Nas_Jurnal #21 Rekayasa Penyandian Konvensional “SUKMEZ”

by Purwanto Purwanto

Submission date: 18-Apr-2020 10:10PM (UTC+0700)
Submission ID: 1300950730
File name: Nas_Jurnal_21_Rekayasa_Penyandian_Konvensional_SUKMEZ_txt.pdf (5.15M)
Word count: 5508
Character count: 30283

JURNAL TEKNOLOGI INFORMASI

Volume 3, Nomor 1, Pebruari 2007
ISSN 1414-9999

CyberKU

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 3 Nomor 1	Halaman 231 - 329	Semarang Pebruari 2007	ISSN 1414-9999

JURNAL TEKNOLOGI INFORMASI

olume 3, Nomor 1, Pebruari 2007
SSN 1414-9999

CyberKU

DEWAN REDAKSI

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 3 Nomor 1	Halaman 231 - 329	Semarang Pebruari 2007	ISSN 1414-9999

JURNAL TEKNOLOGI INFORMASI

Volume 3, Nomor 1, Pebruari 2007
ISSN 1414-9999

CyberKU

DAFTAR ISI

Diterbitkan oleh
Program Pascasarjana Magister Teknik Informatika
UNIVERSITAS DIAN NUSWANTORO

Jurnal Teknologi Informasi	Volume 3 Nomor 1	Halaman 231 - 329	Semarang Pebruari 2007	ISSN 1414-9999

REKAYASA PENYANDIAN KONVENSIONAL "SUKMEZ" UNTUK PENGAMANAN FILE TEKS

Erna Zuni Astutik, Mahasiswa Magister Teknik Informatika Udinus
Mohammad Sidiq, Dosen Magister Teknik Informatika Udinus
Purwanto, Dosen Magister Teknik Informatika Udinus

ABSTRACT

Conventional coding will still axist and have an important role in the future document saving. It can be used by adding several facilities, techniques, perspectives and developing it broadly. "Sukmez" coding is one of conventional coding form. Therefore, "Sukmez" coding will still be able to be applied to save document, especially to save text-form file. To save text-form file using "Sukmez" coding means to save the document's secrecy, authenticity, recognition and integrity control. There are several advantages of "Sukmez" coding compared to the other existed conventional codings, those are: It is relatively newly-found and newly-applied; it can code numbers; it can distinguish upper case letter from the lower case ones; it has many keys; it vories and does not need assistant characters.

Key words : Conventional code, "Sukmez" code, monoalphabetic, "Sukmez" symbol

I. PENDAHULUAN

1.1. Latar Belakang

Laju perkembangan teknologi informasi sekarang ini sangat pesat dan membanggakan. Oleh karena itu masalah keamanan suatu dokumen menjadi topik utama. Menurut jurnal yang ditulis oleh Sasa Rudan, Aleksandra Kovacevic dan Veljko Milutinovic yang berjudul *"Data Assurance in Conventional File systems"* [1], dituliskan bahwa: *" Cryptographic techniques can play an important role in protecting data, since access to data can be limited to those who hold the proper key. There are several basic security service that cryptography may provide: confidentiality, data integrity, authentication, authorization and non repudiation. In many applications, the combination of cryptographic services is desired"*. Bertitik tolak dari jurnal yang disebutkan di atas, maka penyandian atau kriptografi khususnya kriptografi konvensional boleh dikatakan benar-benar memegang peranan penting dalam proteksi, pengamanan dan perlindungan terhadap data atau dokumen.

Mengapa data, naskah atau dokumen itu perlu diberikan proteksi pengamanan dan perlindungan? Pertama karena sifatnya sangat rahasia, kedua karena tidak semua orang punya hak untuk mengetahui isinya dan ketiga karena akhir-akhir ini banyak dikeluhkan masyarakat tentang keberadaan *hacker, cracker* dan *attacker* yang ingin menyusup dan mengganggu naskah orang lain sehingga bisa membahayakan keberadaan, keautentikan dan integritas suatu dokumen .

Salah satu sandi yang sudah dikenal masyarakat dalam melindungi dan mengamankan dokumen rahasia adalah penyandian konvensional. Tetapi sandi konvensional yang ada sekarang ini masih kurang sempurna, karena sebagian besar tidak bisa menyandikan angka, tidak bisa membedakan antara huruf besar dan huruf kecil, tidak memperhatikan tentang spasi yang memisahkan kata yang satu dengan kata yang lain dalam suatu kalimat, sehingga satu kesatuan kalimat terpaksa dijadikan sebagai satu kelompok dan biasanya hanya untuk pesan yang singkat singkat saja. Oleh karena itu perlu dibuatkan sandi konvensional baru yang diharapkan bisa menyempurnakan berbagai kekurangan tersebut.

Pembuatan sandi yang dimaksud disini adalah membuat metode Enkripsi dan Dekripsi penyandian konvensional dari suatu informasi yang berbentuk file teks. Menurut jurnal yang berjudul *"Recent Development in the Design of Conventional Cryptographic Algorithms"* yang ditulis oleh Bart Preneel, Vincent Rijmen dan Anton Bosselaers [3] mengatakan bahwa tujuan

akhir dari penulisan jurnalnya adalah: menunjukkan bahwa jenis penyandian konvensional akan tetap eksis di masa yang akan datang dengan menyediakan berbagai macam teknik dan perspektif pengembangan penyandian secara luas.

Keuntungan penggunaan Enkripsi [4] adalah jika metode lain untuk melindungi data biasanya menggunakan daftar kontrol akses, file *permissions*, *password* dan lain lain yang bisa dibongkar oleh penyusup, maka dengan menggunakan metode Enkripsi ini meskipun penyusup berhasil membuka *password*-nya, maka data maupun informasi yang diperoleh penyusup tersebut tidak akan memberi arti apapun jika tidak bisa menemukan Dekripsinya.

Sampai saat ini, plaintext bisa dinyatakan dalam berbagai macam bentuk seperti aliran bit, file teks, bitmap, aliran suara/file suara (wav, mp3), gambar video digital, file gambar (gif, jpg), file biner (exe, com, ocx), dan lain-lain. Tetapi yang paling banyak dijumpai dimasyarakat adalah naskah atau dokumen yang berbentuk file teks.

Berdasarkan pada latar belakang di atas, maka penulis sangat tertarik untuk mengambil judul: **"Rekayasa penyandian Konvensional "Sukmez" untuk Pengamanan file Teks"** yang belum dikenal oleh masyarakat luas, dan untuk pertama kalinya penulis memperoleh ide ini dari pembuatan penyandian yang diilhami dari sandi sederhana sewaktu penulis mengikuti kegiatan kepramukaan beberapa tahun silam yang sangat berkesan dan menarik.

1.2. Rumusan Masalah

Adapun pokok permasalahan utama dalam penulisan tesis ini dapat dirumuskan sebagai berikut:

1. Bagaimana membuat metode Enkripsi dan Dekripsi penyandian konvensional yang bisa menutupi kelemahan sandi sandi konvensional yang sudah ada sebelumnya.
2. Bagaimana membuat *Software* yang sesuai dengan metode Enkripsi dan Dekripsi yang akan dibuat.

1.3. Tujuan dan Manfaat

1.3.1. Tujuan

Membuat metode Enkripsi, Dekripsi dari kriptografi penyandian konvensional dan *software* penyandian yang sesuai, dari suatu informasi yang berbentuk file teks, baik yang berupa abjad huruf besar/balok, huruf kecil maupun angka, sehingga dokumen menjadi aman dan para penyusup seperti *Hacker*, *Cracker dan Attacker* tidak dapat membaca *ciphertext*-nya, apalagi memahami isi dokumen tersebut meskipun mereka berhasil membongkar *password*-nya.

1.3.2. Manfaat

Dengan dibuatkannya metode Enkripsi dan dekripsi konvensional ini, diharapkan dapat bermanfaat untuk:

a. Melindungi dan mengamankan suatu dokumen yang berupa file teks seperti: surat wasiat, surat perjanjian, akta - akta rahasia, naskah ujian maupun naskah naskah penting lainnya.
b. Menjaga kerahasiaan, keaslian, pengakuan dan kontrol integritas dari suatu dokumen.
c. Menambah wawasan, pengetahuan dan pandangan khususnya ilmu pengetahuan tentang pengembangan Kriptografi di Lingkungan Pendidikan di Indonesia

1.4. Metode Rekayasa dan Pengembangan sistem

Rekayasa penyandian dan Perancangan Sistem penyandian konvensional ini, berpegang pada model pengembangan sistem *Waterfal*, yang berisi rangkaian aktivitas beberapa proses yang

saling terpisah, seperti spesifikasi kebutuhan, implementasi desain perangkat lunak, uji coba dan lain sebagainya.

2. TINJAUAN PUSTAKA

2.1. Kriptografi

Kriptografi terdiri dari Enkripsi dan Dekripsi. Enkripsi didefinisikan sebagai proses konversi dari suatu informasi dalam bentuk yang dapat dibaca ke dalam bentuk yang tidak dapat dimengerti oleh pihak lain melalui kunci tertentu. Sedangkan Dekripsi adalah invers atau kebalikan dari proses Enkripsi, yaitu proses pemulihan atau pengembalian data ke bentuk semula juga melalui kunci tertentu [4].

2.2. Kriptosistem

Kriptosistem merupakan satu kesatuan himpunan pasangan 3 yang tak dapat terpisah-pisahkan yang terdiri dari (G, E, D): di mana G. adalah himpunan algoritma kunci yang bersifat probabilistik selalu menghasilkan output sepasang kunci (k_e, k_d). Dengan k_e adalah kunci enkripsi dan k_d adalah kunci dekripsi. Dalam lingkungan kriptosistem, mengenai kunci dapat dibedakan kedalam 2 tipe sebagai berikut [6]:

a. Dalam penyandian konvensional atau simetri, selalu didapatkan rumusan bahwa $k_e = k_d$. Selanjutnya didefinisikan dua buah simbol himpunan yaitu himpunan P adalah Plaintext, dan himpunan C adalah Ciphertext.
b. Dalam *public-key* atau asimmetri kriptografi, kunci k_e adalah berbeda dengan kunci k_d, karena perbedaan ini maka masalah komputerisasi terpentlng adalah mencarl k_d, apablla k_e sudah diketahui.

Dengan demikian bisa disimpulkan bahwa G adalah himpunan keamanan data yang terdiri dari himpunan Plaintext P, himpunan Ciphertext C, dengan parameter k, dan sebagai input, dan outputnya adalah pasangan (k_e, k_d). E, adalah algoritma untuk membuat enkripsi: algoritma ini melibatkan input k_e dan (x), P dan produk yang dihasilkan adalah output E $k_e(x) = C$. dengan catatan E adalah bersifat probabilistik. D, adalah algoritma untuk membuat dekripsi: algoritma ini memanfaatkan input kd, dan (y), C dan produknya adalah output D $kd(y) = P$. Ini juga boleh berupa probabilitas, tetapi sebagian besar berbentuk *deterministic*.

Jadi, untuk sebuah kriptosistem selalu ditemukan pasangan berurutan dari suatu kunci (k_e, k_d) yang dihasilkan darl G. Jika kemungkinan terjadi kesalahan dekripsi, misalnya untuk setiap x anggota P, $x = Dk_d(Ek_e(x))$. Sudah barang tentu bukan dikarenakan masalah keamanannya, tetapi kemungkinan salah mengenkrip x itu sendiri. [6]

2.3. Kriptanalisis

Tugas utama kriptografi adalah menjaga agar *Plaintext* maupun kuncinya, atau salah satu atau kedua duanya tetap terjaga kerahasiaanya dari penyadap yang tidak bertanggung jawab. Sedangkan Kriptanalisis (analisis sandi), adalah ilmu untuk mendapatkan *plaintext* tanpa harus mengetahui kuncinya secara wajar [2].

Analisis sandi juga dapat menemukan kelemahan dalam kriptosistem yang dibangun. Usaha analisis sandi dikenal dengan istilah *attack*. Menurut Lars Knudsen la menggolongkan berbagai macam jenis pemecahan algoritma antara lain adalah:

a. *Total Break* yaitu seorang analisis menemukan kunci K, yang digunakan untuk melindungi data-data, schingga $D_k(C) = P$
b. *Global deduction*, yaitu analisis sandi mendapatkan algoritma alternatif A, yang ekivalen dengan $D_k(C)$, tanpa mengetahui K
c. *Instance (local) deduction*, yaitu analisis sandi mendapatkan *plaintext* atau *ciphertext* yang disadap

d. *Information deduction*, yaitu analisis sandi hanya memperoleh beberapa informasi saja mengenai kunci atau *plaintext*.

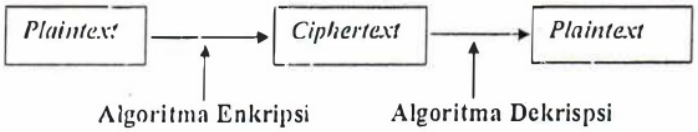
2.4. Algoritma Enkripsi pada Kriptografi

Berdasarkan jenis kuncinya, algoritma kriptografi dibedakan menjadi 2 macam yaitu [2]:

a. **Algoritma Enkripsi simetri (Konvensional):**
Yaitu algoritma yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Algoritma enkripsi ini sering disebut dengan algoritma kunci rahasia, yaitu algoritma dengan satu kunci tertentu yang mengharuskan pengirim dan penerima menyetujui satu kunci tertentu tersebut sebelum mereka dapat berkomunikasi. Jadi keamanan algoritma simetri/konvensional ini tergantung pada satu kunci saja. Yang termasuk dalam kategori algoritma kunci simetri ini antara lain adalah: OTP, DES, RC2, RC4, RC5, RC6, IDEA, Twofish, Magenta, FEAL, SAFER, LOKI, CAST, Rijndael (AES), Blowfish, GOST, A5, Kasumi dan lain sebagainya. Notasi matematis yang biasa digunakan untuk memperjelas dan mempersingkat pernyataan di atas adalah:

$$C = E_k (P) \text{ dan } P = D_k (C)$$

Sedangkan proses dari rangkaian enkripsi dan dekripsi ini dapat digambarkan sebagai berikut:



b. **Algoritma Enkripsi Asimetri (Kunci publik):**
Algoritma ini sering disebut dengan algoritma kunci publik. Kunci yang digunakan untuk Enkripsi berbeda dengan kunci yang digunakan untuk Dekripsi. Kunci Enkripsi dapat diketahui oleh publik artinya sebarang orang bisa menggunakannya untuk mengenkrip pesan, namun hanya orang orang tertentu saja yang dapat melakukan dekripsi terhadap pesan tersebut. Kunci Enkripsi sering disebut dengan Kunci publik, sementara kunci Dekripsi disebut dengan kunci Privat.[20]. Yang termasuk algoritma Asimetri antara lain adalah: ECC, LUC, RSA, El Gamal dan DH.
Notasi matematis yang digunakan untuk menyatakan Enkripsi dengan kunci publik K_e adalah sebagai berikut:
$E_{ke} (M) = C$ sedangkan dengan kunci privat K_d adalah: $D_{kd} (C) = M$ demikian juga sebaliknya: $E_{kd} (M) = C$ dan $D_{ke} (C) = M$ [2].

2.5. Model Kriptografi Konvensional

2.5.1. Model *Cipher* Substitusi

Cipher substitusi ini, dapat dikategorikan menjadi 4 (empat) macam [2], yaitu :

a. ***Monoalfabet*** yaitu setiap karakter *ciphertext* menggantikan satu karakter *plaintext* tertentu.
b. *Polialfabet* : Setiap karakter *ciphertext* dapat menggantikan lebih dari satu macam karakter *plaintext*
c. *Monograf/Unilateral* : Satu enkripsi dilakukan terhadap satu karakter *plaintext*
d. *Polygraf/Multilateral* : Satu enkripsi dilakukan terhadap lebih dari satu karakter *plaintext* sekaligus

2.5.2. Model *Cipher* Transposisi/Permutasi

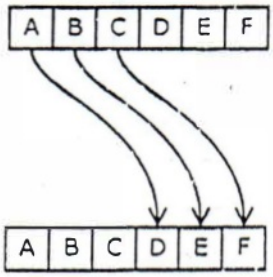
Cipher Transposisi ini bekerja dengan cara mengurutkan kembali huruf namun tidak menyembunyikan kuncinya. *Cipher* transposisi yang biasa dipakai adalah transposisi kolom, dan dikunci dengan suatu kata yang tidak berisi huruf yang sama. Bila kunci yang dipilih ternyata memuat huruf yang sama, maka cukup diambil satu saja, kemudian dilanjutkan dengan mencari huruf yang berbeda dari sebelumnya [5].

2.5.3. Beberapa cipher Konvensional

Cipher-cipher konvensional yang ditulis di bawah ini diambil dari [7], *Chapter* 2 tentang "*Classical Cryptography*" yang berkaitan erat dengan penyandian konvensional "Sukmez" yang akan penulis buat antara lain adalah:

a. ***cipher*** **yang paling tua yaitu *cipher Caesar*.**

Pada metode ini a disamarkan dengan D, b disamarkan dengan E, c disamarkan dengan F dan seterusnya sampai z disamarkan menjadi C, yaitu dengan cara menggeser huruf aslinya ke 3 pergeseran huruf berikutnya. Seperti tabel di bawah ini:



Gambar 2.2: Model Caesar cipher

b. ***Cipher* Transposisi**

Untuk memahami cipher transposisi ini, diberikan contoh dengan kunci: MEGABUCK penggunaan kunci ini ditujukan untuk memberikan nomor kolom. Kolom satu diisi dengan kunci terdekat dengan awal alfabet. *Plaintext* ditulis secara horizontal dan *ciphertext* nya dibaca berdasarkan kolom yang diawali dengan kolom terkecil. Contoh penerapan chiper transposisi ini dapat dilihat pada tabel di bawah :

a. Misalkan *plaintext* bertuliskan: "Mohon segera kirim senjata sesuai pesanan".
b. Proses pembuatan *ciphertext*-nya seperti berikut:

M	E	G	A	B	U	C	K
7	4	5	1	2	8	3	6
M	o	h	o	n	s	e	g
e	r	a	k	i	r	i	m
s	e	n	j	a	t	a	s

c	s	u	a	i	p	e	s
n	n	n	n	x	x	x	x

c. Ciphertext-nya akan berubah bentuk dan susunannya menjadi:
okjanniaixeiaexoresnhanuagmssxmesea

c. Model *Cipher* sandi *Hill*

Menurut Rinaldi munir dalam bukunya yang berjudul Buku Teks Ilmu Komputer "Matematika Diskrit" [8], berdasarkan pada transformasi matriks. Matriks yang digunakan ini disebut dengan sandi *Hill* yang diambil dari nama penemunya yaitu Lester S. Hill yang memperkenalkannya dalam dua makalah yaitu *"Cryptography in an Algebraic Alphabet"* dan *"Concerning Certain Linear Transformation Apparatus of Cryptography"*. Dalam pembahasan sandi *Hill* ini di asumsikan bahwa masing masing huruf dari teks biasa dan teks sandi kecuali Z diberi nilai nol, yaitu nilai numerik yang merinci posisinya dalam abjad baku, seperti terlihat dalam tabel di bawah ini:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
1	2	3	4	5	6	7	8	9	10	11	12	13	14	15

P	Q	R	S	T	U	V	W	X	Y	Z
16	17	18	19	20	21	22	23	24	25	0

Dalam sandi *Hill* yang paling sederhana, pasangan teks biasa yang beruntun ditransformasikan ke teks sandi dengan prosedur sebagai berikut [7]:

Contoh:
Gunakan matriks $\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix}$ sebagai sandi dua Hill untuk menyandikan kata berikut:

" HITUNGLAH "

Jawab:
Jika teks biasa ini dikelompokkan kedalam pasangan pasangan dan menambahkan hûruf boneka 'H' untuk melengkapi pasangan yang terakhir,maka kita peroleh:

H	I	T	U	N	G	L	A	H	H	yang setara dengan:
8	9	20	21	14	7	12	1	8	8	

Untuk menyandikan pasangan tersebut kita bentuk hasil kali matriks:

$$\begin{pmatrix} 1 & 2 \\ 0 & 3 \end{pmatrix} \begin{pmatrix} 8 \\ 9 \end{pmatrix} = \begin{pmatrix} 26 \\ 27 \end{pmatrix}$$

Dilanjutkan hitungan perkalian matriks ini untuk semua pasangan nilai nilai lainnya. Sehingga diperoleh pasangan sebagai berikut:(26,27), (62, 61), (23, 21), (4, 3) dan (24, 24). Jika terdapat bilangan bilangan yang lebih besar dari 26, maka untuk mendapatkan bilangan yang setara dibuatkan kesepakatan yang disebut dengan bilangan modulo 26. Jika terdapat bilangan yang

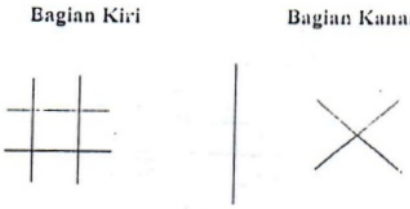
lebih besar dari 25, maka akan digantikan dengan sisa yang dihasilkan jika bilangan ini dibagi 26". Sehingga didapatkan pasangan angka sbb: (0, 1), (0,9), (2, 21), (4,3) dan (24, 24)
Jadi masing masing huruf di atas mempunyai padanan yang bisa dikirim sebagai untaian tunggal yang disebut sebagai chipertext sebagai berikut: *ZAJIBUNCXX* Δ

Karena *Plaintext* dikelompokkan dalam pasangan yang disandikan dengan matriks 2x2, maka disebut sebagai sandi-2 *Hill*. Jika *plaintext* dikelompokkan ke dalam matriks 3x3, maka disebut sebagai sandi-3 *Hill*, demikian seterusnya sampai sandi-n *Hill* yang menggunakan matriks nxn dengan elemen elemennya terdiri dari bilangan bulat.
Selain itu masih ada beberapa macam sandi konvensional yang sudah ada antara lain adalah: **Bifid cipher dan Trifid Cipher, Polyalphabetic cipher dan Sistem Playfair**

3. REKAYASA PENYANDIAN "SUKMEZ"

3.1. Notasi Sandi "sukmez"

Sandi "Sukmez" termasuk dalam sandi simetri Konvensional monoalfabetik, dimana setiap satu huruf digantikan dengan satu simbol lain yang sepadan dengannya. Untuk mengenal simbol-simbol tersebut, yang perlu diperhatikan adalah perancangan/design berikut:



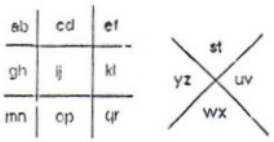
Simbol sandi "Sukmez" terdiri dari 2 bagian, yaitu bagian kiri dan bagian kanan, seperti yang tampak dalam gambar 3.1 di atas. Bagian kiri yaitu bagian yang berbentuk kotak-kotak dan variasinya, sedangkan bagian kanan berupa bagian potongan segitiga dan variasinya. Diagram simbol di bawah ini mewakili sandi dasar "Sukmez". Untuk menggantikan sandi angka yaitu: : 0, 1, 2, 3, 4, 5, 6, 7, 8, 9 seperti terlihat di gambar 3.2 berikut:

1	2	3
4	5	6
7	8	9

Sehingga untuk menyandikan bentuk angka 0 s/d 9 disandikan seperti berikut:

0	1	2	3	4	5	6	7	8	9
•	⌟	⊔	⌞	⊐	⊏	⊏	¬	⊓	⌜

dan bagian lain untuk menyandikan huruf kecil berikutnya adalah:



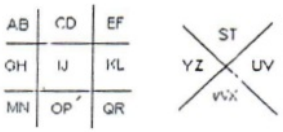
Bagian kiri dipergunakan untuk mewakili pasangan huruf-huruf alfabet dari (a...r): ab, cd, ef, gh, ij, kl, mn, op dan qr. Sedangkan bagian kanan untuk mewakili pasangan huruf-huruf alfabet dari (s....z): st, uv, wx, yz, baik huruf besar/balok maupun huruf kecil.

Penulisan simbol-simbol yang dimaksud seperti di bawah ini:

untuk menyandikan huruf kecil dari a sampai dengan z disandikan seperti tabel 3.2 berikut:

No.	Huruf	Simbol "Sukmez"	No	Huruf	Simbol "Sukmez"
1	a		14	n	
2	b		15	o	
3	c		16	p	
4	d		17	q	
5	e		18	r	
6	f		19	s	
7	g		20	t	
8	h		21	u	
9	i		22	v	
10	j		23	w	
11	k		24	x	
12	l		25	y	
13	m		26	z	

Sedangkan untuk menyandikan huruf besar/Balok A sampai dengan Z disandikan seperti gambar 3.4 berikut:



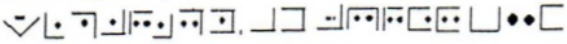
No	Huruf Balok	Simbo Sukmez	No	Huruf Balok	Simbol Sukmez
1	A		14	N	
2	B		15	O	
3	C		16	P	
4	D		17	Q	
5	E		18	R	
6	F		19	S	
7	G		20	T	
8	H		21	U	
9	I		22	V	
10	J		23	W	
11	K		24	X	
12	L		25	Y	
13	M		26	Z	

3.2. Penerapan sandi dasar

Yang dimaksud dengan Penerapan sandi dasar "Sukmez" ini adalah membuat suatu *ciphertext* dari suatu *plaintext* yang sudah ditentukan, tetapi sama sekali belum menggunakan kunci enkripsi maupun kunci dekripsi. Karena sifatnya masih berupa perpindahan dari naskah asli kenaskah yang tersandikan, tetapi belum terkunci, maka disebut sebagai sandi dasar.

Misalkan akan dituliskan suatu kalimat sederhana:

Plaintext : "Semarang, 14 April 2006" maka akan diperoleh

Ciphertext : 

3.3. Aturan Ketentuan Umum

Kunci penyandian "Sukmez" ini bisa diubah-ubah sesuai dengan kehendak. Tetapi kebebasan pemilihan kunci ini harus mengikuti beberapa aturan di bawah ini:

a. Untuk bagian kiri perubahan kunci mengikuti aturan pergeseran kekanan untuk enkripsi dan kekiri untuk dekripsi
b. Perubahan bisa terjadi karena pergeseran sebesar bilangan bulat, atau bisa juga pergeseran sebesar sepasang bilangan pecahan (1/2).

c. Sedangkan untuk bagian kanan, perubahan kunci mengikuti aturan berputar sesuai dengan arah putaran jarum jam untuk enkripsi dan berlawanan dengan arah jarum jam untuk dekripsi.
d. Perubahan karena perputaran juga bisa terjadi karena berputar sebesar bilangan bulat, atau sepasang bilangan pecahan (1/2).
e. Perubahan bagian kiri mengikuti pergeseran bilangan jam sembilanan (0,1,2,.....,8) yang dikenal dengan bilangan modulo 9.
f. Perubahan bagian kanan mengikuti perputaran bilangan Jam empatan (0,1, 2, 3) yang dikenal dengan bilangan modulo 4
g. Merumuskan sandi harus melihat posisi hurufnya. Jika huruf yang akan dipindahkan berada diposisi pertama, maka tidak boleh merumuskan lagi untuk posisi pertama bagian berikutnya yang sama.
h. Perubahan kunci secara umum dibedakan menjadi :
   - Perubahan bagian kiri saja dengan perubahan sebesar bilangan bulat
   - Perubahan bagian kiri saja dengan perubahan sebesar sepasang bilangan pecah =1/2
   - Perubahan bagian kanan saja dengan perubahan sebesar bilangan bulat
   - Perubahan bagian kanan saja dengan perubahan sebesar sepasang bilangan pecah = 1/2
   - Perubahan kombinasi kanan dan kiri secara bersama-sama baik bergeser sebesar bilangan bulat, maupun sepasang bilangan pecah=1/2
i. Khusus untuk angka dalam pembahasan ini tidak disandikan
j. Simbol yang bisa disisipkan sebagai alat bantu adalah bagian-bagian dari potongan diagram di atas, misalnya: . , + , x, - dan lain sebagainya

3.4. Algoritma Pembuatan Kunci

3.4.1. Algoritma Enkripsi Penyandian "Sukmez"

Langkah 1:

Menentukan cukup satu pilihan dari beberapa macam variasi pilihan nilai **a, b, s** dan **t** di bawah ini sebagai wakil kunci enkripsi penyandian konvensional **"Sukmez" sebagai berikut:**

a. Perubahan bagian kiri dengan satu huruf saja yang mengalami pergeseran sebesar pergeseran bilangan bulat dan bagian kanan tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: a = a + k , dengan a adalah variabel yang bisa menggantikan salah satu huruf alfabet yaitu:
   a = a, c, e, g, ...o, q dan (k = 1,2,.....,8).
b. Perubahan Bagian kiri saja, tetapi ada dua huruf yang berubah dengan pergeseran masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan tetap tidak berubah. Secara matematis dapat dirumuskan: a = a + x dan b = b + y di mana a bisa menggantikan huruf-huruf yang terletak diposisi pertama seperti a= a,c,e,g,i,k,m,o,q dan b menggantikan huruf-huruf yang berada pada posisi ke dua b= b,d,f,h,j,l,n,p,r dan (x,y =1,2.....,8) x dan y boleh sama, boleh berbeda.
c. Perubahan bagian kiri saja. Tetapi ada dua huruf yang berubah dengan perubahan pergeseran sebesar sepasang pergeseran bilangan pecahan (1/2), sedangkan bagian kanan tetap tidak berubah. Perumusannya secara matematis dinyatakan sebagai berikut: a= a + (x+1/2), b=b+(y+1/2) dengan a menggantikan huruf-huruf pada posisi pertama a = a,c,e,g,i,k,m,o,q dan b menggantikan huruf-huruf yang berada pada posisi ke dua b= b,d,f,h,j,l,n,p,r dan (x,y=1,2,....,8), dengan x dan y boleh sama boleh berbeda.
d. Perubahan bagian kanan saja dengan satu huruf saja yang mengalami pergeseran sebesar pergeseran bilangan bulat dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: s = s + k , dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet s = s, u, w, y dan (k = 1, 2, 3).

e. Perubahan bagian kanan saja tetapi ada dua huruf yang mengalami pergeseran sebesar pergeseran bilangan bulat dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: $s = s + m$, dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi pertama s = s, u, w, y dan (m= 1, 2, 3) dan t= t+n, dengan t adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi ke dua t=t, v, x, z dan (n= 1, 2, 3).

f. Perubahan bagian kanan saja tetapi ada dua huruf yang mengalami pergeseran sebesar pergeseran sepasang bilangan pecah=1/2 dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: $s=s+(m+1/2)$, dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi pertama s = s, u, w, y dan (m= 1, 2, 3) dan $t=t+(n+1/2)$,
dengan t adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi ke dua t=t, v, x, z dan (n= 1, 2, 3).

g. Perubahan Kombinasi bagian kiri dan kanan, di mana bagian kiri ada dua buah huruf yang berubah dengan perubahan masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan hanya ada satu huruf yang berubah dengan perubahan sebesar perputaran bilangan bulat, dengan rumusan: $a=a+x_1$, $b=b+x_2$, $s=s+x_3$ dimana a dan b menggantikan posisi huruf pertama dan kedua pada bagian kiri sedangkan s menggantikan salah satu huruf yang ada di posisi kiri dari bagian kanan s=s, u, w, z sedangkan (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3=1,2,3).

h. Perubahan Kombinasi bagian kiri dan kanan, dimana bagian kiri ada dua buah huruf yang berubah dengan perubahan masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan juga ada dua buah huruf yang berubah dengan perubahan sebesar perputaran bilangan bulat, dengan rumusan: $a=a+x_1$, $b=b+x_2$, $s=s+x_3$, $t=t+x_4$, di mana a dan b menggantikan posisi huruf pertama dan kedua pada bagian kiri sedangkan s dan t masing-masing menggantikan satu huruf yang ada di posisi pertama dan kedua dari bagian kanan s=s, u, w, z dan t=t, v, x, z sedangkan (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3, x_4 =1,2,3).

i. Perubahan Kombinasi bagian kiri dan kanan, di mana bagian kiri ada dua buah huruf yang berubah dengan masing-masing huruf berubah sebesar pergeseran bilangan pecah (1/2), sedangkan bagian kanan ada dua buah huruf yang berubah dengan perubahan masing-masing huruf juga bergeser sebesar bilangan pecah (1/2), maka rumusan matematisnya adalah: $a=a+(x_1+1/2)$, $b=b+(x_2+1/2)$, $s=s+(x_3+1/2)$ dan $t=t+(x_4+1/2)$ dimana (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3,x_4=1,2,3) x_3 dan x_4 boleh sama boleh berbeda.

Langkah 2:
Menemukan tepat satu pasangan perubahan huruf yang sesuai dengan pilihan kunci tersebut, yaitu dengan cara menggambarkan kerangka posisi huruf dasarnya ke perubahan posisi kunci huruf-huruf barunya.

Langkah 3:
Menemukan ciphertext yang sesuai dengan pergantian perubahan masing-masing hurufnya

Langkah 4:
Menemukan masing-masing huruf sandi "Sukmez" sebagai pengganti masing-masing huruf alfabet aslinya

Langkah 5:
Merangkai huruf sandi hasil penemuan langkah 4 sampai menjadi satu kalimat yang sesuai dengan aslinya.

3.4.2. Algoritma Dekripsi penyandian "Sukmez"

Langkah 1:

Menentukan cukup satu nilai a, b, s dan t sebagai wakil kunci Dekripsi penyandian konvensional "Sukmez" dengan berbagai variasi pemilihan sebagai berikut:

a. Perubahan bagian kiri dengan satu huruf saja yang mengalami pergeseran sebesar pergeseran bilangan bulat dan bagian kanan tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: $a = a - k$, dengan a adalah variabel yang bisa menggantikan salah satu huruf alfabet a = a,b,c,.....o,p,q,r dan (k = 1,2,.....,8).

b. Perubahan Bagian kiri saja, tetapi ada dua huruf yang berubah dengan pergeseran masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan tetap tidak berubah. Secara matematis dapat dirumuskan: $a = a - x$ dan $b = b - y$ dimana a bisa menggantikan huruf-huruf yang terletak diposisi pertama seperti a= a,c,e,g,i,k,m,o,q dan b menggantikan huruf-huruf yang berada pada posisi ke dua b= b,d,f,h,j,l,n,p,r dan (x,y =1,2,.....,8) x dan y boleh sama, boleh berbeda.

c. Perubahan bagian kiri saja. Tetapi ada dua huruf yang berubah dengan perubahan pergeseran sebesar sepasang pergeseran bilangan pecahan (1/2), sedangkan bagian kanan tetap tidak berubah. Perumusannya secara matematis dinyatakan sebagai berikut: a= a-(x-1/2), b=b-(y-1/2) dengan a menggantikan huruf-huruf pada posisi pertama a = a,c,e,g,i,k,m,o,q dan b menggantikan huruf-huruf yang berada pada posisi ke dua b= b,d,f,h,j,l,n,p,r dan (x,y=1,2,....,8), dengan x dan y boleh sama boleh berbeda.

d. Perubahan bagian kanan saja dengan satu huruf saja yang mengalami pergeseran sebesar pergeseran bilangan bulat dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: $s = s - k$, dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet s = s, u, w, y dan (k = 1, 2, 3).

e. Perubahan bagian kanan saja tetapi ada dua huruf yang mengalami perputaran sebesar perputaran bilangan bulat dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: s=s-m , dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi pertama s = s, u, w, y dan (m= 1, 2, 3) dan t= t-n, dengan t adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi ke dua t=t, v, x, z dan (n= 1, 2, 3).

f. Perubahan bagian kanan saja tetapi ada dua huruf yang mengalami perputaran sebesar perputaran sepasang bilangan pecah=1/2 dan bagian kiri tetap tidak berubah. Secara matematis dapat dirumuskan seperti berikut: s=s-(m-1/2) , dengan s adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi pertama s = s, u, w, y dan (m= 1, 2, 3) dan t=t-(n-1/2), dengan t adalah variabel yang bisa menggantikan salah satu huruf alfabet posisi ke dua t=t, v, x, z dan (n= 1, 2, 3).

g. Perubahan Kombinasi bagian kiri dan kanan, di mana bagian kiri ada dua buah huruf yang berubah dengan perubahan masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan hanya ada satu huruf yang berubah dengan perubahan sebesar perputaran bilangan bulat, dengan rumusan: $a=a-x_1$, $b=b-x_2$, $s=s-x_3$, dimana a dan b menggantikan posisi huruf pertama dan kedua pada bagian kiri sedangkan s menggantikan salah satu huruf yang ada di posisi kiri dari bagian kanan s=s, u, w, z sedangkan (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3=1,2,3).

h. Perubahan Kombinasi bagian kiri dan kanan, di mana bagian kiri ada dua buah huruf yang berubah dengan perubahan masing-masing sebesar pergeseran bilangan bulat, sedangkan bagian kanan juga ada dua buah huruf yang berubah dengan perubahan sebesar perputaran bilangan bulat, dengan rumusan: $a=a-x_1$, $b=b-x_2$, $s=s-x_3$, $t=t-x_4$, di mana a dan b menggantikan posisi huruf pertama dan kedua pada bagian kiri sedangkan s dan t masing-masing menggantikan

satu huruf yang ada di posisi pertama dan kedua dari bagian kanan s=s, u, w, z dan t= t, v, x, z sedangkan (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3, x_4 =1,2,3).

i. Perubahan Kombinasi bagian kiri dan kanan, di mana bagian kiri ada dua buah huruf yang berubah dengan masing-masing huruf berubah sebesar pergeseran bilangan pecah (1/2), sedangkan bagian kanan ada dua buah huruf yang berubah dengan perubahan masing-masing huruf juga bergeser sebesar bilangan pecah (1/2), maka rumusan matematisnya adalah: a=a-(x_1.1/2), b=b-(x_2.1/2), s=s-(x_3-1/2) dan t=t-(x_4.1/2) dimana (x_1,x_2 =1,2,....8) dengan x_1 dan x_2 boleh sama boleh berbeda dan (x_3,x_4=1,2,3) x_3 dan x_4 boleh sama boleh berbeda.

Langkah 2:
Menemukan tepat satu pasangan perubahan huruf yang sesuai dengan pilihan kunci tersebut, yaitu dengan cara menggambarkan kerangka posisi huruf dasarnya ke perubahan posisi kunci huruf-huruf barunya.

Langkah 3:
Menemukan *Plaintext* yang sesuai dengan pergantian perubahan masing-masing hurufnya.

Langkah 4:
Menemukan masing-masing huruf sandi "Sukmez" sebagai pengganti masing-masing huruf alfabet aslinya

Langkah 5:
Merangkai huruf sandi hasil penentuan langkah 4 sampai menjadi satu kalimat yang sesuai dengan aslinya.

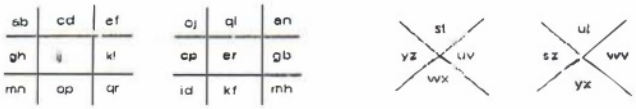
3.4.3. Contoh Penyandian

3.4.3.1. Contoh 1

Perubahan kunci ini, terjadi karena perubahan bagian kiri dan perubahan bagian kanan secara serentak bersama sama, sejauh bilangan bulat saja.

Langkah 1:
Misalkan kunci perubahan yang dikehendaki adalah sebagai berikut:
a = a + 2, b = b + 5, s = s + 3, maka:

Langkah 2:
Menemukan perubahan dari sandi dasar ke perubahan baru yang ditentukan dari rumusan di atas, untuk bagian kiri dan kanan akan berubah seperti:



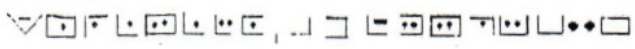
Langkah 3:

Menemukan perubahan penyandiannya akan terlihat seperti berikut:ab, cd, ef, gh, ij, kl, mn, op, qr berubah menjadi aj, ql, an, ep, er, gb, kl, kf, mn, sedangkan bagian kanan st, uv, wx, yz, berubah menjadi ut, wv, yx, sz

Langkah 4 dan 5:

Plaintext : "Semarang, 14 April 2006", berubah menjadi:

Ciphertext :



3.4.3.2. Contoh 2

Perubahan yang terjadi misalnya: $a=a+(x_1+1/2)$, $b=b+(x_2+1/2)$, $s=s+(x_3+1/2)$ dan $t=t+(x_4+1/2)$ di mana $(x_1,x_2 = 1,2,\ldots.8)$ dengan x_1 dan x_2 boleh sama boleh berbeda dan $(x_3,x_4=1,2,\ldots4)$, di mana x_3 dan x_4 boleh sama boleh berbeda.

Langkah 1:

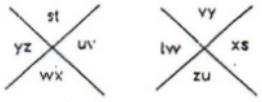
Misalkan dikehendaki **a=a+51/2, b=b+41/2, s=c+11/2** dan **t=t+21/2.**

Langkah 2:

Maka perubahan pasangan sandinya adalah sebagai berikut:

ab	cd	ef
gh	ij	kl
mn	op	qr

ji	lk	nm
po	rq	ba
dc	fe	hg



Langkah 3:

Pasangan perubahan kunci ab, cd, ef, gh, ij, kl, mn, op, qr berubah menjadi ji, lk, nm, po, rq, ba, dc, fe, hg, sedangkan st, uv, wx, yz berubah menjadi vy, xs, zu, dan tw.

Langkah 4 dan 5:

Digabungkan sehingga perubahan ciphertextnya bisa dilihat di bawah ini:

Plaintext : Semarang, 14 April 2006

Ciphertextnya :

3.5. Perbandingan sandi Konvensional "Sukmez" dengan sandi Konvensional yang ada sebelumnya.

Dari beberapa macam kelemahan dan kekurangan sandi-sandi konvensional yang sudah ada, maka secara garis besar dapat dituliskan dan dapat dipertimbangkan dalam tabel di bawah ini:

Nama Sandi	Substitusi	Transposisi	Huruf besar/ kecil	angka	Kombinasi	Huruf Boneka	Tanda Baca
Caesar	*	-	=	-	-	-	-
Transposisi	-	*	=	-	-	*	-
Hill Cipher	-	*	*	-	-	*	-
Bifid Cipher	-	*	-	-	*	*	-
Trifid Cipher	-	*	=	-	*	*	-
Poly alphabetic	*	-	=	-	*	*	-
Playfair	*	-	=	-	-	*	-
"Sukmez"	*	*	≠	*	*	-	=

Keterangan:

* = ya, - = Tidak,

3.5.1. Kelebihan Sandi "Sukmez"

Berdasarkan tabel yang ada, dan contoh-contoh yang sudah diberikan di atas, maka sandi "Sukmez" mempunyai beberapa kelebihan jika dibandingkan dengan sandi-sandi konvensional sebelumnya.

Adapun beberapa kelebihan yang dimaksud antara lain adalah:

a. Bisa menyandikan angka
b. Bisa membedakan antara sandi dengan huruf besar dan sandi dengan huruf kecil
c. Merupakan sandi kombinasi, yaitu gabungan dari substitusi dan Transposisi
d. Setiap kata pada *plaintext* digantikan dengan tepat satu kata pula di dalam *ciphertext* karena termasuk Monoalfabetik
e. Bisa digunakan untuk kalimat yang panjang bahkan satu file teks.
f. Tidak memerlukan huruf boneka
g. Tidak harus mengelompokkan dalam satu kelompok khusus, karena satu huruf digantikan dengan satu kode lain dalam sandinya
h. Kunci bisa diubah ubah dengan aneka macam :model yang sangat kompleks, variatif, unik dan menarik sesuai dengan yang dikehendaki oleh pembuat sandi.
i. Kuncinya tidak mudah ditemukan oleh *hacker*, *cracker* dan *Attacker* karena kemungkinan permutasi perbedaan kuncinya lebih dari :
$(10^1 \cup 10^2 \cup 10^3 \cup 10^4 \cup 10^5 \cup 10^6 \cup 10^7 \cup 10^8 \cup 10^9 \cup 10^{10})^4$
atau sekitar $(11*10^9)^4 = 11^4 * 10^{36}$

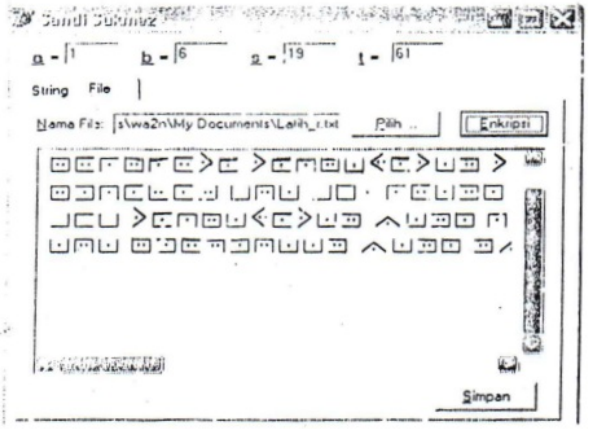
3.5.2. Kekurangan Sandi "Sukmez"

a. Karena termasuk penyandian konvensional, maka untuk proses On line masih perlu pemikiran lebih lanjut.
b. Karena termasuk penyandian Monoalphabetic, maka idealnya harus bisa menggantikan keseluruhan huruf/symbol yang ada dalam ASCII

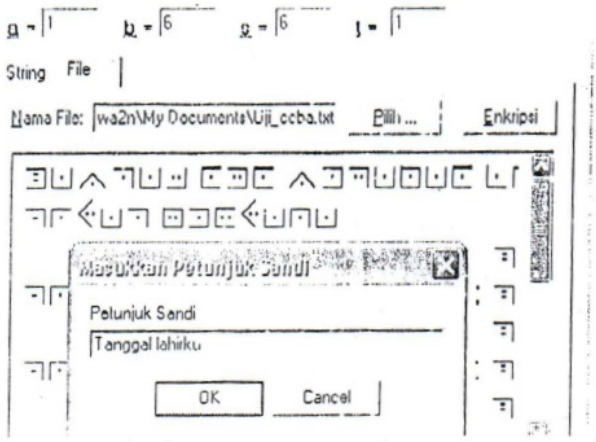
c. Sementara ini baru bisa digunakan khusus untuk file teks, sementara untuk file non teks yang bersifat kompleks belum bisa digunakan
d. Untuk file non teks jika ingin disandikan harus ditransfer terlebih dahulu kedalam file teks
e. Ukuran fontnya menjadi lebih besar dari pada ukuran font file yang lain.

4. Implementasi

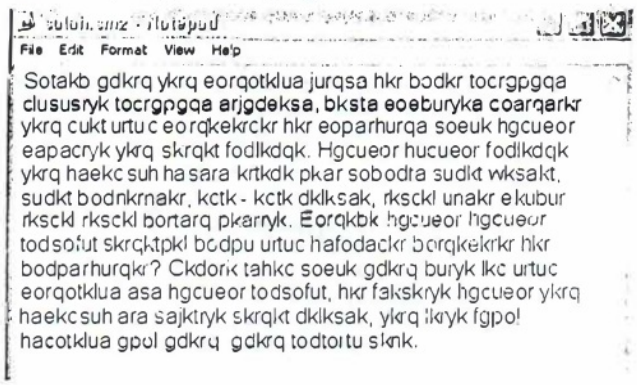
4.1. Mengenkrip file teks



4.2. Mendekripsi file teks



4.3. Mendekrip dengan kunci yang salah



5. Kesimpulan

Dengan memanfaatkan *"The Font Creator Program"* dan proses *editing Font Arial* dalam membuat simbol-simbol penyandian konvensional "Sukmez", kemudian menggabungkannya dengan pemrograman Borland Delphi, serta hasil pengujian yang diperoleh, maka tentang penyandian konvensional "Sukmez" dapat disimpulkan sebagai berikut:

a. Termasuk sandi konvensional yang baru ditemukan dan baru diterapkan
b. Bisa menyandikan angka
c. Bisa digunakan untuk menyandikan satu file teks yang panjang.
d. Kunci enkripsi dan dekripsinya sangat banyak, unik dan variatif
e. Kuncinya tidak mudah untuk ditemukan
f. Tidak memerlukan huruf boneka
g. Sandi "Sukmez" bisa bersaing dengan sandi konvensional yang lainnya

5.1. Saran

Selain adanya beberapa kelebihan dalam kesimpulan, maka ada pula beberapa saran yang perlu dipertimbangkan untuk pengembangan penyandian konvensional "Sukmez" selanjutnya antara lain adalah:

1. Sandi "Sukmez" masih bisa dikembangkan lagi dengan tambahan notasi/simbol baru, yang terkait dengan potongan simbol yang sudah ada.
2. Angka sebenarnya juga bisa disandikan sesuai dengan kesepakatan
3. Program yang digunakan bisa menggunakan bahasa pemrograman yang lain, selain dengan pemrograman Borland Delphi.
4. Karena termasuk sandi konvensional yang tergolong masih baru, maka perlu pengenalan awal dalam penerapan sandi"Sukmez"

6. Daftar Pustaka

[1] Sasa Rudan, Dipl.Ing, Aleksandra Kovacevic, Dipl.Ing, Charles Milligan, PhD, Veljko Milutinovic, Phd, *"Data Assurance in a Conventional File System"* Proceedings of the 38th Hawaii International Conference on System Science – 2005 , 0-7695-2268-8/05/$20.00 (C) 2005 IEEE.

[2] Yusuf Kurniawan Ir,MT, *Kriptografi Keamanan Internet dan Jaringan Komunikasi*, Informatika Bandung 2004

[3] Bart Preneel,Vincent Rijmen and Antoon Bosselaers: ***"Recent Developments in the Design of Conventional Cryptographic Algorithms"***, Journal, Vol 28, No 4, 18 September 2003

[4] Onno W Purbo dan Tony Wiharjito, *Keamanan Jaringan Internet*, PT Elex Media Komputindo, Jakarta 2000

[5] Andrew S. Tanenbaum, *Jaringan Komputer* Edisi Bahasa Indonesia Jilid 2, Prenhallindo, Jakarta 1997

[6] Ivan Damgard, ***"Definitions and results for Cryptosystems"*** Ivan Damgard October 12, 2004

[7] Wikipedia Information: *"Classical cryptography "* ,Ciphers: ADFGVX | Affine | Atbash | Autokey | Bifid | Book | Caesar | Four-square | Hill | Permutation | Pigpen | Playfair | Polyalphabetic | Reihenschieber | Running key | Substitution | Transposition | Trifid | Two-square | Vigenère Wikipedia Information Answer.com, Copyright © 2006Douglas R.Stinson "Cryptography:Theory and practice" di update Jan 2006 http://www.maths.uwa.edu.au/~praeger/teaching/3CC/WWW/chapter2.html

[8] Rinaldi Munir Ir,MT, *Buku teks ilmu Komputer Matematika Diskrit*, cetakan ke II, CV Informatika Bandung 2003

[9] Insap Santosa P, Ir, MSc, *Interaksi Manusia dan Komputer* Teori dan Praktek, Andi Offset, Yogyakarta 1997

[10] Alan Dik, Janet finlay, Gregory Abowd, Russel Beale: ***"Human Computer Interaction"***, Prentice Hall, 1997

[11] Budi Rahardjo. *Keamanan Sistem Informasi Berbasis Internet*, http://budi.insan.co.id diupdate Agustus 2003

[12] Cheryl E.Praeger : *"Classical cryptography"*, file translated from TEX by TTH, version 3, on Sat Oct 27 09:46:31, 2001,

[13] Primeink *"Conventional Cryptography"*, e-Security Tools for Professional Application Development, , www.Cryptomathic.com 2000

[14] Deborah J.Mayhew ***"Principles and Guidelines in Software User Interface Design"***, PTR Prentice-Hall,Inc. 1992

[15] Mel, H.X. Baker, D. ***"Cryptography Decrypted"***. Addison Wesley, 2001

[16] Scneier, B.: ***" Applied Cryptography "*** , New York: Wiley, 1996

[17] Stallings, W. ***" Cryptography and Network Security"*** : Principles and Practice, 2nd edition. Prentice Hall, 1999

[18] Vaudenay, S: ***"A Classical Introduction to Cryptography Applications"*** Security, 2005, XVIII,342 p,149 illus.,Hardcover', http://www.springer.com/0-387-25464-1

[19] Douglas R.Stinson, *"Cryptography Theory and practice"* di update Jan 2006 http://www.maths.uwa.edu.au/~praeger/teaching/3CC/WWW/chapter2.html

[20] Neal R. Wagner, ***"The Laws of Cryptography: Conventional Block Ciphers"***, Copyright© 2002 by Neal R.Wagner. All rights reserved.

Nas_Jurnal #21 Rekayasa Penyandian Konvensional “SUKMEZ”

ORIGINALITY REPORT

2%	2%	0%	1%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	es.scribd.com Internet Source	1%
2	faajihouse.com Internet Source	<1%
3	repositori.uin-alauddin.ac.id Internet Source	<1%

Exclude quotes	Off	Exclude matches	< 5 words
Exclude bibliography	On		