KRIPTOGRAFI DAN KRIPTANALISIS KLASIK

Raka Mahesa (13508074)

Teknik Informatika, Institut Teknologi Bandung
Jln. Ganesha No. 10, Bandung
if18074@students.if.itb.ac.id

ABSTRAK

Kriptologi terus berkembang dari zaman ke zaman, mulai dari kriptologi klasik dimana kriptografi hanyalah mengganti-ganti huruf secara sederhana, kriptologi dengan bantuan mesin pada zaman perang dunia, sampai zaman modern ini, dimana kriptologi merupakan ilmu komputer yang menyandikan ratusan karakter dengan triliunan kemungkinan. Namun, kriptologi tetaplah merupakan suatu peperangan informasi, terlepas dari zamannya, sehingga kriptologi klasik merupakan suatu hal yang penting untuk dikaji. Penulis membagi makalah ini ke dalam dua bagian, bagian pertama membahas kedua jenis kriptografi klasik, dengan fokus terletak pada *cipher* Vigenere, salah satu *cipher* substitusi polialfabetik, dan berbagai *cipher* transposisi. Sementara bagian kedua membahas tentang berbagai kriptanalisis klasik dan metode-metodenya, dengan fokus terletak pada metode analisa frekuensi dan pemeriksaan Kasiski. Selain itu penulis juga menyertakan kriptanalisis terhadap *Caesar Cipher* dan *cipher* Vigenere.

Kata kunci: Kriptografi, kriptanalisis, klasik, *cipher*, Vigenere, substitusi, transposisi, analisa frekuensi.

1. PENDAHULUAN

Semenjak dahulu kala, kerahasiaan dalam penyampaian informasi selalu menjadi masalah yang pelik. Terkadang sebuah informasi tidak dapat disampaikan begitu saja karena mengandung suatu hal yang bersifat rahasia dan berbahaya bila jatuh ke tangan yang salah, karena itu diperlukan sebuah sistem untuk menjaga kerahasiaan tersebut. Dari latar belakang inilah muncul ilmu kriptologi, sebuah ilmu tentang kriptopgrafi – cara untuk menjaga kerahasiaan sebuah informasi melalui penyandian – dan kriptanalisis – cara untuk memecahkan suatu sandi untuk mendapatkan informasi yang terdapat di dalamnya.

Kriptografi klasik terpusat pada bagaimana cara untuk mengubah sebuah *plaintext* – teks jelas – menjadi sebuah *ciphertext* – teks tersandi – dan kembali lagi menjadi sebuah *plaintext*. Proses penyandian ini biasa disebut dengan enkripsi, sementara proses mengembalikan *ciphertext* ke *plaintext* biasa disebut dengan dekripsi. Seluruh sistem ini disebut dengan sistem *cipher*, dimana terdapat sebuah algoritma enkripsi E_K yang mengubah teks P menjadi teks C dan sebuah algoritma dekripsi D_K yang mengubah teks C menjadi teks P. Selain itu terdapat juga sebuah kunci K yang merupakan kunci untuk dapat menjalankan kedua algoritma tersebut.

Sebagaimana semua ilmu, kriptografi berkembang menjadi sesuatu yang jauh lebih kompleks, apalagi setelah ditemukannya komputer yang memungkinkan manusia untuk memecahkan sebuah sandi dengan mencoba segala kemungkinan (*brute force attack*). Karena itu, di masa modern ini, berbagai algoritma enkripsi yang tahan dengan serangan tersebut dikembangkan, mulai dari yang cukup dapat bertahan seperti *Data Encryption Standard* (DES) dan *Advanced Encryption Standar* (AES) sampai dengan yang tahan sepenuhnya seperti algoritma RSA.

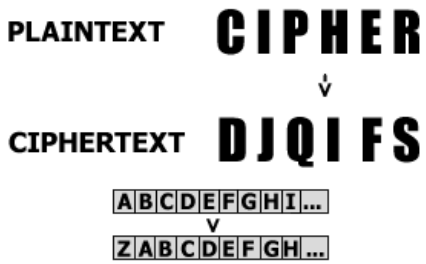
Meskipun skalanya sudah berbeda, dasar kriptografi tersebut tetaplah sama, yaitu sebuah fungsi yang memetakan suatu teks ke teks lain tanpa dapat diketahui teks asalnya (fungsi enkripsi). Pada kriptografi klasik, yang dienkripsi hanyalah sekedar beberapa kata ke dalam bentuk kata juga, sementara pada kriptografi modern, yang dienkripsi adalah ratusan bit yang merupakan satuan komputer. Meskipun begitu, dasar keduanya tetaplah sama.

2. KRIPTOGRAFI KLASIK

Kriptografi klasik adalah kriptografi yang paling sederhana, mengingat kriptografi ini sudah ada sejak ribuan tahun yang lalu, bahkan salah satu kriptografi paling tua yang ditemukan adalah kriptografi yang digunakan oleh Julius Caesar dan *scytale* – kriptografi dengan melilitkan pesan pada tabung – yang digunakan oleh bangsa Sparta. Kriptografi klasik terbagi atas dua jenis *cipher*, substitusi dan transposisi (atau disebut juga permutasi).

2.1 *Cipher* Substitusi

Sistem *cipher* substitusi adalah sebuah algoritma enkripsi dan dekripsi yang mensubstitusi unit-unit sebuah text dengan unit-unit lain berdasarkan aturan tertentu. Unit-unit ini bisa saja sebuah huruf, sepasang huruf, sebuah kata, dan sebagainya. Contoh sederhana *cipher* ini dapat dilihat pada gambar 1.



Gambar 1. *Cipher* Substitusi

Pada gambar 1 di atas, *plaintext* di enkripsi dengan mensubstitusi tiap huruf dengan huruf setelahnya pada alphabet latin. Ini adalah salah satu contoh *cipher* substitusi jenis monoalfabetik.

Cipher subtitusi ini memiliki beberapa jenis, di antaranya adalah sebagai berikut:

- Monoalfabetik
- Polialfabetik
- Homofonik
- Poligram

2.1.1 Substitusi Monoalfabetik

Sistem *cipher* substitusi monoalfabetik memetakan tiap huruf satu per satu seperti pada contoh gambar 1 di atas, dimana tiap huruf alfabet dipetakan ke huruf setelahnya. Untuk melakukan dekripsi dari *ciphertext*, sebuah substitusi kebalikannya dilakukan, misalnya bila enkripsinya adalah mengganti huruf *plaintext* dengan huruf alfabet setelahnya, maka algoritma dekripsinya adalah mengganti huruf pada *ciphertext* dengan huruf alfabet sebelumnya.

Kriptografi Julius Caesar termasuk ke dalam *cipher* jenis ini, dimana pada kriptografinya, tiap huruf dipetakan ke tiga huruf setelahnya, A menjadi D, B menjadi E, dan seterusnya. *Cipher* semacam ini sering disebut dengan *Caesar Cipher*, dimana enkripsi dilakukan dengan menggeser huruf pada alphabet sebanyak jumlah kunci yang diberikan. Contoh lain dari *cipher* jenis ini adalah *cipher* Atbash yang sering dipakai untuk alphabet *Hebrew*, dimana enkripsi dilakukan dengan mengganti huruf pertama dengan huruf terakhir, huruf kedua dengan huruf kedua terakhir, dan seterusnya.

2.1.2 Substitusi Polialfabetik

Cipher polialfabetik pertama kali dijelaskan oleh Leone Battista Alberti pada tahun 1467 sementara *tableau* – sebuah tabel alfabet yang dapat digunakan untuk membantu enkripsi dan dekripsi cipher polialfabetik – diperkenalkan oleh Johannes Trithemius dalam bukunya Steganographia. Pada *cipher* ini, beberapa alfabet *cipher* digunakan sekaligus yang kemudian ditulis di sebuah *tableau*.

Cipher dengan jenis polialfabetik yang paling terkenal adalah *cipher* Vigenère yang ditulis oleh Blaise de Vigenère pada abad ke-16. *Cipher* ini memanfaatkan tabel alfabet 26 X 26 – atau lebih dikenal dengan nama *Tabula Recta* – dan menggunakan kunci dan *plaintext* sebagai penanda posisi pada *Tabula Recta* untuk mendapatkan *ciphertext*-nya. Untuk melakukan dekripsi, kunci dan *ciphertext* digunakan sebagai penanda posisi untuk mendapatkan *plaintext*.

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Gambar 2. *Tabula Recta*

Untuk melakukan enkripsi dengan *cipher* Vigenère, sebuah kata kunci diperlukan. Kata kunci ini akan diulang sampai panjangnya sama dengan panjang *plaintext* dan kemudian digunakan untuk mencari huruf pengganti pada *tabula recta.*

Kata Kunci:	BEG
Plaintext:	**J I D A D**
Kunci:	B E G B E

Dengan kunci dan *plaintext* tersebut, enkripsi Vigenère dapat dilakukan dengan bantuan *tabula recta*. Untuk mendapat huruf pertama *ciphertext*, kita masukkan kunci sebagai baris dan *plaintext* sebagai kolom. Jadi, huruf

pertama *ciphertext* adalah K, huruf yang terdapat pada baris B dan kolom J.

	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

Gambar 3. Enkripsi Huruf Pertama dengan *Cipher* Vigenère

Ulangi untuk huruf *ciphertext* berikutnya, yaitu huruf pada baris E dan kolom I, didapatkan huruf M sebagai huruf *ciphertext* kedua. Langkah-langkah tersebut diulangi sampai *plaintext* sudah habis dienkripsi dan *ciphertext* yang didapat adalah KMJBH.

	A	B	C	D	E	F	G	H	I	J
A	A	B	C	D	E	F	G	H	I	J
B	B	C	D	E	F	G	H	I	J	K
C	C	D	E	F	G	H	I	J	K	L
D	D	E	F	G	H	I	J	K	L	M
E	E	F	G	H	I	J	K	L	M	N
F	F	G	H	I	J	K	L	M	N	O
G	G	H	I	J	K	L	M	N	O	P
H	H	I	J	K	L	M	N	O	P	Q
I	I	J	K	L	M	N	O	P	Q	R
J	J	K	L	M	N	O	P	Q	R	S

Gambar 4. Enkripsi Huruf Kedua dengan *Cipher* Vigenère

Keistimewaan *cipher* ini adalah kemudahanya dalam implementasi dan kekuatannya dalam menghadapi serangan. Meskipun dapat dipakai dengan sederhana, *cipher* ini tergolong amat kuat untuk masanya, bahkan disebut-sebut sebagai *cipher* yang tidak dapat dipecahkan sampai pada abad ke-20.

2.1.3 Substitusi Homofonik

Semenjak ditemukannya analisa frekuensi sebagai salah satu teknik untuk memecahkan kriptopgrafi, berbagai *cipher* yang tahan terhadap teknik tersebut dikembangkan, salah satunya adalah *cipher* homofonik. *Cipher* ini memetakan huruf pada *plaintext* yang sering keluar ke dalam lebih dari sebuah huruf *ciphertext* dengan tujuan mengacaukan hasil analisa frekuensi (yang cara kerjanya adalah dengan menganalisa huruf yang paling sering muncul). Beberapa contoh dari *cipher* jenis ini adalah *cipher* buku yang memanfaatkan literatur dan *cipher straddling checkerboard* yang merepresentasikan huruf dengan angka.

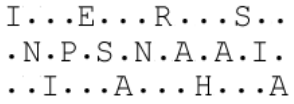
2.2 *Cipher* Transposisi

Sistem *cipher* transposisi adalah sebuah metode enkripsi dan dekripsi dengan cara mengubah susunan huruf pada *plaintext* berdasarkan aturan tertentu. Berikut ini adalah contoh sebuah enkripsi transposisi yang menuliskan *chipertext* berdasarkan urutan huruf 2, 4, 1, 5, 3 pada *plaintex*t.

Gambar 5. *Cipher* Tranposisi

2.2.1 *Rail Fence Cipher*

Cipher ini disebut juga sebagai *cipher* zig-zag, dan sesuai namanya, *cipher* ini mengubah *plaintext* menjadi *ciphertext* dengan menuliskan *plaintext* secara zig-zag dan membacanya secara horizontal. Gambar 6 adalah contoh enkripsi *plaintext* INI PESAN RAHASIA dengan *rail fence cipher* menjadi *ciphertext* IERSN PSNAA IIAHA.

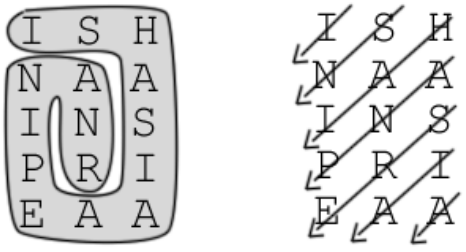


Gambar 6. *Rail Fence Cipher*

Yang menjadi kunci dalam cipher ini adalah jumlah "rel"-nya, yaitu berapa kali menulis huruf *plaintext* sebelum penulisan berubah arah, pada contoh di atas, jumlah relnya adalah 3.

2.2.2 *Route Cipher*

Route cipher adalah *cipher* transposisi lain yang cukup sederhana, *plaintext* dituliskan dalam bentuk matriks (kolom dan tabel) dan kemudian dituliskan kembali menurut rute tertentu menjadi *ciphertext*. Untuk mendekripsikannya, huruf-huruf *ciphertext* ditulis kembali menurut rute enkripsi.



Gambar 7. *Route Cipher*

Rute yang menjadi kunci bisa apapun, gambar 7 di atas memperlihatkan beberapa di antaranya. Gambar di kiri memperlihatkan rute "spiral searah jarum jam dari kiri atas" dengan *ciphertext* berupa ISHAS IAAEP INANR.

Sementara gambar sebelah kanan memperlihatkan rute "diagonal ke kiri bawah dari kiri atas" dengan *ciphertext*-nya adalah ISNHA IANPS REIAA.

2.2.3 Transposisi *Columnar*

Pada sistem *cipher* ini, *plaintext* ditulis dalam matriks secara horizontal seperti pada *route cipher*, namun kali ini penulisan ke dalam matriksnya bergantung kepada kunci yang merupakan sebuah kata. *Ciphertext* didapat dari membaca matriks *plaintext* per kolom dengan urutan alfabetis dari kunci.

```
2431
INIP
ESAN
RAHA
SIAQ
```

Gambar 8. Transposisi *Columnar*

Pada gambar 8, *plaintext*-nya adalah INI PESAN RAHASIA, sementara kata yang menjadi kunci adalah kata HMIF, dan Q di belakang adalah tambahan karena *plaintext*-nya tidak cukup untuk matriks 4x4. Dari kunci HMIF, didapatkan urutan kolom 2431 sesuai dengan urutan huruf pada kunci secara alfabet dan matriks berkolom 4 karena ada 4 huruf pada kunci. Enkripsi dilakukan pada *plaintext* sesuai dengan urutan kolom sehingga *cyphertext*-nya ialah PNAQ IERS IAHA NSAI. Untuk mengembalikan teks tersebut menjadi *plaintext*, cukup dengan menuliskan *cyphertext* secara vertical sesuai dengan kunci dan membacanya secara horizontal.

Untuk memperkuat transposisi ini, terdapat beberapa varian, misalnya dengan menggandakan transposisi. Jadi dengan dua buah kunci, dapat dilakukan dua transposisi pada suatu *plaintext* yang akan menghasilkan sebuah *ciphertext* yang lebih kuat. Varian lainnya adalah dengan menggunakan kunci berhuruf ganda seperti BACA atau DUDUK, dimana kolom yang memiliki huruf ganda dienkripsi menyamping, bukan vertikal. Varian ini disebut juga Transposisi Myszkowski.

3. KRIPTANALISIS KLASIK

Kriptanalisis kerap dilihat sebagai sesuatu yang buruk di masa ini karena dianggap sebagai ilmu yang dekat dengan para *hacker* yang mencoba mendapatkan informasi rahasia yang cukup berharga seperti kode pin ATM dan nomor rekening bank. Padahal kriptanalisis telah berjasa besar pada berbagai peristiwa seperti Perang Dunia I dan II, dimana ilmu kriptanalisis telah membantu menyelesaikan perang. Ataupun pada berbagai peristiwa masa kini dimana kriptanalisis berhasil memecahkan sebuah sandi yang berisi pesan tentang terorisme ataupun menangkap seorang gembong mafia.

Kriptanalisis, seperti yang sudah dijelaskan sebelumnya, adalah ilmu memecahkan sandi kriptografi yang terdiri dari berbagai disiplin ilmu, baik itu matematika, statistika, ilmu bahasa, dan berbagai ilmu lainnya. Teknik-teknik pemecahan sandi ini terus berkembang sesuai dengan perkembangan ilmu kriptografi, mulai dari kriptanalisis sederhana dengan alat tulis untuk kriptografi klasik sampai kriptanalisis yang penuh dengan matematika ilmu komputer untuk memecahkan kriptografi modern.

Terdapat beberapa macam kesuksesan dalam memecahkan sebuah sandi, diantaranya adalah sebagai berikut:

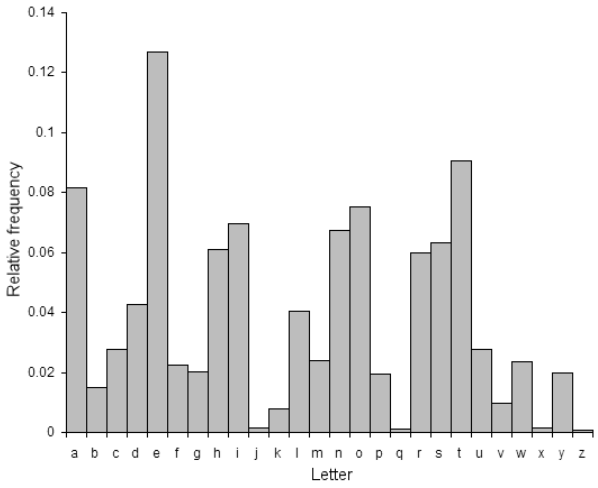
- Pemecahan total
  Mendapatkan kunci enkripsi.
- Deduksi global
  Mendapatkan algorima enkripsi tanpa kunci.
- Deduksi local
  Mendapatkan sebagaian *plaintext*.
- Deduksi informasi
  Mendapatkan entropi Shannon.
- Deduksi algoritma
  Mengetahui bahwa enkripsi tidak *random*.

Beberapa teknik dan metode kriptanalisis klasik adalah sebagai berikut:

- Analisa Frekuensi
- Analisa Kontak
- *Index of Coincidence*
- Pemeriksaan Kasiski

3.1 Analisa Frekuensi

Analisa frekuensi adalah sebuah studi tentang frekuensi munculnya suatu huruf, pasangan huruf, ataupun kata pada suatu bahasa untuk memecahkan sebuah *ciphertext*. Studi ini didasarkan pada kenyataan bahwa sebuah bahasa natural memiliki kecenderungan-kecenderungan tertentu. Misalnya terdapat huruf yang lebih sering muncul daripada yang lain atau pasangan huruf yang jarang muncul. Analisa frekuensi mempelajari hal-hal ini dan memanfaatkannya untuk memecahkan sandi kriptografi.



Gambar 9. *Monograph*

Gambar 9 menunjukkan sebuah *monograph*, sebuah grafik yang menunjukkan frekuensi kemunculan huruf dalam suatu bahasa, dan dapat kita lihat bahwa huruf E dan T adalah 2 huruf yang paling sering muncul pada bahasa Inggris (12 huruf yang paling sering muncul pada bahasa Inggris terdapat pada frase ETAOIN SHRLDU). Selain itu, ada juga kata yang lebih sering muncul pada kalimat, misalnya kata *the* pada bahasa inggris. Sementara pada bahasa Indonesia, huruf V, Q, X, dan Z amat jarang muncul, begitu juga pasangan huruf CK ataupun CT. *Cipher* yang tidak begitu kuat biasanya tidak mampu menyembunyikan sifat-sifat bahasa seperti ini sehingga sandinya dapat terpecahkan.

Analisa frekuensi lebih sering digunakan untuk memecahkan sandi kriptografi dengan *cipher* substitusi monoalfabetik karena *cipher* ini memetakan suatu alfabet ke alfabet lain, dengan kata lain, *cipher* ini bagaikan membuat sebuah bahasa baru dengan aturan yang sama dengan aturan bahasa pada *plaintext*. Misalnya, jika sebuah bahasa banyak memiliki huruf E, dan sebuah *ciphertext* dari bahasa tersebut memiliki banyak huruf K, maka kemungkinan besar huruf K adalah substitusi untuk huruf E pada *cipher* tersebut. Selain itu, berdasarkan analisa terhadap suatu frase, dapat dibentuk sebuah kata yang utuh, misalnya dari frase TEMSAT dapat ditebak bahwa *plaintext*-nya adalah TEMPAT dan S adalah substitusi untuk P, sehingga dapat mendekripsi huruf S pada bagian lain *ciphertext*.

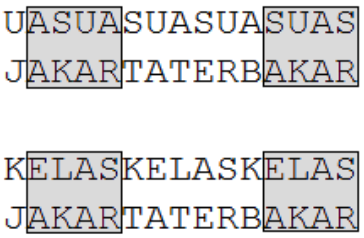
3.2 *Index of Coincidence*

Index of Coincidence adalah sebuah teknik yang ditemukan William F. Friedman yang menghitung jumlah kemunculan sebuah huruf pada lokasi yang sama di dua buah teks yang berbeda. Teknik ini sering diterapkan *cipher* substitusi polialfabetik seperti *cipher* Vigenère, karena jumlah *coincidence* biasanya paling banyak ketika lebar matriks alfabet adalah kelipatan panjang kunci, dan hal ini bisa digunakan untuk mendapatkan panjang kunci yang merupakan langkah pertama untuk memecahkan suatu sandi.

3.3 Pemeriksaan Kasiski

Pemeriksaan Kasiski adalah sebuah teknik Kriptanalisis lainnya yang ditemukan oleh Friedrich Kasiski pada tahun 1863 dalam usahanya memecahkan *cipher* Vigenère. Seperti *index of coincidence*, teknik ini berguna untuk memecahkan sandi dengan *cipher* substitusi polialfabetik dengan mendeduksi panjang kunci yang digunakan. Dan setelah panjang kunci tersebut didapat, *ciphertext* ditulis dalam matriks dengan kolom sebanyak panjang kunci, sehingga tiap kolom dapat dianggap sebagai *ciphertext* substitusi monoalfabetik yang lemah terhadap analisa frekuensi.

Teknik ini berpusat dalam mencari kumpulan huruf yang berulang pada suatu *ciphertext* untuk mendapatkan kelipatan panjang kunci, yang merupakan jarak antara dua buah kumpulan huruf tersebut. Kumpulan huruf yang dimaksud adalah kumpulan huruf dengan jumlah lebih dari tiga huruf, agar tidak tercampur dengan huruf yang berkumpul secara tidak sengaja.

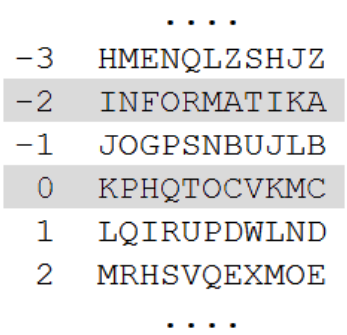


Gambar 10. Keterbatasan Pemeriksaan Kasiski

Sayangnya terdapat keterbatasan pada metode ini karena *ciphertext* hanya akan berulang bila kunci dan jarak antar huruf yang berulang mempunyai nilai tertentu. Seperti yang terlihat pada gambar 10, dengan kunci UAS, huruf-huruf AKAR pertama dan kedua tidak memiliki kunci yang sama, sehingga *ciphertext*-nya tentu tidak berulang juga. Sementara untuk kunci KELAS, kedua AKAR mendapat kunci ELAS sehingga akan terenkripsi ke dalam *ciphertext* yang sama.

3.4 Pemecahan *Caesar Cipher*

Caesar cipher adalah *cipher* substitusi sederhana yang melakukan enkripsi dengan menggeser alfabet beberapa huruf. Sebagai *cipher* substitusi monoalfabetik, *Caesar cipher* lemah terhadap analisa frekuensi yang dapat dengan cepat menebak seluruh algoritma hanya dengan menebak sebuah huruf pada *ciphertext* saja. Bukan hanya itu, *cipher* ini juga lemah terhadap metode kriptanalisis yang paling dasar, *brute force*, karena hanya memiliki 26 kemungkinan kunci.

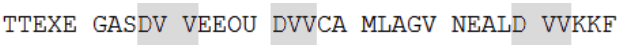


Gambar 11. *Brute force attack* terhadap *Caesar Cipher*

Seperti yang dapat dilihat pada gambar 11, melalui *brute force* dengan cepat *plaintext* bisa didapatkan dengan mencermati hasil pergeseran *ciphertext*. Pada gambar 11, *ciphertext*-nya adalah KPHQTOCVKMC, dan dengan beberapa kali melakukan pergeseran ke kanan dan kiri, dari tabel dapat kita lihat bahwa *plaintext*-nya adalah INFORMATIKA dengan enkripsi berupa pergeseran alfabet sebanyak 2 huruf.

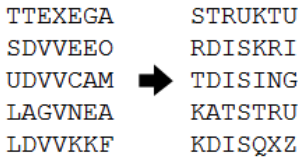
3.5 Pemecahan *Cipher* Vigenere

Cipher Vigenère terbukti sulit untuk dipecahkan dengan analisa frekuensi karena dapat menyembunyikan frekuensi hurufnya dengan baik sehingga tidak dapat dimanfaatkan untuk memecahkan *cipher* ini. Namun kelemahannya terdapat pada kuncinya yang diulang sampai sepanjang *plaintext*-nya sehingga bila panjang kuncinya diketahui, seluruh *ciphertext* dapat dibagi-bagi menjadi beberapa bagian dengan *cipher* substitusi monoalfabetik biasa yang dapat dipecahkan dengan metode analisa frekuensi.



Gambar 12. Pengulangan Pada *Ciphertext*

Metode untuk mencari panjang kata kunci yang biasa dipakai adalah dengan pemeriksaan Kasiski. Misalnya, pada gambar 12 disajikan sebuah *ciphertext* dengan huruf-huruf DVV sebagai elemen yang berulang sebanyak tiga kali pada teks tersebut. DVV pertama berjarak 7 huruf dengan DVV kedua dan 21 huruf dengan DVV ketiga, sementara DVV kedua dan ketiga berjarak 14 huruf. Dilihat dari jarak-jarak ini, dapat diambil kesimpulan bahwa panjang kata kuncinya adalah sepanjang faktor pembagi terbesarnya, yaitu tujuh buah huruf.



Gambar 13. Dekripsi *Ciphertext*

Setelah itu, *ciphertext* dapat dituliskan dalam bentuk matriks berkolom tujuh seperti pada gambar 13 sebelah kiri, dimana tiap kolom merupakan *Caesar Cipher* biasa yang bisa dipecahkan dengan *brute force*. Setelah mencoba berbagai pergeseran, didapatkan matriks seperti pada gambar 13 sebelah kanan yang dibaca STRUKTU RDISKRI TDISING KATSTRU KDISQXZ. Dengan mengubah spasi dan menghilangkan huruf tak berarti di belakang, didapatkan *plaintext* STRUKTUR DISKRIT DISINGKAT STRUKDIS.

4. KESIMPULAN

Pada dasarnya, kriptografi klasik terbagai menjadi dua jenis, yang pertama adalah *cipher* substitusi yang mensubstitusi huruf dengan huruf lain sehingga menjadi sebuah *ciphertext*, dan yang kedua adalah *cipher* transposisi yang mengubah urutan huruf pada *plaintext* dengan aturan tertentu sehingga menjadi tak terbaca lagi. Dua *cipher* substitusi yang terkenal adalah *Caesar Cipher* yang melakukan enkripsi dengan menggeser huruf dan *Cipher* Vigenère yang menggunakan tabel alfabet untuk melakukan enkripsi. Sementara *cipher* transposisi memiliki berbagai variasi yang di antaranya adalah *route cipher* yang menggunakan kunci berupa rute pembacaan teks dan tranposisi *columnar* yang menggabungkan pembacaan secara vertikal dan horizontal untuk membuat *ciphertext*.

Bila kriptografi klasik banyak terfokus pada matematika dan cara pembacaan, maka teknik pada kriptanalisis klasik terfokus pada pemanfaatan sifat bahasa dan pembentukan kalimat untuk memecahkah sandi kriptografi. Salah satu tekniknya adalah analisa frekuensi yang menganalisis frekuensi munculnya huruf dalam sebuah bahasa dan efektif dalam memecahkan sandi dengan *cipher* substitusi monoalfabetik. Teknik kriptanalisis yang lainnya adalah pemeriksaan Kasiski yang mencari panjang kata kunci yang efektif dalam memecahkan sandi dengan *cipher* substitusi polialfabetik.

REFERENSI

[1] http://en.wikipedia.org/wiki/Cryptography
Diakses pada tanggal 17 Desember 2009

[2] http://people.dsv.su.se/~matei/courses/IV2019/
Diakses pada tanggal 17 Desember 2009

[3] http://www.briancarter.info/pubs/classical_ciphers_and_cryptanalysis.pdf
Diakses pada tanggal 17 Desember 2009

[4] www.cs.uwlax.edu/~riley/CS455F09/Handouts/2.1.pdf
Diakses pada tanggal 17 Desember 2009