer *host*, PIN harus dilindungi dari penyadapan oleh orang yang tidak berhak.

Bentuk perlindungan yang dilakukan selama transmisi adalah dengan mengenkripsikan PIN. Di sisi bank, PIN yang disimpan di dalam basisdata juga dienkripsi.

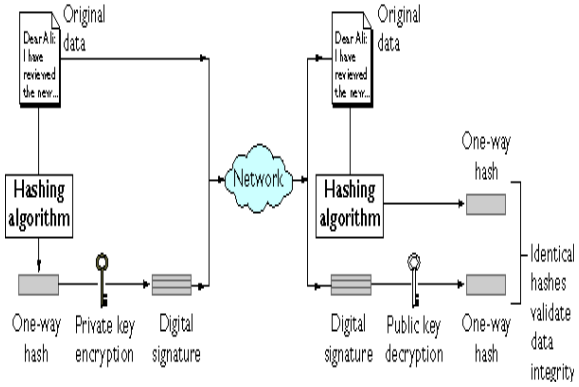
Algoritma enkripsi yang digunakan adalah DES dengan mode ECB. Karena DES bekerja dengan mengenkripsikan blok 64-bit, maka PIN yang hanya terdiri dari 4 angka (32 bit) harus ditambah dengan *padding bits* sehingga panjangnya menjadi 64 bit. *Padding bits* yang ditambahkan berbeda-beda untuk setiap PIN, bergantung pada informasi tambahan pada setiap kartu ATM-nya.

Karena panjang PIN hanya 4 angka, maka peluang ditebak sangat besar. Seseorang yang memperoleh kartu ATM curian atau hilang dapat mencoba semua kemungkinan kode PIN yang mungkin, sebab hanya ada $10 \times 10 \times 10 \times 10 = 10.000$ kemungkinan kode PIN 4-angka. Untuk mengatasi masalah ini, maka kebanyakan ATM hanya membolehkan peng-*entry*-an PIN maksimum 3 kali, jika 3 kali tetap salah maka ATM akan 'menelan' kartu ATM. Masalah ini juga menunjukkan bahwa kriptografi tidak selalu dapat menyelesaikan masalah keamanan data.

2.3.2. Tanda Tangan Digital

Tujuan dari tanda tangan digital adalah untuk mendeteksi modifikasi data yang tidak diotorisasi dan untuk mengotentikasi identitas dari penandatangan, juga untuk non-repudiasi. Fungsi-fungsi ini dicapai dengan menggenerate blok
data yang biasanya ukurannya lebih kecil dari data asli. Blok data yang lebih kecil ini dibubuhkan pada data asli dan pada identitas pengirim. Pembubuhan ini memverifikasi integritas data dan mendukung non-repudiasi.

Untuk menghasilkan tanda tangan digital, program sinyal digital melewatkan file untuk dikirimkan melalui fungsi hash satu arah. Setelah message digest dihitung, kemudian dienkripsi dengan kunci privat pengirim. Penerima kemudian mendekripsi message digest dengan menggunakan kunci publik
pengirim. Jika kunci publik ini membuka message digest dan benar bahwa ia merupakan kunci publik pengirim, verifikasi pengirim telah tercapai. Verifikasi terjadi karena hanya kunci publik pengirim yang dapat mendekrip message digest
yang dienkripsi dengan kunci privat pengirim. Kemudian, penerima dapat menghitung message digest dari file yang diterima menggunakan fungsi hash yang identik dengan pengirim. Jika message digest identik dengan message digest yang dikirim sebagai bagian dari tanda tangan, maka pesan tidak dimodifikasi.



Gambar 7 : penggunaan tanda tangan digital untuk validasi integritas data

2.4. Cryptographic Attacks

Pada dasarnya serangan terhadap primitif dan protokol kriptografi dapat dibedakan menjadi dua jenis yaitu:

- Serangan pasif adalah serangan dimana penyerang hanya memonitor saluran komunikasi. Penyerang pasif hanya mengancam kerahasiaan data.
- Serangan aktif adalah serangan dimana penyerang mencoba untuk menghapus, menambahkan, atau dengan cara yang lain mengubah transmisi pada saluran. Penyerang aktif mengancam integritas data dan otentikasi, juga kerahasiaan.

2.4.1. Serangan pada Enkripsi

Serangan ini secara umum diklasifikasikan dalam enam kategori. Tujuan dari penyerang dalam semua kasus adalah untuk dapat mendekrip sebuah ciphertext baru tanpa informasi tambahan. Yang menjadi idaman bagi penyerang adalah untuk mengekstrak kunci rahasia.

- Serangan *Ciphertext-only* adalah salah satu serangan dimana penyerang mendapatkan contoh dari ciphertext, tanpa plaintext yang berhubungan
dengannya. Data ini relatif mudah didapatkan dalam banyak skenario, tetapi serangan yang berhasil biasanya sulit, dan membutuhkan contoh
ciphertext yang sangat besar.
- Serangan *Known-plaintext* adalah salah satu serangan dimana penyerang mendapatkan contoh ciphertext dan juga plaintext yang berhubungan.

• Serangan *Chosen-plaintext* adalah salah satu serangan dimana penyerang dapat memilih kuantitas plaintext dan kemudian mendapatkan ciphertext terenkripsi yang berhubungan.
• Serangan *Adaptive-chosen-plaintext* adalah kasus khusus dari serangan chosen-plaintext dimana penyerang dapat memilih contoh plaintext secara dinamis, dan mengubah pilihannya berdasar dari hasil enkripsi sebelumnya.
• Serangan *Chosen-ciphertext* adalah salah satu serangan dimana penyerang dapat memilih sebuah ciphertext dan mencoba mendapatkan plaintext terdekripsi yang berhubungan. Tipe serangan ini biasanya banyak dilakukan pada public-key cryptosystems.
• *Adaptive-chosen-ciphertext* adalah versi adaptif dari serangan diatas. Penyerang dapat memuat serangan dari tipe ini dalam skenario dimana ia memiliki penggunaan bebas dari sebuah hardware dekripsi, tetapi tidak dapat mengekstrak kunci dekrpsi darinya.

2.4.2. Serangan pada Protokol

Dibawah ini adalah daftar serangan yang dapat dilakukan pada berbagai protokol. Sampai sebuah protokol terbukti dapat menyediakan layanan yang dimaksud, daftar serangan yang mungkin ini tidak dapat dikatakan lengkap.
• *Known-key attack*. Pada serangan ini penyerang mendapatkan beberapa kunci yang telah digunakan sebelumnya kemudian menggunakan informasi ini untuk menentukan kunci baru.
• *Replay Attack*. Pada serangan ini penyerang merekam sesi komunikasi dan me-reply seluruh atau sebagian sesi, pada suatu saat nanti.
• *Impersonation Attack*. Disini penyerang menggunakan identitas salah satu pihak resmi dalam jaringan.
• *Dictionary Attack*. Biasanya merupakan serangan pada password. Biasanya sebuah password disimpan dalam file komputer sebagai image dari unkeyed hash function. Saat pengguna log on dan memasukkan password, password di-hash dan image-nya dibandingkan dengan nilai yang tersimpan. Penyerang dapat mengambil daftar password yang mungkin, melakukan hash semua entri dalam daftar, dan kemudian membandingkannya dengan daftar password terenkripsi yang asli dengan harapan menemukan yang sesuai.
• *Forward Search Attack*. Serangan ini mirip dengan serangan dictionary dan digunakan untuk mendekripsi pesan.
• *Interleaving Attack*. Tipe serangan ini biasanya mencakup beberapa bentuk impersonation dalam protokol otentikasi.

2.5. Standar Kriptografi

Standar kriptografi dibutuhkan untuk menciptakan interoperabilitas dalam dunia keamanan informasi. Pada dasarnya standar merupakan kondisi dan protokol yang dibuat untuk memungkinkan keseragaman dalam komunikasi, transaksi dan semua aktivitas secara virtual. Evolusi teknologi informasi yang terus berlanjut memotivasi pengembangan lebih banyak lagi standar, yang membantu memandu evolusi ini. Motivasi utama dibalik standar adalah untuk memungkinkan teknologi dari pabrik yang berbeda untuk "berbicara bahasa yang sama", untuk berinteraksi secara efektif.
Dalam kriptografi, standarisasi memiliki tujuan tambahan, yaitu sebagai landasan dari teknik-teknik kriptografi karena protokol yang rumit cenderung memiliki cacat dalam rancangan. Dengan menerapkan standar yang telah diuji dengan baik, industri dapat memproduksi produk yang lebih terpercaya. Bahkan protokol yang amanpun dapat lebih dipercaya pelanggan setelah menjadi standar, karena telah melalui proses pengesahan.
Pemerintah, industri privat, dan organisasi lain berkontribusi dalam pengumpulan luas standar-standar kriptografi. Beberapa dari standar-standar ini adalah ISO, ANSI, IEEE, NIST, dan IETF. Ada banyak tipe standar, beberapa digunakan dalam industri perbankan, beberapa digunakan secara internasional, dan yang lain dalam pemerintahan. Standarisasi membantu pengembang merancang standar baru, mereka dapat mengikuti standar yang telah ada dalam proses pengembangan. Dengan proses ini pelanggan memiliki kesempatan untuk memilih diantara produk atau layanan yang berkompetisi.

3. ANALISIS

3.1. Ilustrasi Penggunaan pada UKM

Ada berbagai macam definisi Usaha Kecil Menengah (UKM) di Indonesia yang diakui oleh semua departemen dan instansi pemerintah, serta swasta di Indonesia. Beberapa definisi yang digunakan oleh departemen dan instansi yang lain berdasarkan pada nilai aset atau omset (penjualan). Misalnya, Kementerian Negara Kooperasi dan UKM mendefinisikan usaha kecil menengah sebagai berikut: (a) usaha dengan hasil penjualan sampai dengan Rp. 1 milyar digolongkan dalam usaha kecil, dan (b) usaha dengan hasil penjualan antara Rp. 1-50 milyar digolongkan dalam usaha menengah. Kontras dengan hal ini, Badan Pusat Statistik mendefinisikan UKM berdasarkan besarnya jumlah tenaga kerja.
Saat ini, hanya Badan Pusat Statistik yang membuat perbedaan sistematis tentang usaha rumah tangga (*cottage*), usaha kecil, menengah dan besar berdasarkan jumlah tenaga kerja. Dalam kaitannya dengan Teknologi Informasi dalam UKM, sampai saat ini belum ada acuan yang jelas berapa banyak jumlah tenaga kerja TI yang dipekerjakan, malahan sebagian besar UKM di Indonesia tidak memiliki divisi khusus untuk TI.

Melihat dari lingkup UKM, sumber dayanya baik sumber daya manusia maupun infrastruktur TI dan biaya, ada beberapa aplikasi kriptografi yang mungkin diterapkan dalam lingkungan UKM. Untuk UKM yang telah memiliki divisi TI sendiri, penerapan aplikasi kriptografi ini akan lebih murah dan mudah.

Aplikasi-aplikasi kriptografi yang dapat diterapkan antara lain enkripsi pada password, file, dan email. Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnya file yang berisi data keuangan). Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES, RSA, dll. Untuk mendapatkan algoritma enkripisi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Biaya yang dibutuhkan hanyalah biaya pengembangan dan biasanya biaya ini tidak terlalu besar jika pengembangannya dilakukan sendiri oleh divisi TI yang dimiliki UKM (*in house development*).

Jika dibutuhkan mekanisme enkripsi password lain yang lebih aman sesuai dengan kebutuhan keamanan data yang lebih tinggi dalam UKM dapat digunakan mekanisme *One Time Password* untuk menggantikan mekanisme password statis.

Keunggulan dari mekanisme *One Time Password* dimana password hanya digunakan satu kali saja setiap pengguna akan *log on* ke dalam sistem ini adalah walaupun penyerang berhasil mendapatkan password namun ia tidak dapat menggunakannya lagi untuk melakukan akses terhadap sistem. Teknik enkripsi yang dapat digunakan untuk mekanisme ini adalah teknik-teknik enkripsi simetris / kunci rahasia. Banyak algoritma yang dapat digunakan untuk mengenkripsi password misalnya DES, AES, Blowfish, RC6, dll. Sekali lagi yang dibutuhkan disini adalah sumber daya manusia yang mampu untuk mengimplementasikan algoritma ini.

Aplikasi kriptografi lain yang dapat diimplementasikan dalam UKM adalah enkripsi email. Enkripsi email dibutuhkan untuk melindungi surat-surat penting yang akan dikirim dari maupun keluar UKM. Misalnya saja pengiriman data-data laporan rugi laba UKM kepada pihak penagih pajak maupun pengiriman surat-surat berharga lainnya. Untuk mengimplementasikan enkripsi email ini UKM harus sudah terkoneksi Internet. Aplikasi enkripsi email yang dapat diadopsi misalnya *Pretty Good Privacy* (PGP) yang dapat diperoleh secara gratis.

Selain mengenkripsi email, PGP juga dapat digunakan untuk tanda tangan digital jika dibutuhkan level keamanan yang lebih tinggi.

4. KESIMPULAN

Kriptografi merupakan salah satu dari media komunikasi dan informasi kuno yang masih dimanfaatkan hingga saat ini. Kriptografi di Indonesia disebut persandian yaitu secara singkat dapat berarti seni melindungi data dan informasi dari pihak-pihak yang tidak dikehendaki baik saat ditransmisikan maupun saat disimpan. Sedangkan ilmu persandiannya disebut kriptologi yaitu ilmu yang mempelajari tentang bagaimana tehnik melindungi data dan informasi tersebut beserta seluruh ikutannya.

Pengguna diberikan ID dan password untuk mengakses sistem yang ada. Password dienkripsi untuk mencegah terjadinya akses illegal terhadap sistem misalnya pencurian data-data penting oleh mereka yang tidak berhak. Demikian juga enkripsi pada file-file penting dapat dilakukan (misalnya file yang berisi data keuangan). Metode enkripsi yang digunakan dapat berbentuk enkripsi kunci simetris, misalnya menggunakan algoritma DES, RSA, dll. Untuk mendapatkan algoritma enkripisi ini tidak dibutuhkan biaya karena telah dipublikasikan secara umum. Oleh karena itu, dapat disimpulkan bahwakriptografi masih merupakan sistem yang efektif dalam hal keamanan dan proteksi serta dapat digunakan secara luas di berbagai bidang usaha dan teknologi.

DAFTAR REFERENSI

[1] Mollin, Richard, “An Introduction to Cryptography, Second Edition (Discrete Mathematics and Its Applications)”, Chapman & Hall/CRC, 2006, pp.9-13.

[2] Munir, Rinaldi, “Matematika Diskrit”, ITB, 2003, pp.V-21 s.d V-25.

[3] Rahardjo, Budi, “Panduan Menulis dan Mempresentasikan Karya Ilmiah: Thesis, Tugas Akhir, dan Makalah”, ITB, 2005.

[4] Robshaw, Matthew, “Algebraic Aspects of the Advanced Encryption Standard (Advances in Information Security)”, Springer-Verlag, 2005, pp.21-23.

[5] http://en.wikipedia.org/wiki/Cryptography/, tanggal akses 29 Desember 2007, pukul 16.20 WIB.