KRIPTOGRAFI SEBAGAI MEDIA PEMBELAJARAN DALAM STUDI MATEMATIKA TINGKAT SEKOLAH

Twindania Namiesyva – NIM : 13505086

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if15086@students.if.itb.ac.id

Abstrak

Makalah ini membahas tentang implementasi *Kriptografi* sebagai media pembelajaran matematika untuk tingkat sekolah. *Kriptografi* adalah ilmu dan seni menjaga kerahasiaan berita. Implementasi kriptografi dalam makalah ini meliputi contoh – contoh penerapan kriptografi sebagai media pembelajaran matematika tingkat pemula dan untuk tingkat SMA. Sebelum membahas implementasi kriptografi, makalah ini terlebih dahulu menerangkan ilmu kriptografi itu sendiri.

Kriptografi mempunyai potensi yang sangat besar dalam memperkaya pendidikan matematika. Selain berkaitan langsung dengan matematika, kriptografi juga dapat digunakan sebagai metode baru pengajaran matematika pada tingkat sekolah. Metode kriptografi diyakini dapat memberikan nuansa baru pada pelajaran matematika, dan dapat mengubah cara pandang para murid terhadap pelajaran matematika ke arah yang lebih positif. Selain itu, dengan kriptografi diharapkan para murid dapat berpikir lebih kritis dan kreatif.

***Kata kunci**: Kriptografi, matematika, chiper substistusi, chiper transposisi, block-chiper, stream-chiper, sandi Caesar, sandi Vigenère*

1. Kriptografi

Kriptografi, secara umum adalah ilmu dan seni untuk menjaga kerahasiaan berita.

Ada empat tujuan mendasar dari ilmu kriptografi ini yang juga merupakan aspek keamanan informasi yaitu :

- Kerahasiaan, adalah layanan yang digunakan untuk menjaga isi dari informasi dari siapapun kecuali yang memiliki otoritas atau kunci rahasia untuk membuka/mengupas informasi yang telah disandi.
- Integritas data, adalah berhubungan dengan penjagaan dari perubahan data secara tidak sah. Untuk menjaga integritas data, sistem harus memiliki kemampuan untuk mendeteksi manipulasi data oleh pihak-pihak yang tidak berhak, antara lain penyisipan, penghapusan, dan pensubsitusian data lain kedalam data yang sebenarnya.
- Autentikasi, adalah berhubungan dengan identifikasi/pengenalan, baik secara kesatuan sistem maupun informasi itu sendiri. Dua pihak yang saling berkomunikasi harus saling memperkenalkan diri. Informasi yang dikirimkan melalui kanal harus diautentikasi keaslian, isi datanya, waktu pengiriman, dan lain-lain.
- Non-repudiasi., atau nirpenyangkalan adalah usaha untuk mencegah terjadinya penyangkalan terhadap pengiriman/terciptanya suatu informasi oleh yang mengirimkan/membuat.

1.1 Algoritma Sandi

Algoritma sandi adalah algoritma yang berfungsi untuk melakukan tujuan kriptografis. Algoritma tersebut harus memiliki kekuatan untuk melakukan (dikemukakan oleh Shannon):

- konfusi/pembingungan (confusion), dari teks terang sehingga sulit untuk

direkonstruksikan secara langsung tanpa menggunakan algoritma dekripsinya
- difusi/peleburan (difusion), dari teks terang sehingga karakteristik dari teks terang tersebut hilang.

sehingga dapat digunakan untuk mengamankan informasi. Pada implementasinya sebuah algoritmas sandi harus memperhatikan kualitas layanan/Quality of Service atau QoS dari keseluruhan sistem dimana dia diimplementasikan. Algoritma sandi yang handal adalah algoritma sandi yang kekuatannya terletak pada kunci, bukan pada kerahasiaan algoritma itu sendiri. Teknik dan metode untuk menguji kehandalan algoritma sandi adalah kriptanalisa.

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara dua himpunan yaitu yang berisi elemen teks terang /plaintext dan yang berisi elemen teks sandi/ciphertext. Enkripsi dan dekripsi merupakan fungsi transformasi antara himpunan-himpunan tersebut. Apabila elemen-elemen teks terang dinotasikan dengan P, elemen-elemen teks sandi dinotasikan dengan C, sedang untuk proses enkripsi dinotasikan dengan E, dekripsi dengan notasi D.

Enkripsi : $E(P) = C$

Dekripsi : $D(C) = P$ atau $D(E(P)) = P$

Secara umum berdasarkan kesamaan kuncinya, algoritma sandi dibedakan menjadi :

- kunci-simetris/symetric-key, sering disebut juga algoritma sandi konvensional karena umumnya diterapkan pada algoritma sandi klasik
- kunci-asimetris/asymetric-key

Berdasarkan arah implementasi dan pembabakan jamannya dibedakan menjadi :

- algoritma sandi klasik
- algoritma sandi modern

Berdasarkan kerahasiaan kuncinya dibedakan menjadi :

- algoritma sandi kunci rahasia/secret-key
- algoritma sandi kunci publik/publik-key

Pada skema kunci-simetris, digunakan sebuah kunci rahasia yang sama untuk melakukan proses enkripsi dan dekripsinya. Sedangkan pada sistem kunci-asimentris digunakan sepasang kunci yang berbeda, umumnya disebut kunci publik(public key) dan kunci pribadi (private key), digunakan untuk proses enkripsi dan proses dekripsinya. Bila elemen teks terang dienkripsi dengan menggunakan kunci pribadi maka elemen teks sandi yang dihasilkannya hanya bisa didekripsikan dengan menggunakan pasangan kunci pribadinya. Begitu juga sebaliknya, jika kunci pribadi digunakan untuk proses enkripsi maka proses dekripsi harus menggunakan kunci publik pasangannya.

1.1.1 Algoritma sandi kunci-simetris

Skema algoritma sandi akan disebut kunci-simetris apabila untuk setiap proses enkripsi maupun dekripsi data secara keseluruhan digunakan kunci yang sama. Algoritma – algoritma yang termasuk dalam algoritma sandi kunci-asimetris diantaranya adalah :

1. Chiper Substitusi (kriptografi klasik)
2. Chiper Tranposisi (kriptografi klasik)
3. Block-Chiper (kriptografi modern)
4. Stream-Chiper (kriptografi modern)

1.1.1.1 Chiper Substitusi

Chiper Substitution adalah sandi dimana setiap karakter dari plaintext (huruf atau angka) diganti atau disubstistusi dengan karakter lain dalam susunan abjad. Tidak ada perubahan dalam susunan abjad asli yang digunakan pada plaintext. Contoh dari Chiper Substitusi adalah sandi Caesar, sandi Vigenère.

1.1.1.2 Chiper Transposisi

Chiper Tansposisi mengubah kembali susunan huruf dari plaintext, tanpa mengganti hurufnya sendiri. Contohnya, chipper transposisi yang sangat sederhana adalah *rail fence*, dimana plaintext ditulis kembali namun dalam dua baris, dengan cara penulisan satu per satu huruf dituliskan di baris yang berbeda secara berurutan. Dalam dua baris rail fence pesan INFORMATIKA menjadi:

I F R A I A

N O M T K

Yang dibaca : IFRAIANOMTK.

1.1.1.3 Block-Cipher

Block-cipher adalah skema algoritma sandi yang akan membagi-bagi teks terang yang akan dikirimkan dengan ukuran tertentu (disebut blok) dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Pada umumnya, block-cipher memproses teks terang dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit penggunaan pola-pola serangan yang ada untuk membongkar kunci. Untuk menambah kehandalan model algoritma sandi ini, dikembangkan pula beberapa tipe proses enkripsi, yaitu :

- ECB, Electronic Code Book
- CBC, Cipher Block Chaining
- OFB, Output Feed Back
- CFB, Cipher Feed Back

1.1.1.4 Stream-Cipher

Stream-cipher adalah algoritma sandi yang mengenkripsi data persatuan data, seperti bit, byte, nible atau per lima bit(saat data yang di enkripsi berupa data Boudout). Setiap mengenkripsi satu satuan data di gunakan kunci yang merupakan hasil pembangkitan dari kunci sebelum.

1.1.2 Algoritma Sandi Kunci-Asimetris

Skema ini adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Skema ini disebut juga sebagai sistem kriptografi kunci publik karena kunci untuk enkripsi dibuat untuk diketahui oleh umum (public-key) atau dapat diketahui siapa saja, tapi untuk proses dekripsinya hanya dapat dilakukan oleh yang berwenang yang memiliki kunci rahasia untuk mendekripsinya, disebut private-key. Dapat dianalogikan seperti kotak pos yang hanya dapat dibuka oleh tukang pos yang memiliki kunci tapi setiap orang dapat memasukkan surat ke dalam kotak tersebut. Keuntungan algoritma model ini, untuk berkorespondensi secara rahasia dengan banyak pihak tidak diperlukan kunci rahasia sebanyak jumlah pihak tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para korensponden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan skema kunci-simetris, jumlah kunci yang dibuat adalah sebanyak jumlah pihak yang diajak berkorespondensi.

2. Kriptografi dan Matematika

Apakah ada cara yang lebih efektif untuk mengajar matematika kepada murid sekolah menengah? Ketika kita masih berada di bangku SMA, guru bisa berdiri di depan ruang kelas, berjalan mengitari kita sambil menjelaskan contoh persoalan, lalu memberi pekerjaan rumah. Metode seperti itu bukanlah metode yang tidak efektif, namun jika kita bisa berandai-andai, apakah ada cara yang lebih menarik dan menyenangkan untuk murid mempelajari matematika.

Selama tiga tahun SMA, sedikit sekali kesempatan yang kita punyai untuk mengaplikasikan pelajaran matematika yang kita dapatkan pada kehidupan yang sebenarnya. Akan sangat baik jika ada sebuah bagian dari pelajaran yang memungkinkan murid untuk mengaplikasikan pelajaran matematika yang telah mereka dapatkan. Dan akan lebih baik bagi jika para guru dapat mengajar dalam cara yang menyenangkan para murid dan membuat mereka melihat kebutuhan akan pelajaran yang mereka dapatkan dalam hidup ini. Murid akan lebih ingin menguasai pelajaran jika mereka mengetahui cara untuk mengaplikasikan pengetahun mereka dalam kehidupan sehari-hari. Untuk itu, salah satu cara yang dapat dilakukan adalah dengan memperkenalkan murid kepada kriptografi.

2.1 Alasan Utama

Mengapa kriptografi? Karena kriptografi adalah salah satu cara paling efektif untuk melakukan pendekatan terhadap aplikasi matematika dalam kehidupan sehari-hari. Mungkin ada yang mempertanyakan hubungan kriptografi dengan matematika. Sebagian besar kode mempunyai kaitan yang erat dengan matematika. Contohnya, nomor kartu kredit, sebenarnya dikodekan untuk menjaga pembelanjaan barang dengan nomor yang salah. Keseluruhan proses pengkodean berbasis matematika. Coba kita lihat contoh berikut ini:

8721 6608 7187 0319.

Untuk mengetahui apakah nomor di atas adalah nomor kartu kredit yang valid, yang pertama harus kita lakukan adalah mengkali duakan semua angka posisi ganjil. 8 menjadi 16, 2 menjadi 4, 6 menjadi 12, dan seterusnya. Nomor kartu kredit kita akan menjadi seperti ini:

16 7 4 1 12 6 0 8 14 1 16 7 0 3 2 9.

Untuk setiap angka yang lebih dari 9, kita harus menguranginya dengan angka 9. Sekarang kita akan mendapatkan nomor kartu seperti berikut,

7741 3608 5177 0329.

Jika jumlah dari semua angka pada nomor kartu kredit yang kita dapatkan dapat dibagi dengan angka 10, maka nomor kartu kredit tersebut adalah valid. Dalam kasus ini, jumlah semua angka adalah 70, maka nomor kartu kredit tersebut adalah valid. Selanjutnya, apakah nomor tersebut berhubungan dengan akun tertentu, itu adalah persoalan yang berbeda. Ini adalah salah satu contoh dimana matematika dapat dipergunakan dalam pengkodean.

Kembali pada topik utama. Para murid seringkali melihat matematika sebagai sesuatu yang membosankan, dan hanya bisa dinikmati oleh mereka – mereka yang sudah terlebih dahulu diklasifikasikan sebagai "orang – orang matematika" Di SMA, matematika menjadi semakin rumit, dan para murid seringkali melihatnya sebagai sebuah kumpulan rumus yang mungkin bisa digunakan dalam berbagai macam situasi masalah. Situasi – situasi seperti ini secara teoritis dapat diaplikasikan dalam sains, namun para murid biasanya jarang mengetahui aplikasi – aplikasi tersebut. Karena pada kenyataannya, kurikulum tidak memfokuskan aplikasi penyelesaian masalah pada situasi yang lebih rumit. Para murid baisanya mempelajari dan memodelkan kemampuan ini setelah diajarkan contoh-contoh sebelumnya. Banyak sikap negatif yang berkembang dari para murid terhadap matematika karena mereka tidak mengetahui keterhubungan matematika itu sendiri dengan cabang ilmu lainnya. Diharapkan pengenalan kriptografi ini akan meningkatkan ketertarikan para murid terhadap matematika karena melibatkan kode – kode rahasia dan spionase. Hampir semua murid mempunyai pengalaman dnegan permainan dan puzzle yang melibatkan petunjuk – petunjuk untuk menyelesaikan suatu masalah. Banyak yang bahkan sudah mencoba untuk mengembangkan kode mereka sendiri untuk berkomunikasi dengan teman – teman mereka sendiri tanpa ada yang dapat mengetahui pesan mereka.

Dalam pelajaran ini, para murid berperan dalam penemuan informasi, sementara guru bertindak sebagai fasilitator. Namun begitu, para guru tidak diharapkan harus menjadi pakar kriptografi. Para guru hanya membutuhkan pemahaman khusus tentang materi, dan bisa ikut bersama-sama belajar dalam proses.

Dalam pelajaran ini, para murid akan memiliki kesempatan untuk merundingkan matematika dan menemukan peraturan kriptografi mereka sendiri. Cara ini akan mendorong mereka untuk berpikir kreatif. Kriptografi bergantung pada kombinasi, topik yang muncul sebagai bagian dari kurikulum. Murid juga akan menggambarkan dan mengobservasi data dalam menghasilkan suatu kesimpulan. Pada kenyataannya, matematika seringkali memunculkan suatu masalah yang membutuhkan waktu berhari – hari, bahkan bertahun – tahun untuk dipecahkan. Bekerja secara kolaboratif sebagai satu tim untuk kemudian menghasilkan cara penyelesaian masalah bukan hanya cara pembelajaran yang berharga, tapi menjadi lebih realistis dalam hubungannya dengan cara memecahkan masalah matematika di kehidupan sehari – hari.

Pelajaran kriptografi ini juga akan menyediakan kesempatan unik bagi para murid untuk melihat bagaimana matematika dan sains bisa bersama mengubah sejarah. Dalam sejarah, selama ini sains dan matematika dikenal berperan dalam sistem pembuatan senjata. Namun ternyata sains dan matematika juga berperan unik dalam usaha intelegensi di masa perang. Para murid dapat mempelajari pengaruh kode dan pemecahan kode selama masa perang dunia ke II. Matematika dan sains seringkali dilihat sebagai subjek yang saling berhubungan, tapi jarangkali para murid mempelajari keuntungan sejarah yang signifikan dalam matematika. Ketika mempelajari perang dunia ke II, murid bisa mengetahui peran kriptografi dalam pengiriman dan penguraian pesan rahasia. Mereka juga bisa mempelajari perkembangan teknologi ini (telegraf menjadi telepon) dan proses penemuan mesin Enigma – mesin sandi untuk mengenkripsi dan mendekripsi pesan.

Kembali lagi, kriptografi digunakan karena banyak aspek berbeda dalam matematika yang

digunakan untuk mengkode pesan. Masalah yang mungkin timbul adalah menemukan bagian dari kriptografi yang tepat dan cocok dengan pelajaran matematika SMA. Didapatkan bahwa beberapa bagian pelajaran yang cocok dengan konsep kriptografi diantaranya kekongruenan dan aritmetika modular, pesamaan linear, persamaan exponen dan exponensial, permutasi dan matriks.

Alasan utama mengajar dengan cara seperti ini adalah untuk mendorong perkembangan kemampuan penyelesaian masalah para murid. Salah satu hal yanag paling penting dari pembelajaran matematika adalah kemampuan untuk menyelesaikan suatu masalah. Diharapkan dengan pengenalan terhadap topik seperti kode, ketertarikan para murid akan subjek akan meningkat, dan para murid kemudian berkeinginan untuk menyelesaikan masalah dengan mengkode dan mengdekode. Lebih lanjut, diharapkan kemampuan penyelesaian masalah para murid akan semakin tajam. Tujuan yang lain adalah untuk memajukan pemikiran kritis para murid. Murid tidak diharapkan untuk dapat menguasai matematika, namun lebih kepada proses belajar para murid dalam menyelesaikan masalah.

2.2 Contoh Penerapan Kriptografi sebagai Media Pembelajaran Matematika

Mengajar kriptografi dapat dilakukan dengan berbagai macam pendekatan. Salah satu keuntungannya adalah unit seperti ini menawarkan para guru fleksibilitas. Unit ini dapat diajarkan di level pelajaran matematika yang lebih tinggi, namun juga bisa diajarkan pada tingkat yang lebih rendah sebagai pengenalan.

Untuk level awal, khususnya anak – anak sekolah dasar, atau juga untuk anak – anak pramuka penggalang, teknik kriptografi yang bisa diperkenalkan adalah sistem sandi Caesar atau sistem sandi Vigenère**.** Kedua macam sandi ini akan dibahas lebih lanjut pada bab berikutnya.

Untuk level yang lebih tinggi, pengajar tidak hanya bisa memberikan materi mengenai dasar kriptografi, namun juga materi yang lebih jauh daripada itu. Di bawah ini, contoh materi yang bisa diberikan kepada murid Sekolah Menengah Atas.

Materi pertama, adalah materi pengenalan. Pengajar bisa memperkenalkan kepada para murid konsep dasar dari kode. Materi dapat dimulai dengan mempelajari sandi Caesar dan sandi Vigenère.

Pada materi kedua, guru mengenalkan dan mengajarkan lebih banyak lagi kode – kode berbeda. Dengan materi ini para murid diharapkan mengetahui bermacam – macam kode yang ada, dan peran kode – kode tersebut dalam kehidupan sehari – hari, misalnya pengkodean pada nomor kartu kredit yang telah dijelaskan sebelumnya, ataupun peran kode dalam perang dunia ke II.

Untuk materi ketiga, kita menggunakan matriks untuk melakukan pengkodean. Pengajar bisa menggunakan matriks 2x2 agar murid merasa bahwa materi yang diberikan tidaklah terlalu berat. Penggunaan matriks merupakan metode yang berbeda dalam pembuatan kode, sebagai suatu variasi pengajaran.

Materi ketiga berhubungan dengan Enigma, yaitu mesin sandi untuk mengenkripsi dan mendkripsi kode atau sandi.

Materi kelima adalah materi utama dari keseluruhan materi, berhubungan dengan Enigma. Para murid diajak memperhatikan persamaan linear dan bagaimana persamaan linear bisa dipakai dalam mengkode. Dengan bentuk mx + b, murid bisa menetapkan nilai untuk m dan b dan membuat suatu sistematis pemberian nilai. Dengan menetapkan nilai – nilai yang berbeda untuk m dan b menggunakan lebih dari satu persamaan, aspek rotor (Enigma) bisa dimasukkan dalam materi ini. Keuntungan lain dari memulai materi dengan persamaan linear adalah pengajar bisa kemudian mengajarkan berbagai macam persamaan – persamaan lainnya, misalnya persamaan eksponensial.

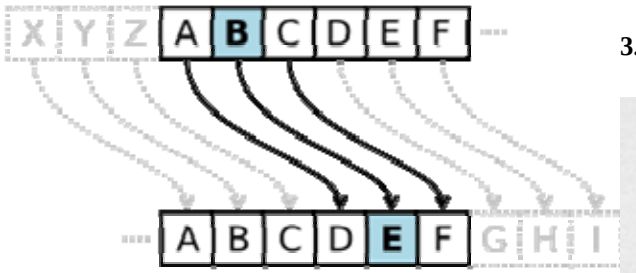
Terakhir, pengajar bisa mengajarkan RSA coding, yaitu algoritma sandi kunci asimetris yang berhubungan dengan bilangan prima, aritmetika modular dan eksponensial. Para pengajar sebaiknya menetapkan angka – angka yang tepat untuk level muridnya, namun juga menunjukkan bagaimana RSA coding ini dengan mudahnya menjadi materi yang sulit.

3. Sandi Caesar dan Sandi Vigenère

Sandi Caesar dan sandi Vigenère adalah dua macam sandi substistusi yang sederhana dan mudah untuk dipelajari. Oleh karena itu kedua sandi tersebut sangat baik untuk digunakan sebagai contoh kriptografi pada materi awal perkenalan dengan kriptografi.

3.1 Sandi Caesar

Dalam kriptografi, sandi Caesar, atau biasa disebut juga sebagai sandi Shift, kode Caesar, atau Caesar's shift, adalah salah satu teknik enkripsi yang paling sederhana dan paling dikenal luas. Ini adalah salah satu tipe dari sandi substitusi dimana masing-masing huruf dari plaintext digantikan dengan huruf-huruf dari alfabet yang sebelmnya telah digeser urutannya terhadap suatu angka. Contoh, dengan pergeseran 3, maka huruf A pada plaintext, akan huruf D pada chipertext, B menjadi E, dan seterusnya. Metode ini dinamakan atas Julius Caesar, yang pertama kali berkomunikasi menggunakan cara ini.



Langkah – langkah enkripsi Caesar seringkali dimasukkan sebagai bagian dalam enkripsi yang lebih rumit, seperti sandi Vigenère. Dengan penggunaan substitusi satu alfabet dalam enkripse sandi, maka sandi Caesar dapat dengan mudah dipecahkan, dan dalam praktiknya, sandi Caesar kurang menjamin kerahasiaan dan keamanan komunikasi.

Sandi Caesar menggunakan pergeseran tiga huruf.

→ Plain:
ABCDEFGHIJKLMNOPQRSTUVWXYZ
→ Cipher:
DEFGHIJKLMNOPQRSTUVWXYZABC

Untuk membuat chipertext, yang harus dilakukan hanyalah melihat huruf yang bersesuaian antara huruf pada alphabet plaintext, dan huruf pada alphabet chipertext. Untuk mengetahui plaintext, lakukan hal yang sebaliknya.

→ Plaintext:
THE QUICK BROWN FOX JUMPS OVER THE LAZY DOG
→ Ciphertext:
WKH TXLFN EURZQ IRA MXPSV RYHU WKH ODCB GRJ

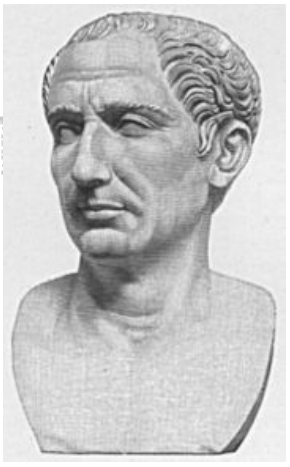
Enkripsi juga dapat direpresentasikan menggunakan aritmetika modulo dengan pertama – tama mentransformasikan huruf menjadi angka. A=0, B=1, …., Z=25. Enkripsi terhadap huruf x dengan pergeseran n dapat dideskripsikan secara matematika sebagai,

$$E_n(x) = (x + n) \mod 26.$$

representasi dekripsi tidak jauh berbeda, yaitu,

$$D_n(x) = (x - n) \mod 26.$$

3.1.1 Sejarah dan Kegunaan



Sandi Caesar berasal dari nama Julius Caesar, yang menggunakan sandi tersebut dengan nilai pergeseran 3 pada alfabet, untuk melindungi pesan militer.

Di abad 19, bagian periklanan pribadi pada surat kabar kadang – kadang digunakan untuk menukarkan pesan rahasia yang dienkripsi dengan chiper substitusi sederhana. Kahn (1967), memberikan contoh pasangan kekasih yang bertunangan dalam komunikasi rahasia dengan

menggunakan sandi Caesar pada surat kabar The Times. Bahkan pada tahun 1915, tentara Rusia menggunakan sandi Caesar sebagai pengganti sandi yang lebih rumit, karena para tentara merasa bahwa agak sulit untuk mendekripsikan sandi yang lebih rumit dari sandi Caesar.

Sandi Vigenère mengimplementasikan sandi Caesar dengan pergesaran yang berbeda pada tiap posisi huruf, dimana pergeserannya didefinisikan dengan menggunakan kata kunci yang berulang. Sandi Vigenere akan dibahas lebih lanjut di pembahasan berikutnya.

3.1.2 Memecahkan Sandi Caesar

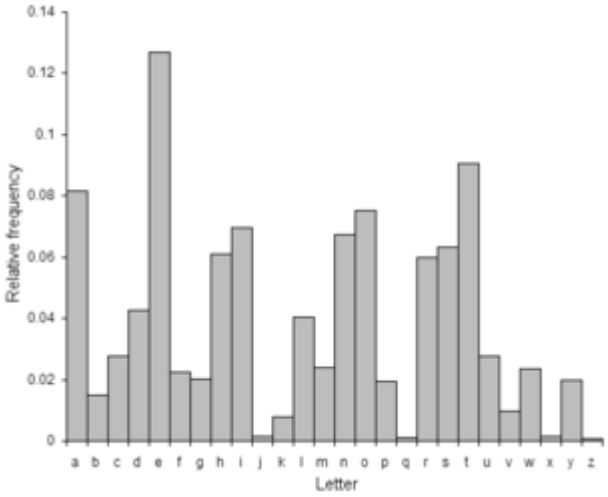
Sandi Caesar dapat dengan mudah dipecahkan. Dua situasi yang mungkin terjadi : 1) pemecah mengetahui (atau menebak) chiper substitusi yang digunakan, namun mungkin bukan chiper substitusi yang benar – benar dipakai; dan 2) pemecah mengetahui bahwa sandi Caesar sedang digunakan, tapi tidak mengetahui nilai pergeserannya.

Dalam kasus pertama, sandi dapat dipecahkan dengan menggunakan teknik yang sama dengan chiper substitusi sederhana pada umumnya, yaitu analisis frekuensi atau pola kata. Selama memecahkan, pemecah akan menyadari keteraturan solusi dan menarik kesimpulan bahwa algoritma yang dipakai dalam kode adalah sandi Caesar.

Dalam contoh yang kedua, memecahkan kode terlihat lebih jelas. Karena sudah diketahui bahwa kode tersebut merupakan hasil enkripsi sandi Caesar, dan hanya terdapat kemungkinan pergeseran yang terbatas (26), maka kode yang akan dipecahkan bisa diujikan dengan cara acak, yang bisaa disebut *brute force attack*. Caranya adalah dengan menuliskan potongan kode dari chipertext pada tabel kemungkinan untuk semua kemungkinan pergeseran – teknik yang kita kenal dengan "melengkapi komponen". Contohnya adalah sebagai berikut, chipertext "`EXXEGOEXSRGI`"; maka dapat dilihat bahwa kemungkinan plaintext adalah "`ATTACKATONCE`", dimana pergeseran huruf adalah 4 (lihat tabel di samping).

Decryption shift	Candidate plaintext
0	`exxegoexsrgi`
1	`dwwdfndwrqfh`
2	`cvvcemcvqpeg`
3	`buubdlbupodf`
4	`attackatonce`
5	`zsszbjzsnmbd`
6	`yrryaiyrmlac`
...	
23	`haahjrhavujl`
24	`gzzgiqgzutik`
25	`fyyfhpfytshj`

Cara acak lainnya adalah dengan memasangkan frekuensi distribusi dari huruf. Distribusi huruf dalam contoh teks dalam bahasa inggris mempunyai bentuk yang khusus dan dapat diprediksi. Pergeseran Caesar menggilirkan distribusi ini, dan sangat mungkin untuk menentukan pergeseran dengan memeriksa hasil dari grafik frekuensi. Dengan menggambarkan grafik frekuensi kemunculan huruf di chipertext, dan dengan mengetahui distribusi yang diinginkan (harapan) terhadap huruf – huruf di bahasa asli dari plaintext, seseorang bisa dengan mudah mengetahui pergeseran huruf dengan melihat grafiknya. Cara ini disebut analisis frekuensi. Contoh, dalam bahasa inggris, frekuensi plaintext dari hurf E,T,(bisaanya paling sering muncul), and Q,Z,(bisaanya paling jarang muncul) terbilang sangat khas. Komputer juga bisa melakukan pengukuran seberapa tepat distribusi frekuensi asli cocok dengan distribusi harapam, misalnya dengan distribusi chi-square (statistika).



Untuk plaintext dalam bahasa yang umum, biasanya hanya akan ada satu kemungkinan dekripsi yang masuk akal, walaupun untuk plaintext yang sangat pendek akan terdapat kandidat yang lebih banyak. Contohnya, untuk chipertext MPQY (dalam bhasa inggris), kemungkinan yang ada adalah "aden" atau "know"; begitu juga dengan "ALIIP" bisa merupakan "dolls" atau "wheel", dan "AFCCP" untuk "jolly" atau "cheer".

3.2 Sandi Vigenère

Sandi Vigenère berasal dari nama penemunya, Blaise de Vigenère (gambar di atas), seorang kriptografer asal Perancis. Walaupun Giovan Batista Belaso telah lebih dahulu menemukan sandi sebelumnya, namun Vigenere berhasil menemukan kunci sandi yang lebih kuat.

Sandi Vigenère adalah salah satu metode enkripsi yang menggunakan sejumlah sandi Caesar ebrbeda berdasarkan huruf – huruf dari sebuah kata kunci. Sandi ini merupakan bentuk sederhana dari substitusi polialfabet.

Sandi ini dikenal luas selain karena mudah dimengerti dan diimplementasi, untuk para pemula sandi ini sering dirasakan tidak dapat dipecahkan (unbreakable), dimana sandi ini sering disebut **le chiffre indéchiffrable** (bahasa perancis untuk "tidak dapat dipecahkan"). Akibatnya, banyak orang yang mencoba untuk mengimplementasikan skema enkripsi yang intinya adalah sandi Vigenère, hanya untuk memecahkannya.

Sandi Polialfabet pertama, diciptakan oleh Leone Battista Alberti, sekitar tahun 1467, menggunakan alat semacam cakram logam untuk menukarkan antar huruf alfabet. Sistem Alberti hanya menukarkan alfabet setelah sejumlah kata, dan penukarannya ditunjukkan dengan menuliskan huruf yang bersesuaian dengan alfabet pada chipertext. Kemudian di tahun 1508, Johannes Trithemius, menemukan tabula recta, komponen penting dari sandi Vigenère. Namun begitu, Trithemius hanya memberikan sistem yang kaku dan dapat diprediksi untuk penukaran antar alfabet sandi.

Sandi yang sekarang ini dikenal sebagai sandi Vigenère pada mulanya digambarkan oleh Giovan Batista Belaso dalam bukunya *La cifra del. Sig. Giovan Batista Belaso* pada tahun 1553. Ia membangun sandi atas tabula recta Trithemius, tetapi menambahkan sebuah kunci perulangan untuk menukar setiap huruf alfabet chiper.

Sandi Vigenère mendapatkan reputasi karena kekuatannya. Matematikawan dan penulis Charles Lutwidge Dodgson (Lewis Carroll), dalam bukunya "The Alphabet Chiper" di tahun 1868 menyebut sandi Vigenère tidak dapat dipecahkan. Di tahun 1917, *Scientific American* mendeskripsikan sandi Vigenère sebagai "translasi yang mustahil". Penghargaan ini kemudian menjadi tidak tepat lagi, sejak Kasiski berhasil memecahkan sandi tersebut pada abad 19.

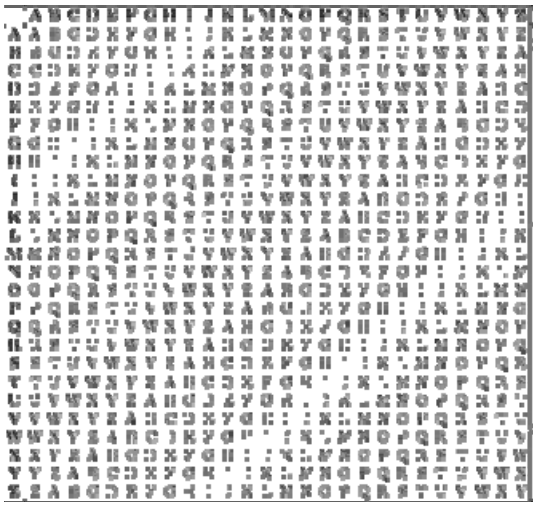
Sandi Vigenère sebetulnya cukup sederhana untuk dipecahkan jika menggunakan cakram sandi. The Confederate States of America misalnya, menggunakan cakram sandi berbahan kuningan untuk mengimplementasikan sandi Vigenère selama perang saudara Amerika. Tiga

kata kunci yang bisaa digunakan oleh The Confederate adalah “Manchester Bluff”, Complete Victory" , dan "Come Retribution”.

Tiruan dari cakram sandi Confederacy, hanya terdapat lima buah yang asli di dunia.

Gilbert Vernam mencoba untuk memperbaiki sandi yang terpecahkan (kemudian menciptakan sandi Vernam-Vigenère), tetapi, apapun yang dia lakukan, sandi Vigenère telah menjadi sangat mudah untuk dikriptanalisis.

3.2.1 Deskripsi



Kotak Vigenère atau tabel Vigenère, juga dikenal dengan tabula recta, dapat digunakan untuk melakukan enkripsi ataupun dekripsi.

Dalam sandi Caesar, tiap – tiap huruf alfabet digeser mengikuti sebuah angka pergeseran. Sandi Vigenère mengandung sejumlah sandi Caesar yang dirangkai dengan angka – angka pergeseran yang berbeda – beda.

Untuk melakukan enkripsi, kita menggunakan tabel Vigenère. Tabel tersebut memuat alfabet yang ditulis 26 kali dalam baris yang berbeda, dengan tiap – tiap alfabet digeser memutar ke kiri terhadap alfabet sebelumnya, bersesuaian dengan 26 kemungkinan sandi Caesar. Pada tiap huruf berbeda dalam proses enkripsi, pengkode menggunakan alfabet berbeda dari salah satu baris. Alfabet yang digunakan pada setiap huruf bergantung kepada kata kunci yang berulang.

Contohnya, misalkan plaintext yang akan dienkripsi berupa

ATTACKATDAWN

Dan orang yang mengirimkan pesan memilih katakunci dan mengulanginya sampai panjang kata kunci cukup dengan panjang plaintext, contoh, kata kunci “LEMON”

LEMONLEMONLE

Huruf pertama dari plaintext adalah A, dienskripsi dengan menggunakan alfabet pada baris L, yang merupakan huruf pertama pada kata kunci. Ini dilakukan dengan melihat huruf yang terdapat pada baris L dan kolom A pada tabel Vigenère, yaitu huruf L.Untuk huruf kedua pada plaintext, kita menggunakan huruf kedua pada kata kunci, yaitu pada baris E dan kolom T, yaitu huruf X. Lakukan terus hingga huruf terakhir plaintext.

Plaintext: ATTACKATDAWN
Kata kunci: LEMONLEMONLE
Ciphertext: LXFOPVEFRNHR

Dekripsi dilakukan dengan cara sebaliknya. Misalkan untuk huruf pertama chipertext, L, kita cari huruf pertama kata kunci pada baris L, dimana hurf pertama kata kunci juga merupakan huruf L. Kemudian kita dapat menemukan pada baris L, huruf L terdapat pada kolom A, yang mengartikan bahwa huruf A merupakan huruf pertama pada plaintext. Begitu seterusnya.

Sandi Vigenère juga dapat direpresentasikan secara aljabar. Jika huruf A-Z dianggap sebagai

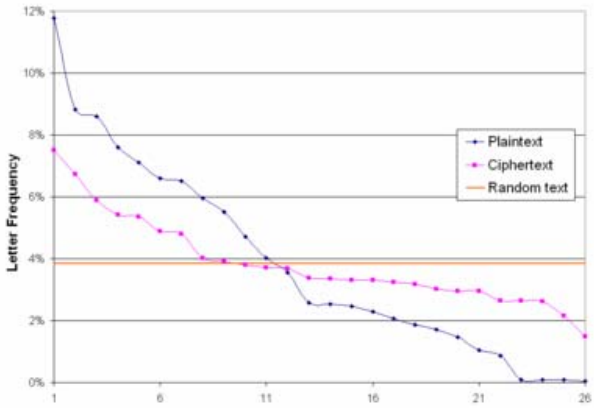
angka 0-25, dengan menggunakan modulo 26, kita bisa menuliskan enkripsi sandi Vigenère sebagai,

$$C_i \equiv (P_i + K_i) \mod 26$$

dan dekripsinya,

$$P_i \equiv (C_i - K_i) \mod 26$$

3.2.2 Kriptanalis



Sandi Vigenère dinilai efektif karena bisa menyembunyikan frekuensi karakteristik huruf dari plaintext (khususnya dalam bahsa inggris), walau beberapa pola seringkali berulang.

Kekuatan dari sandi Vigenère, seperti sandi polialfabet pada umumnya, yaitu kemampuannya melawan analisis frekuensi. Sebaliknya, kelemahan dari sandi Vigenère adalah sifat alami dari kata kuncinya, yaitu pendek dan berulang. Jika seorang kriptanalis mengetahui panjang dari kata kunci, maka chipertext dapat diperlakukan sebagai kumpulam sandi Caesar yang berbed, yang mana mudah untuk dipecahkan. Kasiski tes membantu kita dalam menentukan panjang kata kunci chipertext.

3.2.3 Kasiski Examination

Friedrich Kasiski berhasil menerbitkan pemecahan sandi Vigenère pada tahun 1863. Pengujian Kasiski, bisaadisebut tes Kasiski, mengambil keuntungan dari kenyataan bahwa sejumlah kata umum (dalam bahsa inggris), seperti “the”, dengan perubahan, akan dienkripsi menggunakan huruf kunci yang sama, menurut kumpulan pengulangan huruf pada chipertext. Contoh, pesan yang dienkripsi dengan kata kunci ABCDEF mungkin tidak akan mengenkripsi “crypto” dengan cara yang sama setiap kali kemunculannya pada plaintext.

```
Kata kunci: ABCDEF AB CDEFA BCD EFABCDEFABCD
Plaintext:  CRYPTO IS SHORT FOR CRYPTOGRAPHY
Ciphertext: CSASXT IT UKSWT GQU GWYQVRKWAQJB
```

Chipertext di contoh ini tidak akan mengulang urutan yang bersesuaian dengan urutan pengulangan pada plaintext. Namun begitu, jika panjang kata kunci berbeda, seperti contoh di bawah ini:

```
Kata kunci: ABCDAB CD ABCDA BCD ABCDABCDABCD
Plaintext:  CRYPTO IS SHORT FOR CRYPTOGRAPHY
Ciphertext: CSASTP KV SIQUT GQU CSASTPIUAQJB
```

Maka tes Kasiski akan efektif. Semakin panjang pesan, membuat tes Kasiski semakin akurat, karena bisaanya mengandung lebih banyak bagian chipertext yang berulang. Chipertext di bawah ini mempunyai beberapa bagian pengulangan dan mengizinkan kriptanalis untuk mengetahui panjang kata kunci.

```
Ciphertext:
DYDUXRMHTVDVNQDQNWDYDUXRMHARTJGW
NQD
```

Jarak antara pengulangan DYDUXRMH adalah 18 karakter. Hal ini mengasumsikan bahwa bagian pengulangan menunjukkan bagian plaintext yang sama, yang secara tidak langsung mengatakan bahwa panjang kata kunci adalah 18, 9, 6, 3, atau 2. Jarak antar NQD adalah 20 karakter. Ini berarti bahwa panjang kata kunci adalah 20, 10, 5, 4, atau 2. Dengan mengambil persamaan dari keduanya, kita dapat menyimpulkan bahwa panjang kata kuncinya (hampir pasti) adalah 2.

Jika panjang kata kunci telah diketahui, chipertext dibagi menjadi bagian - bagian dimana tiap bagian bersesuaian dengan sebuah huruf pada kata kunci. Tiap potongan dari

chipertext yang telah dibagi adalah setara dengan chipertext dari sandi Caesar. Dengan menggunakan metode untuk memecahkan sandi Caesar, huruf – huruf pada kata kunci dapat diketahui. Jika kata kunci telah diketahui, kriptanalis dapat dengan mudah mendekripsikan chipertext dan mengungkapkan plaintext.

4. Kesimpulan

Kriptografi adalah ilmu dan seni dalam menjaga kerahasiaan berita. Berdasarkan kesaman kuncinya, algoritma sandi dalam kriptografi dibagi dua, yaitu algoritma sandi kunci simetris, dan algoritma sandi kunci asimetris. Yang termasuk algoritma sandi kunci simetris adalah chiper substitusi, chiper transposisi, block-chiper, stream-chiper.

Kriptografi dapat digunakan sebagai media pembelajaran matematika tingkat sekolah. Sebagai metode baru, selain memberikan suatu variasi baru pengajaran, kriptografi juga dapat memberikan dampak positif lain, yaitu mengajarkan murid untuk dapat lebih berpikir kritis dalam menyelesaikan suatu masalah.

Pada level pemula, murid dapat diperkenalkan dengan dua macam kriptografi sederhana, yaitu chiper substitusi sandi Caesar dan sandi Vigenère. Pada level yang lebih tinggi, khususnya tingkat SMA, kriptografi dapat diimplementasikan dalam materi aritmetika modular, pesamaan linear, persamaan exponen dan exponensial, permutasi dan matriks.

DAFTAR PUSTAKA

[1] Amick, Michael. (2006). An Interdisciplinary Unit on Cryptography. *http://www.chatham.edu/pti/2004%20units/The%20Great%20Problems%20of%20Mathematics/Amick%20unit.pdf/interdisciplinary.* Tanggal akses: 28 Desember 2006 pukul 16:07.

[2] Koblitz, Neal. (2006). Cryptography As a Teaching Tool. *http://www.math.washington.edu/~koblitz/crlogia.html/*. Tanggal akses: 27 Desember 2006 pukul 15:05.

[3] Pell, Oliver. (2006). Cryptology. *http://www.ridex.co.uk/cryptology/.* Tanggal akses: 27 Desember 2006 pukul 15:18.

[4] *http://en.wikipedia.org/wiki/Caesar_cipher/*. Tanggal akses: 27 Desember 2006 pukul 15:23.

[5] *http://id.wikipedia.org/wiki/Kriptografi/*. Tanggal akses: 24 Desember 2006 pukul 10:50.

[6] *http://en.wikipedia.org/wiki/ Vigenère _cipher/*. Tanggal akses: 27 Desember 2006 pukul 15:24.

[7] *http://www.gvsu.edu/math/enigma/School/380term.html* Tanggal akses: 28 Desember 2006 pukul 15:24.