PEMANFAATAN KEMBALI KRIPTOGRAFI KLASIK DENGAN MELAKUKAN MODIFIKASI METODE-METODE KRIPTOGRAFI YANG ADA

Primanio
NIM : 13505027

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15027@students.if.itb.ac.id

Abstrak

Kriptografi klasik adalah cara penyamaran berita yang dilakukan oleh orang-orang dulu ketika belum ada komputer. Tujuannya adalah untuk melindungi informasi dengan cara melakukan penyandian. Di era komputer, informasi dikirimkan melalui jaringan dan disimpan di komputer. Tetapi kebutuhan akan keamanan data sama. Kriptografi pun dilakukan di era komputer tetapi dikenal sebagai kriptografi modern yang menggunakan algoritma matematika yang cukup rumit dan penggunaan kunci. Dengan demikian, kriptografi meliputi semua hal mengenai cara menghindari dan menemukan semua penipuan dan semua ketidakjujuran yang terjadi pada suatu pengiriman informasi baik secara manual pada kriptografi klasik ataupun secara matematika pada kriptografi modern. Dan pada dasarnya yang dilakukan pada kedua-duanya sama yaitu transposisi dan substitusi huruf untuk menghasilkan berita acak yang tidak bisa dibaca. Kriptografi modern banyak digunakan dalam pengiriman informasi melalui Internet. Makalah ini akan kembali mengulas tentang kriptografi klasik, namun dengan kombinasi-kombinasi baru yang tingkat keamanannya menigkat sehingga masih relevan dengan masalah-masalah privas ringan di era modern ini.

Kata kunci: kriptografi, *chypertext*, enkripsi, dekripsi, *caesar cryptograph, Vigenère, autokey cryptograph, ASCII*

1. Pendahuluan

Kemajuan teknologi di bidang komputer memungkinkan ribuan orang dan komputer di seluruh dunia terhubung dalam satu dunia maya yang dikenal sebagai *cyberspace* atau Internet. Begitu juga ratusan organisasi seperti perusahaan, lembaga negara, lembaga keuangan, militer dan sebagainya.Tetapi sayangnya, kemajuan teknologi selalu diikuti dengan sisi buruk dari teknologi itu sendiri. Salah satunya adalah rawannya keamanan data sehingga menimbulkan tantangan dan tuntutan akan tersedianya suatu sistem pengamanan data yang sama canggihnya dengan kemajuan teknologi komputer itu sendiri. Ini adalah latar belakang berkembangnya sistem keamanan data untuk melindungi data yang ditransmisikan melalui suatu jaringan komunikasi. Ada beberapa cara melakukan pengamanan data yang melalui suatu saluran, salah satu diantaranya adalah kriptografi. Dalam kriptografi, data yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa sehingga kalaupun data itu bisa dibaca maka tidak bisa dimengerti oleh pihak yang tidak berhak. Data yang akan dikirimkan dan belum mengalami penyandian dikenal dengan isitilah *plaintext*, dan setelah disamarkan dengan suatu cara penyandian, maka plaintext ini akan berubah menjadi *ciphertext*.

Kriptografi mempunyai sejarah yang panjang, mulai dari kriptografi Caesar yang berkembang pada zaman sebelum Masehi sampai kriptografi modern yang digunakan dalam komunikasi antar komputer di abad 20. Kata kriptografi sendiri berasal dari bahasa Yunani, yaitu *kryptós* yang berarti tersembunyi, dan *gráphein* yang berarti

menulis. Jadi Kriptografi berarti penulisan rahasia.

Pembakuan penulisan pada kriptografi dapat ditulis dalam bahasa matematika. Fungsi-fungsi yang mendasar dalam kriptografi adalah enkripsi dan dekripsi. Enkripsi adalah proses mengubah suatu *plaintext* menjadi suatu pesan dalam *ciphertext*.

C = E (M)

Dimana:
M = pesan asli
E = proses enkripsi
C = pesan dalam bahasa sandi (untuk ringkasnya disebut sandi)

Sedangkan dekripsi adalah proses mengubah pesan dalam suatu bahasa sandi menjadi pesan asli kembali.

M = D (C)

Dimana:
D = proses dekripsi

Umumnya, selain menggunakan fungsi tertentu dalam melakukan enkripsi dan dekripsi, seringkali fungsi itu diberi parameter tambahan yang disebut dengan istilah kunci.

Misalnya teks asli: “pengalaman adalah guru yang terbaik”. Setelah disandikan dengan algoritma sandi xyz dan dengan kunci pqr menjadi teks sandi: V583ehao8@$%.

Ada dua cara yang paling dasar pada kriptografi klasik. Yang pertama adalah transposisi. Transposisi adalah mengubah susunan huruf pada plaintext sehingga urutannya berubah.

Cara kedua adalah cara substitusi yaitu setiap huruf pada plaintext akan digantikan dengan huruf lain berdasarkan suatu cara atau rumus tertentu. Ada dua macam substitusi yaitu *polyalphabetic substitution cipher* dan *monoalphabetic substitution cipher*. Pada polyalphabetic substitution cipher, enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda sehingga lebih sulit untuk menemukan pola enkripsinya. Pada monoalphabetic substitution cipher maka satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain, sehingga pola enkripsinya lebih mudah diketahui, karena satu huruf pada ciphertext pasti merepresentasikan satu huruf pada plaintext.

Kriprografi/penyandian termasuk metode pengamanan yang tangguh. Disebut tangguh karena, sekali data tersebut disandikan dengan algoritma sandi yang baik, data tersebut akan tetap aman kendati setiap orang dapat mengaksesnya secara bebas. Dan selama algoritma sandi tersebut tetap terjaga, data yang disandikan akan tetap aman.

Kriptografi biasanya hanya diterapkan pada data-data yang dinilai penting dan sensitif, yang perlu dilindungi dari akses pihak-pihak yang tidak diinginkan dan dari potensi ancaman pencurian oleh pihak-pihak yang memperoleh akses terhadapnya. Secara prinsip, keamanan data yang disandi sangat tergantung dari terjaganya kerahasiaan kunci dan algoritma sandinya. Dapat dikatakan bahwa kriptografi hanya mengubah masalah keamanan. Yaitu mengubah dari melindungi data rahasia (besar,kompleks dan banyak) menjadi melindungi algoritma sandi dan kunci (satu hal). Biasanya data-data dilindungi baik kerahasiaannya maupun integritasnya. Tetapi terkadang data tertentu tidak perlu dirahasiakan namun perlu dijaga integritasnya. Kriptografi dapat juga digunakan untuk menjamin integritas data yaitu agar data tidak dimanipulasi oleh pihak-pihak yang tidak diinginkan. Kriptografi tidak menjamin keamanan 100 %, sebab tidak ada pengamanan yang sempurna. Perkembangan teknologi pengamanan selalu diimbangi dengan teknologi untuk membongkar keamanan yang diterapkan. Selain itu tingkat kesadaran individu yang bersentuhan dengan data-data yang diamankan tersebut, sangat menentukan lambat atau cepatnya sebuah pengamanan terbongkar

2. Kriptografi Klasik

2.1. Kriptografi Reverse

Ini adalah contoh kriptografi klasik yang menggunakan transposisi yaitu mengganti satu huruf dengan huruf lain. Ini contoh yang paling sederhana dari transposisi yaitu mengubah suatu kalimat dengan menuliskan setiap kata secara terbalik

Contoh Kriptografi Reverse:

Plaintext:	IBU AKAN DATANG BESOK PAGI
Ciphertext:	UBI NAKA GNATAD KOSEB IGAP

2.2. Kriptografi Kolom

Pada kriptografi kolom (column cipher), plaintext disusun dalam kelompok huruf yang terdiri dari beberapa huruf. Kemudian huruf-huruf dalam kelompok ini dituliskan kembali kolom per kolom, dengan urutan kolom yang bisa berubah-ubah. Kriptografi kolom adalah salah satu contoh kriptografi yang menggunakan metode transposisi.

Contoh Kriptografi Kolom:
Kalimat 'AYAH SUDAH TIBA KEMARIN SORE', jika disusun dalam kolom 7 huruf, maka akan menjadi kolom-kolom berikut :

AYAHSUD
AHTIBAK
EMARINS
OREAAAA

Untuk melengkapi kolom terakhir agar berisi 7 huruf, maka sisanya diisi dengan huruf 'A' atau bisa huruf apa saja sebagai huruf pelengkap. Kalimat tesebut setelah dienkripsi dengan 7 kolom huruf dan urutan kunci 6725431, maka hasil enkripsinya:

DKSAATAEUANASBIAHIRAAAEOYHMR

2.3. Kriptografi Caesar

Salah satu kriptografi yang paling tua dan paling sederhana adalah kriptogtafi Caesar. Menurut sejarah, ini adalah cara Julius Caesar mengirimkan surat penting pada para gubernurnya. Dalam kriptografi Caesar, maka setiap huruf akan dituliskan dalam huruf lain hasil pergeseran 3 buah huruf. Kriptografi Caesar ini adalah kriptografi substitusi karena setiap huruf akan digantikan huruf lain. Sebagai contoh, huruf A akan digeser 3 huruf menjadi huruf D, B akan digeser 3 huruf menjadi E, J akan digeser menjadi M, O akan menjadi R dan seterusnya. Pergeseran ini juga berputar kembali ke awal abjad sehingga sesudah huruf Z diikuti kembali oleh huruf A. Kriptografi Caesar ini dikenal sebagai monoalphabetic substitution cipher karena satu huruf tertentu pasti akan berubah menjadi huruf tertentu yang lain.

Perubahan pada kriptografi Caesar bisa dituliskan sebagai berikut:

Plaintext	:	ABCDEFGHIJKLMNOPQRSTUVWXYZ
Ciphertext	:	DEFGHIJKLMNOPQRSTUVWXYZABC
Plaintext	:	KITA JUMPA BESOK PAGI
Ciphertext	:	NLWD MXPSD EHVRN SDJL

Jika kita memberi nomor ke pada huruf-huruf abjad dan kita mulai dengan huruf A=0, B=1, C=2 dstnya sampai dengan Z=25, maka kriptografi Caesar memenuhi rumus sebagai berikut : $C = (P + 3) \bmod 26$, di mana C adalah nomor abjad ciphertext, P adalah nomor abjad plaintext . Dan dekripsinya adalah $P = (C - 3) \bmod 26$. Kripotogtafi Caesar ini kemudian berkembang di mana pergeseran tidak hanya 3 huruf tetapi ditentukan oleh suatu kunci yang adalah suatu huruf. Huruf ini yang menentukan pergeseran dari huruf pada plaintext. Jika kunci adalah A maka pergeseran adalah 0, B pergeseran adalah 1, C 2 dan seterusnya. Rumus di atas tetap berlaku tetapi pergeseran huruf ditentukan oleh nilai pergeseran k (lihat tabel 1) dan bisa berubah-ubah sesuai kunci yang digunakan.

Tabel pergeseran huruf pada kriptografi Caesar:

Kunci	A	B	C	D	E	F	G	H	I
Pergeseran k	0	1	2	3	4	5	6	7	8
Kunci	J	K	L	M	N	O	P	Q	R
Pergeseran k	9	10	11	12	13	14	15	16	17
Kunci	S	T	U	V	W	X	Y	Z	
Pergeseran k	18	19	20	21	22	23	24	25	

Rumus kriptografi Caesar, secara umum bisa dituliskan sebagai berikut:

C = E(P) = (P + k)mod 26
P = D(C) = (C − k)mod26

di mana **P** adalah plaintext, **C** adalah ciphertext, **k** adalah pergeseran huruf sesuai dengan kunci yang
dikehendaki.

2.4. Kriptografi Vigenère

Sistem sandi ini pertama kali dipopulerkan oleh Blaise de Vigenère seorang diplomat Perancis pada abad 15, sehingga disebutlah metode ini dengan sistem sandi Vigenère. Sistem sandi Vigenère adalah sistem sandi substitusi multi-alfabet, yaitu sistem sandi Caesar tetapi dengan pergeseran alfabet yang berlainan disesuaikan dengan kata kuncinya.

Pada kriptografi Caesar pergeseran akan sama pada seluruh pesan. Jika kunci yang digunakan adalah huruf E, maka setiap huruf pada pesan akan bergeser 4 huruf. Begitu juga bila digunakan kunci-kunci lainnya. Pada kriptografi Vigenere, plaintext akan dienkripsi dengan pergeseran huruf seperti pada kriptografi Caesar tetapi setiap huruf di dalam plaintext akan mengalami pergeseran yang berbeda. Kunci pada kriptografi Vigenere adalah sebuah kata bukan sebuah huruf. Kata kunci ini akan dibuat berulang sepanjang plaintext, sehingga jumlah huruf pada kunci akan sama dengan jumlah huruf pada plaintext. Pergeseran setiap huruf pada plaintext akan ditentukan oleh huruf pada kunci yang mempunyai posisi yang sama dengan huruf pada plaintext. Kriptografi Vigenere ini dikenal sebagai polyalphabetic substitution cipher, karena enkripsi terhadap satu huruf yang sama bisa menghasilkan huruf yang berbeda. Pergeseran huruf pada plaintext ditentukan oleh tabel yang sama dengan tabel pada kriptografi Caesar.

Rumus kriptografi Caesar tetap berlaku pada kriptografi Vigenere, baik pada enkripsi maupun dekripsi.

Sebagai contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kunci ini akan diulang sama panjang dengan plaintext. Setiap huruf pada kata BESOK mempunyai pergeseran yang berbeda, sehingga setiap huruf akan mengalami pergeseran yang berbeda. Huruf yang sama bisa menghasilkan cipher yang berbeda. Hasil enkripsinya seperti berikut:

Plaintext	I	N	I		P	E	S	A	N
Kunci	B	E	S		O	K	B	E	S
Pergeseran k	1	4	18		14	10	1	4	18
Ciphertext	J	R	A		D	O	T	E	F
Plaintext	R	A	H	A	S	I	A		
Kunci	O	K	B	E	S	O	K		
Pergeseran k	14	10	1	4	18	14	10		
Ciphertext	F	K	I	E	K	W	k		

Ada cara lain untuk melakukan kriptografi Vigenere yaitu dengan menuliskan abjad berurutan dari A sampai Z, kemudian kata kuncinya dituliskan secara vertikal di bawah huruf A. Setiap huruf dari kata kunci ini kemudian dilengkapi dengan abjad selanjutnya dalam urutan alfabet dan setelah huruf Z kembali lagi ke huruf A,B dan seterusnya. Jika kita menggunakan kata kunci BESOK, maka akan dituliskan sebagai berikut :

ABCDEFGHIJKLMNOPQRSTUVWXYZ ----------> Alfabet
BCDEFGHIJKLMNOPQRSTUVWXYZA
EFGHIJKLMNOPQRSTUVWXYZABCD
STUVWXYZABCDEFGHIJKLMNOPQR
OPQRSTUVWXYZABCDEFGHIJKLMN
KLMNOPQRSTUVWXYZABCDEFGHIJ

Untuk melakukan enkripsi terhadap suatu pesan, maka cari posisi setiap huruf pada plaintext pada baris paling atas, kemudian cari huruf pada lokasi yang sama di baris bawahnya. Huruf pertama diubah dengan huruf yang ada pada posisi yang sama pada baris ke dua atau baris dari huruf pertama pada kata kunci. Huruf ke dua pada

plaintext dikonversi dengan huruf pada posisi yang sama pada baris selanjutnya. Huruf ketiga dikonversi dengan baris ke tiga dan seterusnya. Jika semua baris sudah terpakai maka kembali ke baris paling atas dari kata kunci, sampai semua huruf pada plaintext dienkripsi.

Cara lain untuk melakukan kriptografi Vigenere adalah dengan menggunakan *tabula recta* sebagai berikut : Baris paling atas adalah alfabet dari A sampai dengan Z. Di baris ke dua, tuliskan alfabet mulai dengan B sampai dengan Z kemudian kembali ke A. Di baris bawahnya C diikuti alfabet selanjutnya sampai dengan Z dan kembali lagi ke A. Sampai huruf Z. Cara penulisan ini dikenal sebagai *tabula recta*. Kemudian enkripsi dilakukan sama dengan enkripsi menggunakan Table 4. Huruf-huruf pada kata kunci sebagai huruf pertama pada baris-baris pada tabula recta dan huruf-huruf pada plaintext dicari di baris pertama tabula recta. Berikut digambarkan Tabula Recta:

ABCDEFGHIJKLMNOPQRSTUVWXYZ
BCDEFGHIJKLMNOPQRSTUVWXYZA
CDEFGHIJKLMNOPQRSTUVWXYXAB
D .....
.....
.....
XYZABCDEFGHIJKLMNOPQRSTUVW
YZABCDEFGHIJKLMNOPQRSTUVWX
ZABCDEFGHIJKLMNOPQRSTUVWXY

Penggunaan lebih dari satu huruf dalam suatu enkripsi ini yang membuat kriptografi Vigenere disebut polyalphabetic cipher. Keuntungan dari kriptografi polyalphabetic cipher adalah sulitnya melakukan analisa frekwensi (*frequency analysis*) terhadap munculnya suatu huruf dalam ciphertext. Analisa frekwensi adalah suatu cara untuk melakukan cryptanalysis terhadap suatu ciphertext dengan menghitung berapa sering suatu huruf muncul pada ciphertext tersebut dengan memperbandingkan dengan berapa sering suatu huruf muncul dalam pesan atau tulisan normal. Contohnya jika huruf P sering muncul pada suatu ciphertext dalam bahasa Inggeris, huruf P ini sangat mungkin adalah huruf E, karena huruf E adalah huruf yang paling sering digunakan dalam tulisan-tulisan bahasa Inggeris. Analisa frekwensi ini sulit dilakukan dalam kriptografi Vigenere karena satu huruf tertentu pada plaintext bisa berubah menjadi beberapa huruf-huruf lain pada ciphertext tergantung pada kata kuncinya, sehingga frekwensi suatu huruf yang muncul pada ciphertext tidak merepresentasikan suatu huruf pada plaintext.

Kriptografi Vigenere ini bukan yang terbaik yang dihasilkan oleh Vigenere. Dia mengembangkan kriptografi lain yang dikenal sebagai kriptografi Autokey yang konon lebih handal dari pada kriptografi Vigenere, tetapi nama Vigenere sudah terlanjur melekat pada kriptografi sebelumnya. Sampai dengan kurun waktu 300 tahun, kedua kriptografi ini dianggap *'unbreakable'*, tetapi pada pertengahan abad 19, Charles Babbage dan Friedrich Kasiski secara terpisah mampu memecahkan cara penyandian ini.

2.5. Kriptografi Autokey

Kriptografi Autokey adalah pengembangan dari kriprografi Caesar dan Vigenere. Cara melakukan enkripsi sama dengan kedua kriptografi sebelumnya. Pada kriptografi Autokey juga digunakan sebuah kata sebagai kunci. Kunci ini kemudian diikuti dengan plaintext sehingga membentuk huruf-huruf yang sama panjang dengan plaintext. Urutan huruf-huruf ini yang akan digunakan sebagai kunci pada saat enkripsi.

Rumus yang berlaku untuk kriptografi Autokey sama dengan untuk Caesar dan Vigenere. Tabel pergeseran huruf pun sama dengan Caesar dan Vigenere.

Contoh, jika plaintext adalah INI PESAN RAHASIA, maka jika kita gunakan kunci kata BESOK, maka kata BESOK akan disisipkan di depan plaintext INI PESAN RAHASIA. Kemudian enkripsi dilakukan sama dengan enkripsi Caesar dan Vigenere.

Prosesnya adalah sebagai berikut :

Plaintext	I	N	I		P	E	S	A	N
Kunci	B	E	S		O	K	I	N	I
Pergeseran k	1	4	18		14	10	8	13	8
Ciphertext	J	R	A		D	O	A	N	V
Plaintext	R	A	H	A	S	I	A		
Kunci	P	E	S	A	N	R	A		
Pergeseran k	15	4	18	0	13	17	0		
Ciphertext	G	E	Z	A	F	Z	A		

3. Kelemahan Kriptografi Klasik

Zaman dahulu, metode-metode kriptografi klasik ini sulit dipecahkan karena belum banyak yang bisa membaca. Para kurir raja sendiri pun kebanyakan dipilih dari kaum yang tidak bisa membaca, sehingga mereka tidak mengetahui isi dari pesan yang dikirimkan.
Saat ini, kebanyakan manusia sudah bisa membaca. Selain itu, sudah banyak teknologi yang mampu memecahkan metode kriptografi klasik ini. Semakin cepatnya pemrosesan suatu mesin, maka semakin mudah proses dekripsi dilakukan tanpa harus mengetahui kunci yang diberikan.

Kelemahan-kelemahan kriptografi klasik ini terletak pada algoritmanya yang terlalu sederhana. Selain itu kerahasiaan algoritmanya tidak terjamin dan mudah terbongkar.

Misalkan saja, pada kriptografi caesar, asalkan kita tahu beberapa huruf depan, maka kita akan mengetahui polanya, dan kunci akan dengan mudah ditemukan. Atau dengan menganalisis kemunculan huruf dalam suatu bahasa tertentu, maka akan didapatkan pola-pola tertentu yang diterapkan pada *chipertext* tersebut.

Kriptografi Caesar juga bisa dipecahkan dengan cara *brute-force.* Hanya ada 26 jenis Kunci. Kita bsa menciba satu-persatu kunci pada sebuah potongan kata di kalimat *chipertext.* Bila kita mendaatkan satu buah kata yang logis, maka kuncu tersebut mungkin merupakan kunci Kadang-kadang satu kunci yang potensial menghasilkan pesan yang bermakna tidak selalu satu buah. Untuk itu, kita membutuhkan informasi lainnya, misalnya konteks pesan tersebut atau mencoba mendekripsi potongan chiperteks lain untuk memperoleh kunci yang benar.

Atau kita tinjau kriptografi reverse. Secara fisik, kriptografi ini mudah dipecahkan. Dengan melihat kata-kata yang pendek, atau kata yang merupakan palindrome (bila ada) pada maka *chipertext,* maka akan dengan mudah diubah menjadi plaintext asal.

Mengapa kriptografi klasik mudah dipecahkan? Alasannya adalah sebagai berikut:

- Terdapat bagian pesan atau kata-kata yang berulang pada ciphertext-nya. Tanpa perulangan, akan sangat kesulitan untuk memperkirakan plaintext suatu kata. Bila diffusion berjalan baik. Maka akan sangat sulit untuk melihat perulangan-perulangan ini.

- Terdapat hubungan yang jelas antara plaintext dengan ciphertex-nya. Artinya, confusion (proses membingungkan pembaca) tidak berlangsung dengan baik. Plaintext yang sering muncul akan tercermin pada sering munculnya ciphertext.

- Terdapat keteraturan pada susunan plaintext, ciphertext ataupun kuncinya. Dalam setiap contoh pemecahan kode rahasia di atas, selalu menganggap terdapat keteraturan plaintext, misalnya susunan plaintext-nya beraturan dari “a” lalu “b” disusul “c” dan seterusnya. Keteraturan ciphertext yang juga mencerminkan keteraturan plaintext jugasangat membantu pemecahan kode rahasia ini.

- Jumlah ciphertext-nya terlalu banyak. Yang dimaksud terlalu banyak di sini karena sampai menimbulkan perulangan, baik perulangan kunci, perulangan plaintext, maupun perulangan ciphertext. Bila jumlah ciphertext-nya sedikit sehingga tidak menimbulkan perulangan baik plaintext, ciphertext, kunci, maupun pola-pola keteraturannya, maka pemecahan kode tentu akan sangat sulit sekali. Namun

apakah setiap pesan akan enkrip dengan sistem yang berbeda? Bagaimana bila memeiliki 1000 pesan perbulan? Haruskah menciptakan puluhan macam sistem enkripsi baru setiap bulannya?

- Bila mengetahui bahasa penyusun plaintext-nya, orang akan lebih mudah mendekripsinya. Dalam perang dunia kedua, Amerika tidak menggunakan bahasa Inggris, melainkan menggunakan bahasa Navajo (bahasa Indian) untuk keperluan militernya, sehingga Jerman dan Jepang yang menjadi lawannya tidak mempunyai petunjuk apapun mengenai kode rahasia Amerika Serikat.

- Kita mengetahui sistem enkripsi yang digunakan. Dalam kasus tertentu, penyembunyian algoritma enkripsi memang dapat meningkatkan keamanan sisitem, namun itu bukan hal yang mutlak! Sebab dari ciphertext-nya analis sandi dapat memperkirakan sistem enkripsi yang digunakan.

- Jumlah kemungkinan terkaan yang mungkin terjadi, terbatas. Dalam artian, semua kemungkinan sistem enkripsi yang digunakan dapat dicoba. Apalagi dengan penggunaan komputer, hampir semua kemungkinan sistem yang dijelaskan pada bab sebelum ini, dapat dicoba oleh komputer dalam waktu singkat Harus diingat, bahwa bila salah menerka sistem enkripsi yang digunakan, harus menggunakan perkiraan sistem yang lain. Dan ini tentunya mudah bila dilakukan dengan komputer. Bila dengan komputer pun diperlukan waktu satu tahun untuk memecahkan sandinya, sementara informasi hanya perlu diamankan selama 6 bulan, maka sistem aman. Dan bila sebaliknya, maka sistem tidak aman.

Kadang-kadang pemecah enkripsi (*kriptanalis*) melakukan terkaan untuk mengurangi jumlah kunci yang mungkin ada. Terkaan juga dilakukan kriptanalis untuk memperoleh sebanyak mungkin plainteks dari potongan chiperteks yang disadap. Plainteks yang diperoleh dari hasil terkaan ini biasanya digunakan dalam *known-plaintext attack*. Metode paling umum dalam memecahkan chipertext adalah Statistika. Selain itu *brute-force attack* juga dapat dilakukan oleh kriptanais bila cara sederhana sudah sulit untuk dilakukan. Hal ini mengurangi keamanan data hasil enkripsi metode klasik ini.

Akibat ketidakamanan ini, maka kriptografi klasik banyak ditinggalkan oleh penggunanya. Orang banyak beralih ke metode kriptografi modern. Padahal dengan sedikit modifkasi, maka tingkat keamanan kriptografi ini akan bisa dinaikkan.

4. Modifikasi Kriptografi Klasik

Kelemahan-kelemahan kriptografi klasik ini bisa dikurangi dengan mengkombinasikan metode-metode yang ada sehingga algoritma kriptografinya menjadi lebih rumit dan tidak dapat ditebak dengan sekali lihat. Konsekuesinya, modifikasi yang dilakukan pada metode yang ada akan meningkatkan keamanan dari enkripsi itu sendiri

Berikut ini adalah beberapa modifikasi dari metode kriptografi klasik

4.1. Kriptografi Kombinasi

Beberapa Kelemahan kriptografi klasik bisa ditutupi dengan mengombinasikannnya. Sebab, kekurangan sebuah metode kriptogafi klasik dapat ditutupi oleh kelebihan kriptografi lain.

Selain itu, dengan mengombinasikan metode enkripsi, artinya kita melakukan enkripsi berlapis ganda.

Sebagai contoh, metode Autokey dapat dikombinasikan dengan metode reverse. Kelemahan metode reverse akan ditutupi oleh kesulitan memecahkan enkripsi autokey. Huruf-huruf pada hasil enkripsi Autokey pun akan tersamarkan posisinya karena proses enkripsi dan dekripsi yang sebenarnya dilakukan dari belakang, bukan dari depan seperti enkripsi autokey normal.

4.2. Kriptografi One-Time Pad

One-Time Pad adalah kriptografi yang merupakan perbaikan terhadap kriptografi Caesar. One-Time Pad menggunakan kunci yang mempunyai panjang sama dengan plaintext dan kunci ini hanya digunakan 1 kali. Karena itu, cara enkripsi ini dikenal sebagai One-Time Pad dan kriptografi ini tidak bisa dipecahkan karena kunci hanya digunakan satu kali sehingga tidak ada suatu pola tertentu. Satu-satunya cara melakukan dekripsi adalah dengan mengetahui kunci yang digunakan.

Enkripsi dilakukan dengan cara sama dengan enkripsi Caesar, tetapi karena panjang kunci sama dengan plaintext, maka setiap huruf pada plaintext akan mengalami pergeseran yang berbeda.

Memang One-Time Pad adalah kriptografi yang tidak pernah bisa dipecahkan. Kunci hanya bisa digunakan sekali dan harus mempunyai panjang yang sama dengan plaintextnya. One-Time Pad ini biasanya digunakan dalam situasi yang kritis. Biasanya keputusan-keputusan militer seperti peluncuran peluru kendali nuklir di era perang dingin. Sampai sekarang One-Time Pad ini masih digunakan oleh kedutaan-kedutaan besar untuk pengiriman berita diplomatik.

4.3. Kriptografi Random Subtitution

Ide dari metode kriptografi ini adalah menyusun abjad secara acak. Huruf-huruf awalnya diambil dari huruf-huruf yang muncul pada kunci, setelah itu dilanjutkan dengan huruf alfabet sisanya.

Misalnya pada kunci yang berupa kalimat kalimat AYAH SUDAH PULANG, huruf-huruf yang muncul adalah: A, Y, H, S, U, D, P, L, N, G

Jika dibuat dalam tabel konversi :

```
n:ABCDEFGHIJKLMONPQRSTUVWXYZ
k:AYHSUDPLNGBCEFIJKMOQRTVWXZ
```

Huruf-huruf yang berkorespondensi dengan key di bawah akan disubtitusi oleh korespondennya.

Misalnya pada plaintext “IBU SEDANG MEMASAK” setelah didekripsi akan menghasilkan “NYR OUSAIP EUEAOAQ”

Kriptografi ini memiliki tingkat kerumitan yang tidak terlalu tinggi tetapi memiliki kombinasi kemungkinan yang sangat banyak. Bila huruf alfabet ada 26, maka kombinasi kunci ini ada 26! buah atau sekitar 403.291.461.126.605.635.584.000.000 buah kombinasi. Bila sebuah mesin pemecah bisa memproses sekitar 1 bilyun kemungkinan per detik, maka dibutuhkan waktu 403.291.461.126,606 detik atau 306.918,920 tahun untuk menyelesaikannya.

4.4. Penerapan Pada Karakter Selain Alfabet

Pada kriptografi klasik biasa, kebanyakan plaintext hanya berisi alfabet saja. Bila kita masukkan angka atau karakter lain, maka teks tidak bisa dienkripsi.

Untuk mengakomodasi hal ini, maka kita akan menggunakan standar ASCII untuk merepresentasikan karakter-karakter standar yang ada. Untuk karakter standar ASCII, ada 128 karakter yang ada. Berikut adalah tabel karakter ASCII :

Binary	Oct	Dec	Hex	Abbr	PR[1]	CS[2]	CEC[3]	Description
0000 0000	000	0	00	NUL	NUL	^@		Null character
0000 0001	001	1	01	SOH	SOH	^A		Start of Header
0000 0010	002	2	02	STX	STX	^B		Start of Text
0000 0011	003	3	03	ETX	ETX	^C		End of Text
0000 0100	004	4	04	EOT	EOT	^D		End of Transmission
0000 0101	005	5	05	ENQ	ENQ	^E		Enquiry
0000 0110	006	6	06	ACK	ACK	^F		Acknowledgment
0000 0111	007	7	07	BEL	BEL	^G	\a	Bell
0000 1000	010	8	08	BS	BS	^H	\b	Backspace[4][8]
0000 1001	011	9	09	HT	HT	^I	\t	Horizontal Tab
0000 1010	012	10	0A	LF	LF	^J	\n	Line feed
0000 1011	013	11	0B	VT	VT	^K		Vertical Tab
0000 1100	014	12	0C	FF	FF	^L	\f	Form feed

0000 1101	015	13	0D	CR	CR	^M	\r	Carriage return[7]
0000 1110	016	14	0E	SO	SO	^N		Shift Out
0000 1111	017	15	0F	SI	SI	^O		Shift In
0001 0000	020	16	10	DLE	DLE	^P		Data Link Escape
0001 0001	021	17	11	DC1	DC1	^Q		Device Control 1 (oft. XON)
0001 0010	022	18	12	DC2	DC2	^R		Device Control 2
0001 0011	023	19	13	DC3	DC3	^S		Device Control 3 (oft. XOFF)
0001 0100	024	20	14	DC4	DC4	^T		Device Control 4
0001 0101	025	21	15	NAK	NAK	^U		Negative Acknowledgement
0001 0110	026	22	16	SYN	SYN	^V		Synchronous Idle
0001 0111	027	23	17	ETB	ETB	^W		End of Trans. Block
0001 1000	030	24	18	CAN	CAN	^X		Cancel
0001 1001	031	25	19	EM	EM	^Y		End of Medium
0001 1010	032	26	1A	SUB	SUB	^Z		Substitute
0001 1011	033	27	1B	ESC	ESC	^[	\e	Escape[6]
0001 1100	034	28	1C	FS	FS	^\		File Separator
0001 1101	035	29	1D	GS	GS	^]		Group Separator
0001 1110	036	30	1E	RS	RS	^^		Record Separator
0001 1111	037	31	1F	US	US	^_		Unit Separator
0111 1111	177	127	7F	DEL	DEL	^?		Delete[5][8]

Binary	Dec	Hex	Glyph
0110 0000	96	60	`
0110 0001	97	61	a
0110 0010	98	62	b
0110 0011	99	63	c
0110 0100	100	64	d
0110 0101	101	65	e
0110 0110	102	66	f
0110 0111	103	67	g
0110 1000	104	68	h
0110 1001	105	69	i
0110 1010	106	6A	j
0110 1011	107	6B	k
0110 1100	108	6C	l
0110 1101	109	6D	m
0110 1110	110	6E	n
0110 1111	111	6F	o
0111 0000	112	70	p
0111 0001	113	71	q
0111 0010	114	72	r
0111 0011	115	73	s
0111 0100	116	74	t
0111 0101	117	75	u
0111 0110	118	76	v
0111 0111	119	77	w
0111 1000	120	78	x
0111 1001	121	79	y
0111 1010	122	7A	z
0111 1011	123	7B	{
0111 1100	124	7C	|
0111 1101	125	7D	}
0111 1110	126	7E	~

Binary	Dec	Hex	Glyph
0010 0000	32	20	(blank) (SP)
0010 0001	33	21	!
0010 0010	34	22	"
0010 0011	35	23	#
0010 0100	36	24	$
0010 0101	37	25	%
0010 0110	38	26	&
0010 0111	39	27	'
0010 1000	40	28	(
0010 1001	41	29	)
0010 1010	42	2A	*
0010 1011	43	2B	+
0010 1100	44	2C	,
0010 1101	45	2D	-
0010 1110	46	2E	.
0010 1111	47	2F	/
0011 0000	48	30	0
0011 0001	49	31	1
0011 0010	50	32	2
0011 0011	51	33	3
0011 0100	52	34	4
0011 0101	53	35	5
0011 0110	54	36	6
0011 0111	55	37	7
0011 1000	56	38	8
0011 1001	57	39	9
0011 1010	58	3A	:
0011 1011	59	3B	;
0011 1100	60	3C	<
0011 1101	61	3D	=
0011 1110	62	3E	>
0011 1111	63	3F	?

Binary	Dec	Hex	Glyph
0100 0000	64	40	@
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z
0101 1011	91	5B	[
0101 1100	92	5C	\
0101 1101	93	5D	]
0101 1110	94	5E	^
0101 1111	95	5F	_

Dengan pemanfaatan karakter-karakter ASCII ini, kriptografi klasik masih bisa digunakan di zaman modern seperti sekarang. Keterbatasan penggunaan hanya pada alfabet bisa dieliminasi dengan cara ini. Selain itu, kerumitan algoritma juga akan semakin meningkat karena jumlah kemungkinan-kemungkinan yang ada menjadi semakin besar. Mungkin metode kriptografi klasik – selain Caesar – akan menjadi sulit untuk ditembus bila kemungkinannya menjadi 128!.

Karakter ASCII ini sudah menjadi standar dalam penggunaan teknologi yang umum. Semua pengguna teknologi rata-rata mengetahui standar ASCII sehingga proses enkripsi-dekripsi bisa dilakukan dengan baik.

Lebih luasnya lagi, karakter ASCII memiliki *extended character* yang jumlahnya 128, sehingga jumlah total karakter yang bisa digunakan adalah 256. Sangat bantak jika dibandingkan dengan karakter alfabet yang “hanya” berjulah 26.

Beberapa metode kriptografi modern menggunakan enkripsi dengan cara ini. File-file sistem, file rahasia atau *password* sandi-lewat *(password)* disimpan dan digunakan dengan cara ini.

5. Kesimpulan

Kriptografi klasik adalah cara penyamaran berita yang dilakukan oleh orang-orang dulu ketika belum ada komputer. Tujuannya adalah untuk melindungi informasi dengan cara melakukan penyandian. Penyandian dilakukan secara manual. Caranya adalah dengan cara transposisi dan substitusi huruf. Pada penggunaan transposisi, posisi huruf diubah-ubah, sementara pada substitusi, huruf digantikan dengan huruf atau simbol lain sehingga informasi sulit dibaca dan dikenali karena tampak diacak-acak.

Di era modern, kriptografi tidak dilakukan secara manual, melainkan dengan algoritma yang rumit dan penggunan kunci yang sangat aman. Kriptografi modern ini banyak digunakan dalam pertukaran data melalui jaringan internet. Saat ini, metode kriptografi modern ini dianggap sudah sangat aman.

Namun, keamanan kriptografi klasik tidak bisa dipandang sebelah mata. Dengan sedikit modifikasi, maka metode kriptografi klasik masih bisa digunakan di zaman komputer seperti sekarang ini sebagai alternatif dari kriptografi modern yang sudah ada.

Salah satu doktrin ancaman terhadap keamanan adalah "**merasa aman/kuat merupakan kelemahan pengamanan**". Merasa aman/kuat akan memberikan rasa percaya diri yang berlebihan dan akibatnya akan mengabaikan prosedur pengamanan berikutnya. Kita tidak boleh merasa kuat agar kita selalu waspada.

Daftar Pustaka

[1] Munir, Rinaldi.
2004. *Diktat Kuliah IF2153 Matematika Diskrit – Edisi Keempat*. Bandung: Program Studi Tenik Informatika, STEI ITB.

2004. *Sistem Chiper Klasik.* http://kur2003.if.itb.ac.id/file/Sistem%20Chiper%20Klasik.doc

[2] Febrian, Jack.
2004. *Pengetahuan Komputer dan Teknologi Informasi.* Bandung: Informatika.

[3] Abdul Kadir.
2002. *Pengenalan Sistem Informasi.* Yogyakarta: Penerbit Andi.

[4] ---.
23 Desember 2006. *Pengamanan Informasi dan Kriptografi - Menambah khasanah bacaan kriptologi dan pengamanan informasi bagi masyarakat Indonesia*. http://hadiwibowo.wordpress.com/

Desember 2006. http://ilmukomputer.com

1 Januari 2006. http://www.geocities.com/amwibowo/

2 Januari 2006. http://www.cert.or.id/~budi/courses/ec7010/