Perbandingan Enkripsi dan Kriptanalisis Substitusi Monoalfabetik pada Aksara Batak dan Aksara Latin

Parel Wellman Hutahaean (13507138)[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]*parel_hutahaean@s.itb.ac.id*

Abstrak* — Substitusi monoalfabetik merupakan salah satu metode kriptografi klasik. Metode ini masih dapat dikembangkan dengan menggunakan aksara non-Latin sebagai pasangan karakter Latin pada pesan yang ingin disembunyikan. Makalah ini akan mengkaji metode substitusi monoalfabetik yang melibatkan aksara Batak – sebagai aksara non-Latin – dan aksara Latin. Pertama yaitu mengkaji substitusi karakter-karakter aksara Latin sebagai plainteks ke dalam aksara Batak sebagai cipherteksnya. Selanjutnya mengkaji substitusi karakter-karakter plainteks aksara Batak dengan karakter aksara Batak lainnya sebagai cipherteksnya. Setelah itu akan dilakukan analisis untuk memecahkan cipherteks untuk mendapatkan isi pesan semula.

***Kata Kunci* — kriptografi klasik, substitusi monoalfabetik, aksara Batak, analisis frekuensi, kriptanalisis, *dictionary attack*.**

I. PENDAHULUAN

Metode substitusi monoalfabetik dalam kriptografi merupakan metode yang telah kadaluwarsa untuk dipakai pada zaman sekarang. Namun, penelitian terhadap metode ini masih menarik untuk dilakukan, terutama implementasinya terhadap aksara selain aksara Latin. Seperti eksperimen yang dilakukan oleh [1]. Pada eksperimen tersebut, pesan disembunyikan dengan menukar karakter-karakter pada pesan dalam aksara Latin dengan pasangan masing-masing karakter dalam aksara non-Latin, seperti aksara Yunani, Kiril (Rusia), Hangul (Korea), dan Jepang. Tujuan mengubah pesan ke aksara yang berbeda adalah mengecoh kriptanalis sehingga menyangka bahasa dari pesan tersebut adalah bahasa sesuai aksara cipherteksnya sehingga semakin sulit untuk memecahkan isi pesan tersebut.

Aksara-aksara di nusantara Indonesia sangat beragam dan dapat dijadikan kajian untuk memperkaya ilmu kriptografi terutama dalam menambah tingkat keamanan pada enkripsi pesan yang memakai metode substitusi monoalfabetik sehingga akan lebih sulit dalam memecahkannya bagi pihak yang tidak berkepentingan. Apalagi aksara yang dimaksud tidak dikenal secara luas oleh semua orang, hanya kalangan tertentu saja.

Saat ini beberapa aksara dari daerah di nusantara telah terdaftar dalam *The Unicode Standard* (Unicode). Versi yang paling baru sampai saat ini adalah versi 6.2 [2]. Unicode ini merupakan standar untuk *encoding*, representasi karakter, dan penanganan teks pada sistem penulisan digital. Sistem e*ncoding* karakter merupakan sistem penyandian dengan memasangkan karakter dengan representasinya dalam pola bit.

Aksara Batak merupakan salah satu aksara yang telah masuk dalam Unicode versi 6.2. UTF-8 (UCS Transformation Format 8 bit) adalah format Unicode yang paling umum digunakan baik pada sistem operasi maupun pada World Wide Web. Perangkat lunak pemroses kata (seperti Microsoft Word) dan aplikasi email dengan dukungan terhadap Unicode sudah dapat memuat aksara Batak dan aksara lain yang telah terdaftar dalam Unicode. Dengan demikian mengirimkan pesan tidak melulu hanya dengan menggunakan huruf Latin dan enkripsi pesan sebelum mengirimkannya telah dapat menerapkan substitusi monoalfabetik ke aksara non-Latin.

II. AKSARA BATAK

A. Latar Belakang

Suku Batak adalah salah satu suku di nusantara yang berasal dari Sumatera Utara. Dilihat dari kemiripan bahasa dan bukti-bukti historis, suku ini tergolong rumpun Austronesia (termasuk di antaranya penduduk asli Madagaskar, Taiwan, Filipina, Indonesia, Malaysia, dan sebagian besar wilayah kepulauan di Pasifik) dan merupakan kelompok suku Proto Melayu (termasuk orang Asli di Malaysia, Negrito di Filipina, serta Kubu, Toraja, dan Dayak di Indonesia). Suku Batak sebenarnya bukan merupakan satu suku melainkan beberapa suku yang digabung menjadi satu suku – karena kedekatan bahasa dan adat istiadat – oleh pemerintah kolonial Belanda, yang terbagi menjadi beberapa subsuku diantaranya Batak Toba, Karo, Simalungun, Pakpak, dan Mandailing/ Angkola.

Masyarakat tradisional Batak terbiasa berkomunikasi secara lisan, namun jarang menggunakan tulisan. Hanya kalangan tertentu saja yang mengenal dan fasih dengan aksara lokal, utamanya para dukun (*datu*) [3]. Dukun ini biasa menuliskan kitab yang terbuat dari kulit kayu berisi ilmu-ilmu hitam, putih, dan nujum dalam bahasa dan aksara setempat. Tulisan Batak selain dalam kitab ilmu

nujum (*pustaha*) juga ditemukan dalam bambu, tulang rusuk kerbau, dan kertas yang banyak berisi surat ancaman dan syair ratapan. Sementara yang termasuk sastra Batak seperti fabel, mitos, legenda, perumpamaan (*umpasa*), *torhan-torhanan*, *turi-turian*, dan *huling-hulingan* dituturkan hanya secara lisan.

Seiring dengan sampainya penjajah kolonial Belanda yang mendukung pula misi pengabaran Injil oleh misonaris Jerman di tanah Batak, maka aksara Batak semakin dikenal luas oleh masyakat setempat melalui Alkitab dengan cetakan bahasa dan aksara Batak. Fasilitas-fasilitas umum mulai memakai papan nama bertuliskan aksara Batak, dan sekolah-sekolah mengajarkan pelajaran bahasa Batak dalam aksara aslinya selain aksara Latin.

Masyarakat suku Batak telah tersebar ke luar daerah asalnya dan banyak yang merantau ke berbagai daerah di Indonesia dan mancanegara. Realitas menunjukkan hampir tidak ada di antara mereka yang menggunakan aksara Batak dalam komunikasi tertulis, meskipun dalam komunikasi lisan banyak yang menggunakan bahasa ibu. Sebagai wujud pelestarian budaya, menggunakan aksara Batak dalam komunikasi sesama orang Batak merupakan langkah sederhana yang dapat dilakukan, sebagai contoh dalam berkirim email. Untuk menjaga kerahasiaan, enkripsi pesan dengan substitusi monoalfabetik dapat digunakan dalam hal ini

B. Alih Aksara antara Aksara Batak dan Aksara Latin

Aksara Batak dikenal masyarakat setempat dengan sebutan *Surat* Batak (*surat* disini tidak sama artinya dengan 'surat' pada bahasa Indonesia, melainkan berarti aksara). Terdapat beberapa abjad dalam aksara Batak yang berbeda antara subsuku yang satu dengan subsuku yang lain. Ada pula abjad yang tidak dipakai pada beberapa subsuku karena faktor bahasa. Penulis akan memilih varian aksara Batak Toba sebagai contoh dalam pembahasan.

Aksara Batak dibagi menjadi *ina ni surat* (literal: induk aksara) dan *anak ni surat* (literal: anak aksara). *Ina ni surat* terdiri dari abjad utama yang membentuk konsonan, sementara *anak ni surat* terdiri dari abjad yang membentuk vokal. Kalau dalam aksara Latin satu huruf dapat merupakan konsonan atau vokal, sementara dalam aksara Batak satu huruf *ina ni surat* merupakan konsonan diikuti vokal 'a' (kecuali 'i' dan 'u'). Contoh huruf h dibaca 'ha'. Untuk membentuk konsonan dan vokal selain 'a' (KV) maka diperlukan *anak ni surat*. Abjad pada *anak ni surat* yang ditulis mengikuti suatu *ina ni surat* akan mengubah bunyi vokalnya. Contoh huruf h diikuti huruf o (yang berbunyi 'o') menjadi ho dibaca 'ho'.

Pada Tabel 1 dapat diketahui huruf mana dalam bahasa Latin yang tidak dipakai dalam aksara Batak, yaitu 'q', 'x' dan 'z'. Pada tabel tersebut terdapat vokal 'a', 'i', dan 'u' yang termasuk *ina ni surat* untuk dipakai tanpa mengikuti konsonan, seperti 'i' pada kata *ina* (arti: ibu). Lalu bagaimana dengan 'e' dan 'o'. Pada aksara Batak untuk membentuk 'e' dilakukan dengan memakai a ('a') diikuti *anak ni surat* seperti pada Tabel 2 menjadi ae ('e') dan ao ('o').

	Mandailing	Simalungun	Toba	Pakpak	Karo
a					
ha					
ka					
ba					
pa					
na					
wa					
ga					
ja					
da					
ra					
ma					
ta					
sa					
ya					
nga					
la					
nya					
ca					
nda					
mba					
i					
u					

Tabel 1. Daftar abjad *ina ni surat* dalam aksara Batak dan variannya [4]

	Karo	Pakpak	Simal.	Toba	Mand.
-ĕ					
-e					
-i					
-o					
-ou					
-u					
-ng					
-h					
-					

Tabel 2. Daftar abjad *anak ni surat* dalam aksara Batak dan variannya (bentuk oval menunjukkan *ina ni surat*) [4]

Ada abjad yang bukan merupakan bunyi tapi sebagai pembunuh vokal yang disebut *pangolat* atau \. Abjad ini apabila ditulis mengikuti *ina ni surat* maka akan menghilangkan vokal 'a'-nya. Contoh h (yang juga dibaca sebagai 'ka') apabila diikuti *pangolat* \ menjadi h\ akan dibaca 'k' seperti pada kata *mula*k (arti: pulang). Untuk bunyi sengau '–ng' ada abjad tersendiri pada *anak*

ni surat, tidak memakai ‘na’ + *pangolat* + ‘ga’ + *pangolat* (`n\g\`) maupun ‘nga’ + *pangolat*.

Satu lagi yang perlu diingat adalah pada penulisan kata *sintong* (arti: benar) dimana suku kata ‘sin’ merupakan fonem konsonan-vokal-konsonan (KVK) dengan vokal bukan ‘a’. Kalau dari penjelasan sebelumnya kita bisa mulai mengalihaksarakannya ke aksara Batak, diuraikan sebagai berikut:

sin = *ina ni surat* ‘sa’ (`s`) + *anak ni surat* ‘i’ (`i`) + *ina ni surat* ‘na’ (`n`) + *pangolat* (`\`) = `sin\`

namun penulisan tersebut dalam aksara Batak tidak benar. Yang benar adalah *anak ni surat* harus diletakkan pada *ina ni surat* yang dikenai *pangolat*, atau K kedua pada fonem KVK tersebut. Berikut ini adalah bentuk yang benar:

sin = *ina ni surat* ‘sa’ (`s`) + *ina ni surat* ‘na’ (`n`) + *anak ni surat* ‘i’ (`i`) +*pangolat* (`\`) = `sni\`

Kemudian untuk suku kata ‘tong’ yang diikuti dua *anak ni surat* (o dan ng) maka letakkan saja keduanya pada ina ni surat tersebut, seperti berikut ini:

tong = *ina ni surat* ‘ta’ (`t`) + *anak ni surat* ‘o’ (`o`) + *anak ni surat* ‘ng’ (`^`) + *pangolat* (`\`) = `to^`

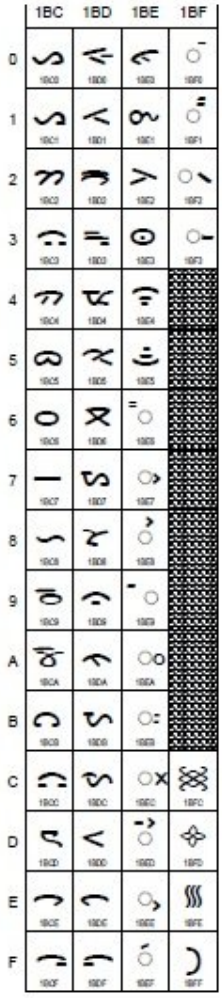
Berikut ini adalah perbadingan abjad dengan variasi *anak ni surat*-nya:

ha = `h`	hang = `h^`	han = `hn\`
he = `he`	heng = `he^`	hen = `hne\`
hi = `hi`	hing = `hi^`	hin = `hni\`
ho = `ho`	hong = `ho^`	hon = `hno\`
hu = `H`	hung = `H^`	hun = `hN\`

Alih aksara dari aksara Latin ke aksara Batak sebaiknya dilakukan pada tulisan yang menggunakan bahasa Batak. Jika alih aksara dilakukan pada bahasa Indonesia, maka akan ditemukan kendala terutama yang mengandung fonem KK, kecuali ‘mb’, ‘nd’, ‘ng’, atau ‘ny’, apalagi jika menggunakan bahasa Inggris yang mengandung huruf ‘q’, ‘x’, dan ‘z’.

C. Aksara Batak pada Unicode 6.2

Unicode merupakan standar untuk *encoding* teks dalam pertukaran informasi. Dalam Unicode tersebut aksara Batak dimulai dari U+1BC0 sampai U+1BFF. Meskipun aksara Batak memiliki variasi menurut dialek Toba, Karo, Simalungun, Pakpak, dan Mandailing/Angkola, semuanya digabung ke dalam kelompok representasi Unicode tersebut.



Tabel 3. Daftar abjad aksara Batak pada Unicode (baris menunjukkan LSB) [5]

Saat in telah ada *add-ins* jenis tulisan (*font*) untuk mengetikkan aksara Batak pada Microsoft Office [6]. *Add-ins* tersebut memisahkan antara dialek-dialek Batak. Jadi untuk mengaktifkan *font* Batak Toba, instalasi *add-ins* yang untuk aksara Toba saja. Pemakai harus tahu tombol mana di *keyboard* untuk mengetikkan abjad tertentu, misalnya dengan mengetikkan ‘m’ lalu ‘a’ tidak serta-merta tampil `m` melainkan `ma`.

III. ENKRIPSI PESAN AKSARA LATIN KE AKSARA BATAK

A. Substitusi Monoalfabetik

Substitusi monoalfabetik adalah algoritma enkripsi dengan cara mengganti setiap huruf yang ada pada plainteks dengan huruf lain yang telah ditentukan pada tabel konversi. Tabel konversi berisi semua huruf dalam alfabet beserta huruf pasangannya (huruf pengganti). Tabel konversi ini menjadi kunci untuk digunakan pada proses enkripsi dan dekripsi. Algoritma ini telah dipakai sejak zaman Kerajaan Romawi yang dikenal dengan

Caesar Cipher. Huruf-huruf pengganti pada Caesar Cipher tersebut dibuat hanya dengan menggeser 3 urutan dari abjad semula.

Plain	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
Cipher	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

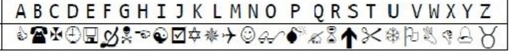
Tabel 4. Tabel Konversi Caesar Cipher

Tabel konversi bisa juga dibuat dengan memasangkan huruf plainteks dengan huruf pengganti yang acak.

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

Tabel 5. Tabel Konvesi Substitusi Monoalfabetik 1

Atau bisa pula dengan memakai simbol-simbol sebagai huruf pengganti.

Plain	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
Cipher	

Tabel 5. Tabel Konvesi Substitusi Monoalfabetik 2

B. Analisis Frekuensi pada Substitusi Monoalfabetik

Kriptanalisis adalah ilmu yang mempelajari metode untuk memecahkan cipherteks. Orang yang berperan dalam kriptanalisis disebut kriptanalis.

Cipherteks yang menggunakan algoritma substitusi monoalfabetik dapat dipecahkan dengan analisis frekuensi, dimana frekuensi huruf atau simbol yang muncul pada cipherteks menggambarkan huruf sebenarnya pada plainteks. Artinya, kita bisa menganggap huruf atau simbol yang paling sering muncul pada cipherteks merupakan pasangan atau pengganti huruf yang paling sering muncul pada teks pada umumnya. Frekuensi huruf yang paling sering muncul pada teks pada umumnya ini dianggap sama dengan frekuensi huruf pada plainteks.

Analisis frekuensi mudah dipecahkan hanya bila kriptanalis tahu bahasa yang dipakai pada pesan (plainteks) tersebut, karena frekuensi huruf pada tiap bahasa bisa berbeda-beda. Huruf yang paling sering mucul pada teks bahasa Inggris pada umumnya secara berurut adalah E, T, A, O, I, N, S, H, R, D, L, dan U. Pada teks berbahasa Indonesia tentu lain halnya, tidak bisa menggunakan huruf diatas sebagai acuan.

C. Substitusi Monoalfabetik dari Aksara Latin ke Aksara Batak

Sebagaimana dijelaskan pada [1], algoritma yang cukup aman untuk substitusi monoalfabetik adalah dengan meng-*encode* plainteks terlebih dahulu dengan Base64 sebelum dienkripsi dengan substitusi. Cara kerja Base64 tersebut adalah sebagai berikut.

- Kelompokkan pesan setiap 3 karakter (3 byte = 24 bit).
- Bila terdapat sisa di akhir, tambahkan (*padding*) bit 0 sehingga panjangnya genap 24 bit.
- Pecah 24 bit tadi menjadi 4 kelompok yang masing-masing beranggotakan 6 bit.
- Setiap kelompok sekarang punya 2^6 kemungkinan susunan bit, berarti ada $2^6 = 64$ karakter tersedia untuk merepresentasikan 6 bit ini.
- Petakan setiap kelompok dengan karakter yang terdapat dalam tabel

Jadi, karakter yang dipakai termasuk huruf kapital A-Z (26 karakter), huruf kecil a-z (26 karakter), angka 0-9 (10 karakter) dan simbol + dan / sehingga total karakter ada 64.

Bit	Desimal	Karakter	Bit	Desimal	Karakter
000 000	0	A	100 000	32	g
000 001	1	B	100 001	33	h
000 010	2	C	100 010	34	i
000 011	3	D	100 011	35	j
000 100	4	E	100 100	36	k
000 101	5	F	100 101	37	l
000 110	6	G	100 110	38	m
000 111	7	H	100 111	39	n
001 000	8	I	101 000	40	o
001 001	9	J	101 001	41	p
001 010	10	K	101 010	42	q
001 011	11	L	101 011	43	r
001 100	12	M	101 100	44	s
001 101	13	N	101 101	45	t
001 110	14	O	101 110	46	u
001 111	15	P	101 111	47	v
010 000	16	Q	110 000	48	w
010 001	17	R	110 001	49	x
010 010	18	S	110 010	50	y
010 011	19	T	110 011	51	z
010 100	20	U	110 100	52	0
010 101	21	V	110 101	53	1
010 110	22	W	110 110	54	2
010 111	23	X	110 111	55	3
011 000	24	Y	111 000	56	4
011 001	25	Z	111 001	57	5
011 010	26	a	111 010	58	6
011 011	27	b	111 011	59	7
011 100	28	c	111 100	60	8
011 101	29	d	111 101	61	9
011 110	30	e	111 110	62	+
011 111	31	f	111 111	63	/

Tabel 6. Daftar Base64 lengkap

Berikut ini adalah contoh *encoding* menggunakan Base64.

Plainteks Nama saya Parel.

<table>
<tr><td colspan="3">N</td><td colspan="3">a</td><td colspan="2">m</td></tr>
<tr><td colspan="3">0100 1110</td><td colspan="3">0110 0001</td><td colspan="2">0110 1101</td></tr>
<tr><td colspan="2">010 011</td><td colspan="2">100 110</td><td colspan="2">000 101</td><td colspan="2">101 101</td></tr>
<tr><td colspan="2">T</td><td colspan="2">m</td><td colspan="2">F</td><td colspan="2">t</td></tr>
</table>

Encoding TmFtYSBzYXlhIFBhcmVsLgAA

Pada langkah enkripsi, ada 64 karakter unik dalam aksara latin yang harus disubstitusi ke aksara Batak. Tentunya minimal harus ada 64 abjad Batak tersedia sebagai pengganti 64 karakter tersebut. Agar cipherteks yang dihasilkan mengikuti aturan penulisan yang tepat

dalam aksara Batak, maka ada beberapa hal yang harus dipertimbangkan untuk memilih karakter-karakter sebagai pengganti abjad plainteks, yaitu:

- Terlebih dahulu pilih aksara dialek mana yang akan dipakai.
- Jangan pernah memakai *anak ni surat* sendirian sebagai pengganti karakter Latin.
- Karakter pengganti boleh hanya *ina ni surat* saja maupun kombinasi 1 *ina ni surat* dan (1 atau 2) *anak ni surat*.
- Jangan mengkombinasi *ina ni surat* a, i, dan u dengan *pangolat*
- Karakter pengganti ini tidak selalu suku kata. Ada suku kata yang terdiri dari 2 karakter pengganti (2 *ina ni surat*), contoh: sin (`sni\`)

Berikut ini adalah contoh daftar aksara apa saja dalam dialek Toba yang bisa dijadikan pengganti abjad Latin. Ada 99 abjad yang merupakan 1 dan 2 karakter (untuk yang 3 karakter tidak ditampilkan) seperti ditunjukkan pada Tabel 7.

	a	e	i	o	u	pangolat
a	a	ae	I	ao	U	
ha/ka	h	he	hi	ho	H	h\
ba	b	be	bi	bo	B	b\
pa	p	pe	pi	po	P	p\
na	n	ne	ni	no	N	n\
wa	w	we	wi	wo	W	w\
ga	g	ge	gi	go	G	g\
ja	j	je	ji	jo	J	j\
da	d	de	di	do	D	d\
ra	r	re	ri	ro	R	r\
ma	m	me	mi	mo	M	m\
ta	t	te	ti	to	T	t\
sa	s	se	si	so	S	s\
ya	y	ye	yi	yo	Y	y\
nga	<	<e	<i	<o	>	
la	l	le	li	lo	L	l\
nya	[	[e	[i	[o	]	

Tabel 7. Daftar abjad pengganti dalam aksara Toba

Misalkan tulisan "Nama saya Parel." tadi dienkripsi. Salah satu contoh cipherteksnya adalah `RnoJmojehwimijeg\PpbeJwipbnom\m\n\gene ne`.

Berbeda halnya kalau kita tidak menggunakan *encoding* Base64 dalam enkripsi ini, kita hanya butuh mensubstitusi 26 huruf Latin dan mengabaikan tanda baca atau simbol lain. Cipherteks yang dihasilkan tidak akan sepanjang yang memakai *encoding* namun pastinya lebih tidak aman karena dapat dipecahkan dengan analisis frekuensi. Bedanya kalau karakter penggantinya memakai aksara Batak ini, kriptanalis akan keliru kalau memeriksa karakter per karakter, karena bisa jadi ada 2 karakter aksara Batak yang berkorespondensi dengan satu karakter Latin.

IV. SUBSTITUSI MONOALFABETIK DARI AKSARA BATAK KE AKSARA BATAK

Jika sebelumnya dibahas tentang substitusi monoalfabetik dari aksara Latin ke aksara Batak, kali ini akan dibahas yang dari aksara Batak ke aksara Batak. Maksud bagian ini adalah mencoba melihat metode ini dari sisi bahasa Batak. Pembahasan biasanya melulu dilakukan terhadap bahasa Inggris. Penutur bahasa Batak semestinya sudah bisa menggunakan aksara Batak dalam komunikasi tulisan, sama seperti bahasa Mandarin memakai aksara Mandarin.

A. Enkripsi Pesan

Ada dua pendekatan bagaimana kita melakukan substitusi monoalfabetik pada aksara Batak, pertama kita mensubstitusi per karakter atau mensubstitusi per *ina ni surat*.

1. Substitusi per karakter

   Ini adalah pendekatan yang paling mudah diimplementasi. Artinya satu karakter Unicode akan disubstitusi dengan satu karakter Unicode lainnya. Namun kekurangannya adalah cipherteks akan mengabaikan penulisan aksara yang benar. Huruf *ina ni surat* bisa disubstitusi dengan huruf *anak ni surat*, begitu juga sebaliknya. Sehingga akan ada cipherteks yang seperti ini `\ap\<hio`, dimana *pangolat* terdapat di awal dan ada *anak ni surat* tidak punya *ina ni surat*.

   Kekurangan tersebut tidak perlu dipermasalahkan karena sebenarnya orang yang baca cipherteks diasumsikan sudah mengerti bahasa Batak dan aksaranya, sehingga tahu cipherteks itu adalah bukan isi sebenarnya.

   Contoh tabel konversi:

plain	a	h	b	p	n	eew	i	o	\
ciph.	i	d	r	o	\	t	g	a	b

2. Substitusi per *ina ni surat*

   Pendekatan ini sama seperti yang dipakai pada substitusi dari aksara Latin ke aksara Batak. Cipherteks yang dihasilkan menggunakan penulisan yang benar dan kriptanalisis akan lebih rumit, namun kita akan berhadapan dengan masalah bahwa 1 karakter Unicode bisa jadi berkorespondensi dengan 2 atau 3 karakter Unicode lain. Artinya implementasi menjadi lebih rumit.

   Contoh tabel konversi:

plain	a	bi	ro	ti\	L
ciph.	m\	T\	l	de	s

B. Kriptanalisis

Ada berbagai cara untuk menganalisis cipherteks hasil substitusi monoalfabetik. Salah satu caranya adalah dengan *dictionary attack* [8]. Algoritma ini tidak memerlukan analisis frekuensi karena akan mecoba memecahkan cipherteks dengan mensubstitusi semua kemungkinan kata yang ada dalam kamus dengan setiap kata pada cipherteks. Namun, penelitian yang telah dilakukan hanya menangani cipherteks yang dipisahkan spasi dan mengasumsikan spasi tersebut memisahkan masing-masing kata. Sementara teks bahasa Batak sebenarnya tidak mengenal spasi. Sebenarnya *dictionary attack* masih bisa dikembangkan untuk cipherteks yang tidak dipisahkan spasi, tapi pasti komputasinya akan lebih lama.

Cara lainnya adalah dengan analisis frekuensi. Untuk saat ini, *bibel* (atau alkitab dalam bahasa Batak) belum ada yang format digitalnya dalam aksara Batak. Sehingga analisis frekuensi terhadap abjad-abjad dalam aksara Batak belum bisa dilakukan oleh penulis. Namun, jika analisis frekuensi dilakukan pada *bibel* yang format digitalnya dalam aksara Latin, maka metode ini tidaklah mudah dipakai untuk menganalisis cipherteks. Tetapi dibandingkan menggunakan algoritma *bruteforce* dalam memecahkannya, analisis frekuensi bisa menjadi pilihan yang lebih efisien. Tentunya perlu intervensi manusia dalam prosesnya dan akan memakan waktu yang lebih lama daripada pada kriptanalisis dalam aksara Latin.

Berikut ini adalah daftar 5 huruf Latin yang sering muncul dalam teks berbahasa Batak. Penghitungan dilakukan terhadap *bibel* hanya pada Surat Kejadian, Keluaran, Imamat, Bilangan, dan Ulangan, karena sangat banyak kalau mengambil keseluruhan isi *bibel*.

Huruf	Persentase
A	15,9
N	10,2
I	7,0
O	5,8
U	4,7

Huruf A adalah yang paling sering muncul. Namun dalam aksara Batak ‘a’ terkandung dalam semua abjad *ina ni surat*. Kita tidak boleh menganggap a adalah abjad Batak yang paling sering muncul karena pada kenyataannya kata-kata yang paling banyak digunakan yang adalah yang ‘a’-nya melekat pada *ina ni surat* selain a (perbandingan pada a dengan *ina ni surat* lain 1:15).

Dengan huruf N yang kedua paling sering muncul, maka kita bisa menganggap n adalah termasuk aksara paling sering muncul karena ‘n’ merupakan n\.

Huruf I dan U masing-masing memiliki dua bentuk; ‘i’: I dan i, ‘u’: U dan >. Kedua bentuk ‘i’ kemunculannya hampir sama. Sementara betuk ‘u’ yang > paling sering dipakai. Hal ini menyebabkan keduanya tidak lagi masuk pada abjad paling sering muncul.

Huruf O memiliki bentuk ao dan o. Abjad o bisa dianggap sebagai abjad Batak yang termasuk paling sering muncul. Bentuk bisa menambah frekuensi abjad , namun pemakaian ‘o’ bentuk ini tidaklah banyak sehingga tidak signifikan.

Bentuk dan adalah abjad yang sering muncul, namun analisis frekuensi akan lebih akurat jika dilakukan langsung terhadap teks dengan aksara Batak karena akan didapat urutan abjad (karakter Unicode) Batak yang paling sering muncul.

Metode kriptanalisis ini hanya bisa dipakai pada substitusi monoalfabetik dengan pendekatan pertama pada penjelasan subbab sebelumnya, sementara untuk yang pendekatan kedua tidak dibahas.

V. KESIMPULAN

Metode substitusi monoalfabetik untuk enkripsi teks Latin ke teks aksara Batak lebih aman dibandingkan apabila dienkripsi ke teks Latin. Dengan menambahkan langkah *encoding* dengan Base64 akan meningkatkan keamanan namun menambah ukuran teks.

Enkripsi substitusi monoalfabetik dari dan ke teks aksara Batak dapat dilakukan dengan 2 pendekatan dengan kelebihan dan kekurangannya. Kriptanalisis cukup rumit dan menjadi tugas kita selanjutnya bagaimana memecahkannya

VI. REFERENSI

[1] Yusuf Adriansyah, “Enkripsi sederhana dengan Base64 dan substitusi monoalfabetik ke huruf non-Latin”, 2010.

[2] http://www.unicode.org/versions/Unicode6.2.0, diakses 24 Maret 2013

[3] Kozok, Uli, *Surat Batak: Sejarah Perkembangan Tulisan Batak Berikut Pedoman Menulis Aksara Batak dan Cap Sisingamangaraja XII*, hal. 16-19. Jakarta: Kepustakaan Populer Gramedia dan Ecole française d'Extrême-Orient.

[4] http://ulikozok.com/aksara-batak/belajar-aksara-batak, diakses 24 Maret 2013

[5] http://www.unicode.org/charts/PDF/U1BC0.pdf, diakses 24 Maret 2013

[6] http://ulikozok.com/aksara-batak/batak-font, diakses 25 Maret 2013

[7] http://crypto.lkdev.com, diakses 27 Maret 2013

[8] Haryus Aminul Akbar, “Analisis Serangan *Dictionary Attack* pada Cipherteks Berbasis Substitusi Monoalfabetik”, 2011

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 4 April 2013

Parel Wellman Hutahaean
13507138