PENYANDIAN DATA TEKS MENGGUNAKAN ALGORITMA *CIPHER FEED-BACK* DAN *CHAOTIC SKEW TENT MAP*

Anita M. Sonbay [1], Adriana Fanggidae [2], Kornelis Letelay [3]
[1,2,3] Jurusan Ilmu Komputer, Fakultas Sains dan Teknik, Universitas Nusa Cendana

INTISARI

Keamanan dokumen yang berisi teks rahasia dan penting bagi sebuah perusahaan, institusi, atau organisasi dari gangguan pihak yang tidak bertanggung jawab adalah sebuah keharusan atau kebutuhan utama yang wajib dilakukan, sehingga diperlukan suatu perangkat lunak yang dapat melindungi dokumen–dokumen penting tersebut. Kombinasi dari algoritma *Chiper Feed-back* (CFB), *Chaotic Skew Tent Map* (CSTM), dan teknik pembangkitan nilai awal dengan *Session Keys* mampu mengenkripsi teks dengan baik. Pengujian dilakukan terhadap 26 *file* doc, docx dan txt dimana tiap pengujian akan dianalisis korelasi, standar deviasi dan variansi, serta histogram. Pengujian dilakukan untuk *file* doc, docx, dan txt dengan ukuran ≤ 35 kb, 30-60 kb, 61-80 kb dan > 80 kb. Hasil pengujian diperoleh nilai rata-rata korelasi = 0,163326411, standar deviasi = 1.068,070, variansi = 1.550.358,492, dan histogram *ciphertext* yang secara visual terlihat seragam, sehingga mempersulit analisis statistik untuk menganalisis karakter atau kunci.

Kata kunci: enkripsi teks, *cipher feed-back, chaotic skew tent map, session keys*

ABSTRACT

Security for documents that contain confidential text and important for a company, institution, or organization from disorders irresponsible organisation is a necessity or a major requirement that must be done, so we need a software that can protect these vital documents. The combination of algorithms Chiper Feed-back (CFB), Chaos Skew Tent Map (CSTM), and the initial value generation techniques with Session Keys capable of encrypting the text properly. Tests conducted on 26 files doc, docx and txt where each test will be analyzed the correlation, standard deviation and variance, as well as the histogram. Testing is done to the file doc, docx, and txt with a size ≤ 35 kb, 30-60 kb, 61-80 kb and > 80 kb. The test results obtained by the value of the average correlation = 0.163326411, standard deviation = 1.068,070, variance = 1.550.358,492, and the ciphertext histogram that visually looks uniform, making it difficult to analyze the statistical analysis of the character or key.

Keywords: text encryption, ciphers feed-back, chaos skew tent map, session keys

I. PENDAHULUAN

Menjaga keamanan dokumen rahasia dan penting bagi sebuah perusahaan, institusi, atau organisasi dari gangguan pihak-pihak yang tidak bertanggung jawab adalah sebuah keharusan/kebutuhan utama atau sesuatu hal yang wajib dilakukan. Saat ini sebagian besar dokumen-dokumen menggunakan aplikasi *microsoft word.* Pengolahan kata pada aplikasi *microsoft word* begitu mudah digunakan, sehingga siapapun yang menggunakannya akan merasa nyaman dengan aplikasi pengolahan kata ini. Penelitian ini bertujuan untuk membantu mengatasi keamanan data pada aplikasi *microsoft word* dan *notepad* dari pencurian dokumen-dokumen baik yang tidak penting maupun yang penting dan rahasia. Oleh karena itu dibutuhkan sebuah metode kriptografi yang akan

ISSN 2337-7631

ISSN 2337-7631

mengenkripsi dan mendekripsikan data. Salah satu metode yang akan digunakan dalam pembuatan perangkat lunak ini adalah metode *Chiper Feed Back* (CFB). Pada mode CFB, data dienkripsikan dalam unit yang lebih kecil daripada ukuran blok, misalnya dienkripsikan satu karakter setiap kalinya (seperti *cipher* aliran) sehingga tidak membutuhkan sinkronisasi *ciphertext*. Algoritma ini juga merupakan salah satu mode operasi pada *cipher* blok yang tidak membutuhkan *padding* pada blok [1]. Namun algoritma ini memiliki kelemahan pada kuncinya dimana setiap blok memiliki kuncinya yang sama, sehingga diperlukan metode pembangkit bilangan acak (*chaotic)* untuk menghasilkan kunci yang berbeda pada setiap bloknya agar tahan terhadap kriptanalis. Penggunaan *chaotic* dalam kriptografi dapat menghasilkan efek *confusion* (menyembunyikan hubungan apapun yang ada pada *plaintext,* kunci, dan *ciphertext.*

II. MATERI DAN METODE

2.1 Data Penelitian

Data yang digunakan dalam penelitian ini adalah teks asli yang diperoleh dari internet, dimana teks ini dimasukan oleh pengguna berupa 18 *file* doc dan docx serta 8 *file* txt dengan ukuran bervariasi mulai dari 24 kb sampai 305 kb.

2.2 Modifikasi Algoritma CFB

Pada mode CFB yang asli, kunci yang digunakan pada setiap blok sama. Oleh karena itu, diusulkan mode CFB dengan menggunakan kunci yang berbeda pada setiap blok. Setiap kunci tersebut diperoleh dari bilangan acak yang dibangkitkan oleh fungsi *chaotic skew tent map* (CSTM).

2.2.1 *Session keys*

Pada bagian ini akan dibahas mengenai langkah-langkah untuk mengubah karakter kunci menjadi nilai numerik yang akan dipakai pada fungsi CSTM. Algoritma yang diusulkan menggunakan panjang kunci 16 karakter desimal atau sebesar 128-bit.

$$K = k_1, k_2, \dots, k_{16} \quad (1)$$

dimana k_1-k_{16} adalah karakter kunci yang digunakan. Langkah-langkah yang digunakan untuk mencari x_0 adalah sebagai berikut:

1) Setiap karakter tersebut dikonversi ke dalam bentuk ASCCI.
$$K = K_1 K_2 \dots k_{16} \quad (2)$$
dimana, K_1 sampai K_{16} mempresentasikan 8-bit biner dari setiap karakter kunci.

2) Potong 16 karkter kunci tersebut masing-masing bagian yakni 4 karakter. Potongan i=$K_1K_2K_3K_4$, potongan ii=$K_5K_6K_7K_8$, potongan iii=$K_9K_{10}K_{11}K_{12}$, potongan iv=$K_{13}K_{14}K_{15}K_{16}$.

3) Mencari x_{01}, x_{02}, x_{03} dan x_{04} manggunakan potongan-potongan tersebut. Berikut disajikan pencarian x_{01} potongan i.
$$\begin{aligned} x_{01} = (&k_{1,1} * 2^0 + k_{1,2} * 2^1 + \dots + k_{1,8} * 2^7 + \\ &k_{2,1} * 2^8 + k_{2,2} * 2^9 + \dots + k_{2,8} * 2^{15} + \\ &k_{3,1} * 2^{16} + k_{3,2} * 2^{17} + \dots + k_{3,8} * 2^{23} + \\ &k_{4,1} * 2^{24} + k_{4,2} * 2^{25} + \dots + k_{4,8} * 2^{31})/2^{32}. \end{aligned}$$
Mencari x_0 menggunakan $x_{01}, x_{02}, x_{03}, x_{04}$ sebagai berikut :
$$x_0 = (x_{01} + x_{02} + x_{03} + x_{04}) \bmod 1 \quad (3)$$

2.2.2 Pembangkitan Kunci

Langkah-langkah pembangkitan kunci dapat dijelaskan sebagai berikut:

1) Penentuan iterasi awal menggunakan fungsi pemotongan:

$$T(x, size) = \|x * 10^{count}\|, x \neq 0 \quad (4)$$

dimana T adalah fungsi dari x dan *size*, $x \in [0,1]$, *size* adalah panjang angka *integer* yang diinginkan dari nilai x sedangkan *count* bernilai 1 dan bertambah 1 sampai $x * 10^{count} > 10^{size-1}$.

2) Membangkitkan bilangan acak kunci menggunakan fungsi CSTM:

$$\mathbf{f}(x_{k+1}) = \begin{cases} \frac{Xk}{a} & if\ 0 \leq x \leq a \\ \frac{1-Xk}{1-a} & if\ a < x \leq 1 \end{cases} \quad (5)$$

dimana $x_k \in [0,1]$, x_0 merupakan nilai kondisi awal dan p merupakan sistem parameter dimana $p \in [0,1]$. Fungsi dari persamaan (4) akan dikatakan *chaos* jika $0 < p < 1$ dan $p \neq 0{,}5$[2].

3) Membangkitkan bilangan acak total pergeseran bit karakter teks menggunakan persamaan (4). Untuk memperoleh bilangan acak pertama, nilai x_0 yang telah diperoleh dimasukkan ke persamaan (4) untuk menghasilkan nilai $CSTM_1$ melalui iterasi awal yang diperoleh dari langkah 1, kemudian nilai $CSTM_1$ tersebut dipotong dengan persamaan (3) dengan *size* yang diinginkan. Untuk memperoleh bilangan acak jumlah pergeseran berikutnya, maka x_0 adalah nilai CSTM kunci kedua dan seterusnya sampai $CSTM_N$.

2.2.3 Enkripsi dan Dekripsi

Bagian ini akan dijelaskan algoritma untuk proses enkripsi dan dekripsi.

1) Algoritma enkripsi

a. Masukan *plaintext*, kunci dan ukuran blok.
b. Bagi blok *plaintext* sesuai dengan ukuran blok dan jumlah karakter *plaintext.*
c. Lakukan fungsi CSTM dan fungsi pemotongan untuk membangkitkan deretan bilangan acak kunci dan total pergeseran.
d. Lakukan operasi CFB dan pergeseran karakter ke kanan sebesar total pergeseran.
e. Hasil enkripsi (*ciphertext*).

2) Algoritma dekripsi

a. Masukan *ciphertext*, kunci dan ukuran blok.
b. Bagi blok *plaintext* sesuai dengan ukuran blok dan jumlah karakter *plaintext*.
c. Lakukan operasi CFB dan pergeseran karakter ke kiri sebesar total pergeseran.
d. Lakukan fungsi CSTM dan fungsi pemotongan untuk membangkitkan deretan bilangan acak kunci dan total pergeseran.
e. Hasil dekripsi (*plaintext*).

2.2.4 Korelasi

Korelasi koefesien merupakan sebuah perhitungan untuk mencari derajat korelasi di antara dua variabel yang menunjukkan teks asli (*plain-text*) dan teks hasil proses (*cipher-text*) Dengan demikian dapat diketahui seberapa besar perbedaan dari setiap karakter *plain-text* dan *cipher-text* yang berdekatan. Kuatnya hubungan antara *plaintext* dan *ciphertext* ditunjukan dengan angka 0 – 1. Angka 0 menunjukan hubungan yang tidak ada dan angka 1 menunjukan hubungan yang sempurna. Untuk penghitungan keofisien korelasi (r_x) berdasarkan sekumpulan data (x,y) berukuran n dapat digunakan rumus[3].

ISSN 2337-7631

$$r_x = \frac{cov\ (x,y)}{\sqrt{D(x)D(y)}} \quad (6)$$

$$cov\ (x,y) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)][y_i - E(y)] \quad (7)$$

$$D(x) = \frac{1}{n}\sum_{i=1}^{n}[x_i - E(x)]^2 \quad (8)$$

$$E(x) = \frac{1}{n}\sum_{i=1}^{n} x_i \quad (9)$$

2.2.5 Standar Deviasi dan Variansi

Standar deviasi merupakan variasi sebaran data, semakin besar nilai sebarannya berarti data semakin bervariasi. Standar deviasi merupakan akar kuadrat positif dari variansi. Jadi jika salah satu nilai dari ukuran tersebut diketahui maka akan diketahui juga nilai ukuran yang lain.

2.2.6 Histogram

Analisis histogram didasarkan pada kenyataan bahwa, dalam setiap peregangan tertentu bahasa tertulis, surat dan kombinasi huruf tertentu terjadi dengan frekuensi yang berbeda-beda[2]. Histogram memperlihatkan distribusi frekuensi karakter pada teks. Kriptanalis menggunakan histogram untuk menganalisis frekuensi kemunculan banyaknya suatu karakter dalam sebuah teks. Agar serangan dengan analisis statistik tidak dimungkinkan, maka penting menghasilkan histogram *ciphertext* yang memiliki distribusi frekuensi seragam dan berbeda dengan histogram *plaintext.*

III. HASIL DAN PEMBAHASAN

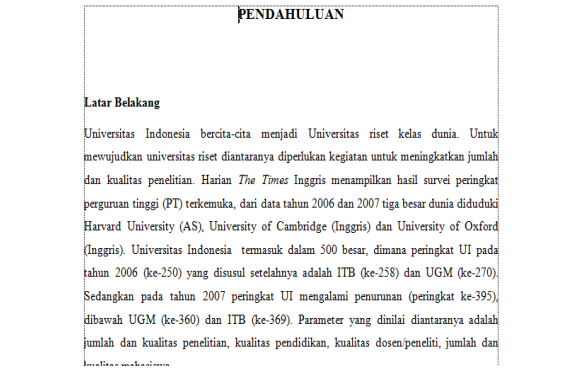
Algoritma yang diusulkan ini disimulasikan pada *file* uji yaitu 18 *file* doc, docx dan 8 *file* txt, dengan 4 macam pengujian.

3.1 Hasil

Hasil yang diperoleh terdiri dari hasil proses enkripsi dan proses dekripsi yang diuji berdasarkan 4 pengujian yakni: (i) pengujian 1 (ukuran *file* ≤ 35kb dan ukuran *file* mod blok = 0), (ii) pengujian 2 (ukuran *file* 36kb – 60kb dan ukuran *file* mod blok = 0), (iii) pengujian 3 (ukuran *file* 61kb – 80kb dan ukuran *file* mod blok ≠ 0) dan (iv) pengujian 4 (ukuran *file* > 80kb dengan ukuran *file* mod blok ≠ 0).

3.1.1 Enkripsi dan Dekripsi

Hal pertama yang dilakukan untuk pengujian enkripsi dan dekripsi terhadap *plaintext* dan *ciphertext* adalah menentukan kunci, nilai *iv* dan ukuran blok. Kunci, nilai *iv* dan ukuran blok ini yang menjadi keamanan dari *plaintext* yang telah diuji. Kunci yang digunakan untuk proses enkripsi dan dekripsi adalah "ANITAMARIANYSONB". Gambar 1 memperlihatkan hasil enkripsi *file* "jurnal 36.doc" dengan ukuran blok = 100 dan *file* "opini publik.txt" dengn ukuran blok = 22, sedangkan gambar 2 memperlihatkan hasil dekripsinya dengan ukuran blok yang sama.

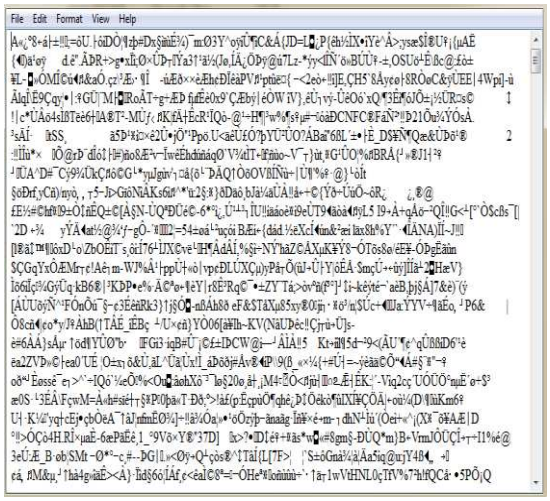


PENDAHULUAN

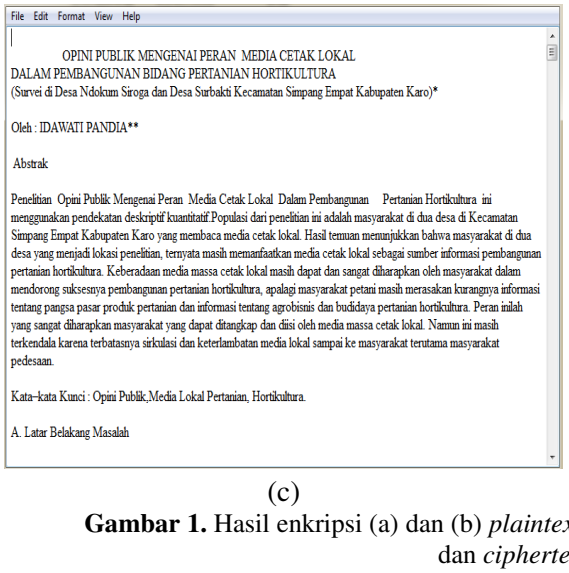
Latar Belakang

Universitas Indonesia bercita-cita menjadi Universitas riset kelas dunia. Untuk mewujudkan universitas riset diantaranya diperlukan kegiatan untuk meningkatkan jumlah dan kualitas penelitian. Harian *The Times* Inggris menampilkan hasil survei peringkat perguruan tinggi (PT) terkemuka, dari data tahun 2006 dan 2007 tiga besar dunia dibuduki Harvard University (AS), University of Cambridge (Inggris) dan University of Oxford (Inggris). Universitas Indonesia termasuk dalam 500 besar, dimana peringkat UI pada tahun 2006 (ke-250) yang disusul setelahnya adalah ITB (ke-258) dan UGM (ke-270). Sedangkan pada tahun 2007 peringkat UI mengalami penurunan (peringkat ke-395), dibawah UGM (ke-360) dan ITB (ke-369). Parameter yang dinilai diantaranya adalah jumlah dan kualitas penelitian, kualitas pendidikan, kualitas dosen/peneliti, jumlah dan

(a)



(b)



OPINI PUBLIK MENGENAI PERAN MEDIA CETAK LOKAL
DALAM PEMBANGUNAN BIDANG PERTANIAN HORTIKULTURA
(Survei di Desa Ndokum Siroga dan Desa Surbakti Kecamatan Simpang Empat Kabupaten Karo)*

Oleh : IDAWATI PANDIA**

Abstrak

Penelitian Opini Publik Mengenai Peran Media Cetak Lokal Dalam Pembangunan Pertanian Hortikultura ini menggunakan pendekatan deskriptif kuantitatif.Populasi dari penelitian ini adalah masyarakat di dua desa di Kecamatan Simpang Empat Kabupaten Karo yang membaca media cetak lokal. Hasil temuan menunjukkan bahwa masyarakat di dua desa yang menjadi lokasi penelitian, ternyata masih memanfaatkan media cetak lokal sebagai sumber informasi pembangunan pertanian hortikultura. Keberadaan media massa cetak lokal masih dapat dan sangat diharapkan oleh masyarakat dalam mendorong suksesnya pembangunan pertanian hortikultura, apalagi masyarakat petani masih merasakan kurangnya informasi tentang pangsa pasar produk pertanian dan informasi tentang agrobisnis dan budidaya pertanian hortikultura. Peran inilah yang sangat diharapkan masyarakat yang dapat ditangkap dan diisi oleh media massa cetak lokal. Namun ini masih terkendala karena terbatasnya sirkulasi dan keterlambatan media lokal sampai ke masyarakat terutama masyarakat pedesaan.

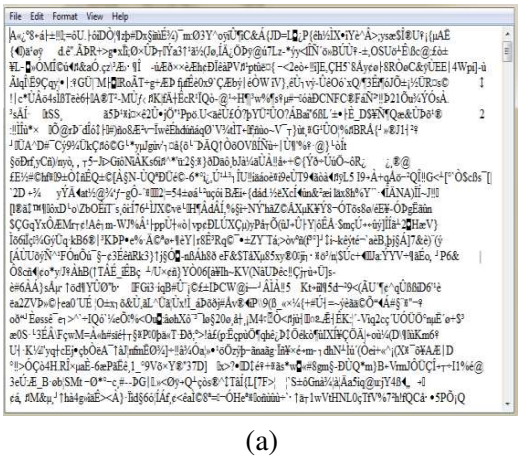
Kata–kata Kunci : Opini Publik,Media Lokal Pertanian, Hortikultura.

A. Latar Belakang Masalah

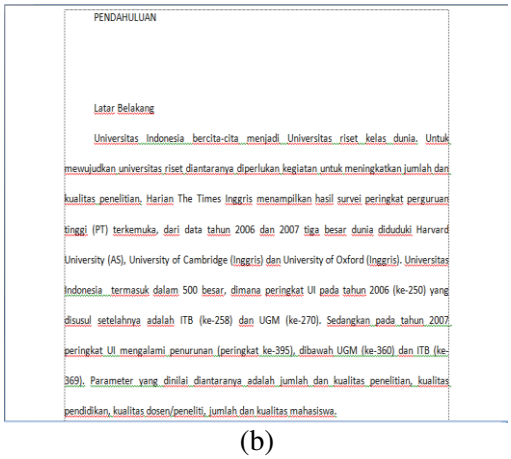
(c)

(d)

Gambar 1. Hasil enkripsi (a) dan (b) *plaintext* dan *ciphertext* "jurnal 36.doc" (c) dan (d) *plaintext* dan *ciphertext* "opini publik.txt"



(a)



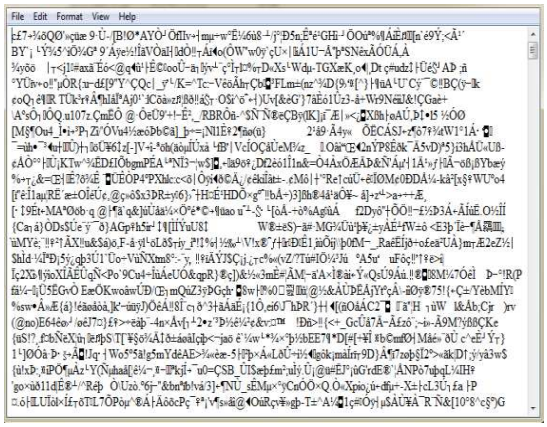
PENDAHULUAN

Latar Belakang

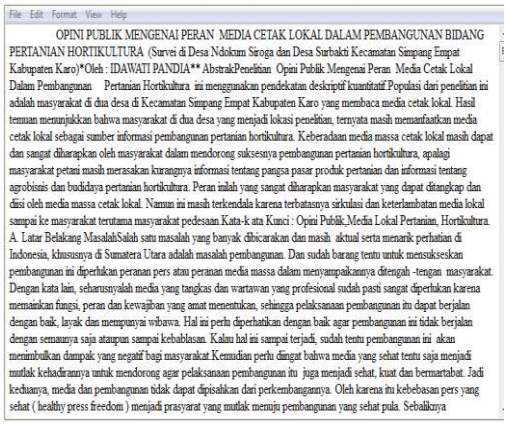
Universitas Indonesia bercita-cita menjadi Universitas riset kelas dunia. Untuk mewujudkan universitas riset diantaranya diperlukan kegiatan untuk meningkatkan jumlah dan kualitas penelitian. Harian The Times Inggris menampilkan hasil survei peringkat perguruan tinggi (PT) terkemuka, dari data tahun 2006 dan 2007 tiga besar dunia dibuduki Harvard University (AS), University of Cambridge (Inggris) dan University of Oxford (Inggris). Universitas Indonesia termasuk dalam 500 besar, dimana peringkat UI pada tahun 2006 (ke-250) yang disusul setelahnya adalah ITB (ke-258) dan UGM (ke-270). Sedangkan pada tahun 2007 peringkat UI mengalami penurunan (peringkat ke-395), dibawah UGM (ke-360) dan ITB (ke-369). Parameter yang dinilai diantaranya adalah jumlah dan kualitas penelitian, kualitas pendidikan, kualitas dosen/peneliti, jumlah dan kualitas mahasiswa.

(b)

ISSN 2337-7631



(c)



(d)

Gambar 2. Hasil dekripsi (a) dan (b) *ciphertext* dan *plaintext* "jurnal 36.doc" (c) dan (d) *ciphertext* dan *plaintext* "opini publik.txt"

3.2 Pembahasan

Ciphertext yang dihasilkan harus tahan terhadap berbagai serangan dari kriptanalis. Oleh karena itu perlu diuji tingkat keamanannya menggunakan 3 macam pengujian yaitu, analisis korelasi, analisis standar deviasi dan variansi, serta analisis histogram.

3.2.1 Analisis Korelasi

Berdasarkan pengujian korelasi dari 26 *file* uji, didapat nilai rata-rata analisis korelasi sebagai berikut:

Tabel 1. Rata-rata nilai analisis korelasi pada *plaintext* dan *ciphertext*

Pengujian	Banyak *file*	*File*	Rata-rata	Rata-rata
1	5	doc dan docx	0,000365359	0,257300484
	2	Txt	0,514235609	
2	5	doc dan docx	0,019480446	0,31721505
	2	Txt	0,614949654	
3	4	doc dan docx	0,0023413841	0,00019316705
	2	Txt	-0,0011823818	
4	4	doc dan docx	0,471442756	0,078596945
	2	Txt	0,00138917215	
Total rata-rata				**0,163326411**

Berdasarkan hasil pengujian pada tabel 1 menunjukan rata-rata nilai analisis korelasi dari pengujian 1-4 yang 17tatis mendekati 0 yaitu 0,163326411. Hal ini membuktikan bahwa hubungan antara *plaintext* dan *ciphertext* adalah "LEMAH" yakni tidak adanya kesamaan antara *plaintext* dan *ciphertext* yang memudahkan serangan dari kriptanalis.

3.2.2 Analisis Standar Deviasi dan Variansi

Berdasarkan pengujian standar deviasi dan variansi dari 26 *file* uji, didapat nilai rata-rata analisis standar deviasi dan variansi sebagai berikut:

Tabel 2. Rata-rata nilai standar deviasi dan variansi pada *plaintext*

Pengujian	Tipe *file*	Rata-rata nilai standar deviasi	Rata-rata variansi
1	doc dan docx	139,554	14.555,25
	Txt	360,325	157.534,795
2	doc dan docx	118,102	25.427,33
	Txt	253,75	70.634,795
3	doc dan docx	120,1	23.680,11
	Txt	85,34	10 574,66
4	doc dan docx	226,28	58687,565
	Txt	181,3	32869,69
Total rata-rata		**371,18**	**98491.04**

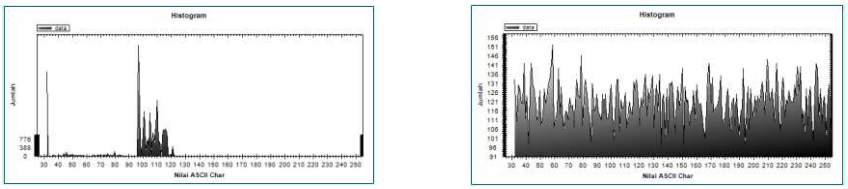
Tabel 3. Nilai standar deviasi dan variansi pada *ciphertext*

Pengujian	Tipe *file*	Rata-rata standar deviasi	Rata-rata variansi
1	doc dan docx	215,89	51.868,80
	Txt	720,40	740.976,34
2	doc dan docx	216,82	65.263,42
	Txt	2.038,45	39.825.026,49
3	doc dan docx	204,13	62.783,99
	Txt	172,09	39.285,47
4	doc dan docx	339,79	130.606,44
	Txt	540,10	111.540,13
Total rata-rata		**1111,9175**	**10.256.837,77**

Standar deviasi merupakan variasi sebaran data, semakin besar nilai sebarannya berarti data semakin bervariasi. Tabel 1 dan 2 menunjukan rata-rata nilai standar deviasi dan variansi dari *plaintext dan ciphertext* yang memiliki perbedaan cukup besar yaitu nilai standar deviasi dari *plaintext* =371,18 dan *ciphertext* = 1111,9175 sedangkan nilai variansi *plaintext* = 98491.04 dan *ciphertext* = 10.256.837,77. Hal ini menunjukan bahwa data pada *ciphertext* lebih bervariasi dibandingkan dengan *plaintext.*

3.2.3 Analisis Histogram

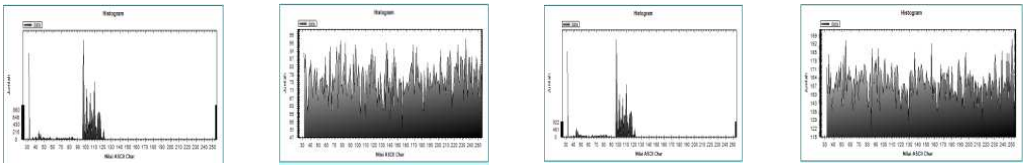
Berdasarkan hasil pengujian terhadap 26 *file* uji, didapat histogram *plaintext* dan *ciphertext* sebagai berikut:



(a) **(b)**

Gambar 3. Histogram *file* txt, (a) *plaintext* dan (b) *ciphertext* "sistem informasi pemerintahan.txt"

ISSN 2337-7631



(a) **(b)** **(c)** **(d)**

Gambar 4. Histogram *file* doc dan docx, (a) *plaintext* dan (b) *ciphertext* "tayangan kekerasan ditelevisi.docx", (c) *plaintext* dan (d) *ciphertext* "gaya hidup masyarakat.docx"

IV. PENUTUP

4.1 Kesimpulan

Dari hasil uji dan analisis yang dilakukan maka dapat disimpulkan beberapa hal sebagai berikut:

a. Algoritma yang diusulkan cocok untuk enkripsi teks yang bertipe doc, docx dan txt. Secara kasat mata hasil *ciphertext* yang dihasilkan sangat berbeda dengan *plaintext.*
b. Analisis rata-rata nilai korelasi terhadap *plaintext* dan *ciphertext* pada 26 *file* uji yang mendekati 0 yakni 0,163326411. Hal ini menunjukan hubungan yang "LEMAH" antara *ciphertext* dan *plaintext.*
c. Analisis rata-rata nilai standar deviasi dan variansi dari *plaintext* dan *ciphertext* yang memiliki perbedaan cukup besar yaitu nilai standar deviasi dari *plaintext* = 371,1*8* dan *ciphertext* = 555,964885 sedangkan nilai variansi *plaintext* = 98491.04 dan *ciphertext* =5.128.418,89. Hal ini menunjukan bahwa data pada *ciphertext* lebih bervariasi dibandingkan dengan *plaintext*.
d. Analisis histogra*m ciphertext* yang diperoleh dari 4 pengujian terhada*p file* doc, docx, dan txt diperoleh hasil histogram *ciphertext* yang seragam terhadap semu*a file* uji sehingga mempersulit analisis statistik untuk menganalisis karakter atau kunci.
e. Proses enkripsi dan dekripsi membutuhkan waktu yang cukup lama, ini dipengaruhi oleh ukuran *file,* banyaknya karekter, dan besarnya ukuran blok.

4.2 Saran

Berdasarkan hasil pengujian sistem yang telah dilakukan. Maka diberikan beberapa saran untuk pengembangan sistem sebagai berikut:

a. Sistem kriptografi yang dikembangkan hanya mampu mengenkripsi teks yang ada pada *file* doc dan docx, sedangkan untuk gambar, tabel, equation, dan lain-lain yang terdapat pada *file* doc dan docx belum dapat dilakukan sehingga perlu adanya pengembangan dari sistem ini.
b. Memperbaiki algoritma yang digunakan agar tidak membutuhkan waktu komputasi yang lama.
c. Memperbaiki algoritma yang digunakan sehingga ukuran *file* setelah enkripsi sama dengan ukuran *file* sebelum enkripsi.

DAFTAR PUSTAKA

[1] Martin, K., 2012, *Everyday Cryptography. Oxford University Press.*

[2] Ye, Ruisong dan Gou, Weichuang., 2013, *A Chaos-based Image Encryption Scheme Using Mulltimodal Skew Tent Map*, http://www.cisjournal.org/journalofcomputing/archive/vol4no10/vol4no10, 10 Oktober 2013, diakses tanggal 23 Mei 2014.

[3] Munir, R., 2012, Security Analysis of Selective Image Encryption Algorithm Based on Chaos and CBC-like Mode, *International Conference on Telecommunication Systems, Services, and Applications* (TSSA), Bandung, *http://informatika.stei.itb.ac.id*, diakses tanggal 18 Maret 2014.