ISBN: 978-602-6697-66-0

SUPER ENKRIPSI FILE DOKUMEN MENGGUNAKAN BEAUFORT CIPHER DAN TRANSPOSISI KOLOM

SUPER ENCRYPTION DOCUMENT FILE USING BEAUFORT CIPHER AND COLUMNAR TRANSPOSITION

[1)]Candra Irawan, [2)] Eko Hari Rachmawanto, [3)]Christy Atika Sari, [4)]Castaka Agus Sugianto
[1)]Program Studi Sistem Informasi, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang 50131
Email: [1]candra.irawan@dsn.dinus.ac.id
[2,3)]Program Studi Teknik Informatika, Fakultas Ilmu Komputer
Universitas Dian Nuswantoro
Jl. Imam Bonjol 207 Semarang 50131
Email: [2]eko.hari@dsn.dinus.ac.id, [3]christy.atika.sari@dsn.dinus.ac.id
[4)]Program Studi Teknik Informatika
Politeknik TEDC Bandung
Jl. Politeknik Jl. Pesantren No.2, Cibabat, Kec. Cimahi Utara, Kota Cimahi, Jawa Barat 40513
Email: [1]castaka@poltektedc.ac.id

ABSTRAK

Proses pengamanan data teknik super enkripsi perlu dikaji kembali khususnya optimalisasi kunci yang berdampak pada keamanan yang dihasilkan. Beaufort cipher merupakan algoritma sederhana dan cepat dalam operasi. Panjang kunci beaufort mengikuti panjang file sehingga apabila ukuran file besar maka kunci menjadi panjang. Panjang kunci tidak selalu menghasilkan keamanan yang tinggi sehingga perlu optimasi panjang kunci menggunakan algoritma lain. Transposisi kolom digunakan untuk mengoptimasi panjang kunci pada beaufort cipher sehingga kunci menjadi lebih acak. Tujuan pengacakan ganda adalah meningkatkan keamanan data. Uji coba dilakukan pada enkripsi beaufort cipher saja dan optimasi beaufort cipher-transposisi kolom. Pengujian enkripsi menggunakan *Entropy*, sedangkan dekripsi menggunakan *Avalanche Effect (AE)* dan *Bit Eror Rate (BER)*. Dari 30 dataset dengan ukuran file 1kb sampai 500kb, telah dihitung pula waktu pemrosesan enkripsi dan dekripsi menggunakan RAM Intel® Core ™ i5-8400 CPU @ 2.80GHz (6 CPUs) 16 GB. File 500kb dapat diproses dengan waktu 0.0044 detik untuk enkripsi. *Entropy*, AE, BER terbaik yang diperoleh berturut-turut yaitu 7.8665, 56% dan 0. Pengujian menggunaan *tool sofware PDF Password Remover* dan membuktikan bahwa aplikasi tidak bisa membaca file pdf yang teracak karena proses enkripsi.

Kata Kunci : Super enkripsi, file dokumen, beaufort cipher, transposisi kolom.

ABSTRACT

Super encryption technique data security process needs to be reviewed, especially key optimization which has an impact on the resulting security. Beaufort cipher is a simple algorithm and fast in operation. The length of the beaufort key follows the length of the file so that if the file size is large, the key becomes long. Key length does not always result in high security so it is necessary to optimize the key length using another algorithm. Column transposition is used to optimize the key length of the beaufort cipher so that the keys become more random. The purpose of multiple randomisation is to increase data security. Experiments were carried out on the Beaufort Cipher encryption only and the optimization of the Beaufort Cipher-column transposition. The encryption test uses Entropy, while the decryption uses the Character Error Rate (CER), Avalanche Effect (AE) and Bit Error Rate (BER). From 30 datasets with file sizes of 1kb to 500kb, the processing time for encryption and decryption has also been calculated using Intel® Core ™ i5-8400 CPU @ 2.80GHz (6 CPUs) 16 GB of RAM. 500kb files can be processed in 0.0044 seconds for encryption. The best Entropy, AE, BER obtained 7.8665, 56% and 0. The test used the PDF Password Remover software and proved that the application cannot read randomized PDF files due to the encryption process.
***Keywords** : Super encryption, document file, beaufort cipher, columnar transposition*.

ISBN: 978-602-6697-66-0

PENDAHULUAN

Algoritma kriptografi adalah suatu teknik atau rumus yang membuat data atau jaringan menjadi aman dengan memberikan keamanan. Kriptografi adalah ilmu merancang metode yang memungkinkan informasi dikirim dalam bentuk yang aman sedemikian rupa sehingga satu-satunya orang yang dapat mengambil informasi ini adalah penerima yang dituju. Penggunaan jaringan yang tinggi menyebabkan pertukaran data melalui jaringan saat berkomunikasi ke satu dan sistem lain. Sedangkan komunikasi sangat penting untuk mengenkripsi pesan sehingga penyusup tidak dapat membaca pesan tersebut. Keamanan jaringan sangat didasarkan pada kriptografi.

Kriptografi adalah seni menyembunyikan informasi dengan mengenkripsi pesan. Seni melindungi informasi (enkripsi) itu ke dalam format yang tidak terbaca (teks terenkripsi), disebut teks sandi (Ginting, Isnanto, & Windasari, 2015). Hanya mereka yang memiliki kunci rahasia yang dapat memecahkan sandi (mendekripsi) pesan menjadi teks biasa. Sistem di mana data pertama (teks biasa) dienkripsi di sisi pengirim dan didekripsi menjadi teks biasa lagi di ujung penerima menggunakan kunci unik atau rumus tertentu disebut sistem kriptografi. Pesan terenkripsi terkadang dapat dipecahkan oleh kriptanalisis, juga disebut pemecah kode meskipun teknik kriptografi modern hampir tidak bisa dipecahkan (Rosyadi, 2012). Ketika Internet dan bentuk komunikasi elektronik lainnya menjadi lebih umum, keamanan elektronik menjadi semakin penting. Kriptografi digunakan untuk melindungi pesan email, informasi kartu kredit, dan data perusahaan. Salah satu sistem kriptografi terpopuler yang digunakan di Internet adalah Pretty Good Privacy karena efektif dan gratis. Berdasarkan data masukan, algoritme sandi diklasifikasikan sebagai sandi blok, di mana ukuran blok berukuran tetap untuk enkripsi dan sandi aliran di mana aliran berkelanjutan dilewatkan untuk enkripsi dan dekripsi. Di antara algoritma yang dipertimbangkan, beberapa di antaranya adalah block cipher seperti RSA, DES, AES, Blowfish, Twofish, Threefish dan lainnya. Jenis lain adalah stream cipher misalnya ECC, RC5.

Symmetric dan Asymmetric adalah dua jenis enkripsi. Dalam teknik enkripsi simetris menggunakan kunci yang sama untuk tujuan enkripsi dan dekripsi. Enkripsi kunci asimetris menggunakan kunci publik dan privat, kunci publik diumumkan ke semua anggota sementara kunci privat disimpan aman oleh pengguna (Sari, Rachmawanto, Astuti, & Umaroh, 2016). Pengirim menggunakan kunci publik penerima untuk mengenkripsi pesan. Penerima menggunakan kunci pribadinya sendiri untuk mendekripsi pesan. Dalam metode simetris, ada dua teknik (substitusi dan transposisi) yang digunakan sebagai metode klasik (Permana, Sari, Rachmawanto, & Subhiyakto, 2017). Sandi Beaufort, adalah sandi substitusi yang mirip dengan sandi Vigenère, dengan mekanisme penyandian dan tabel yang sedikit dimodifikasi (Emy, 2015). Penerapannya yang paling terkenal adalah pada mesin sandi berbasis rotor. Substitusi memiliki dua jenis lebih lanjut, sandi mon oalphabetic dan polyalphabetic. Secara monoalphabetic karakter pada Plaintext diubah menjadi karakter yang sama pada Ciphertext (Widyastuti, 2014). Dalam polyalphabetic cipher satu karakter dalam Plaintext diubah menjadi banyak karakter dalam Ciphertext. Teknik termutasi adalah salah satu di mana Plaintext tetap sama, tetapi urutan karakter diacak untuk mendapatkan Ciphertext. Cipher simetris dapat dibagi menjadi cipher Stream dan cipher blok, sebagai cipher modern. Stream cipher mengenkripsi digit (biasanya byte), atau huruf (dalam sandi pengganti) dari sebuah pesan satu per satu. Block cipher mengambil sejumlah bit dan mengenkripsi mereka sebagai satu kesatuan, mengisi teks biasa sehingga merupakan kelipatan dari ukuran blok.

Sedangkan untuk transposisi kolom adalah salah satu macam algoritma yang mentransposisikan huruf untuk menenkripsi ataupun mendekripsi (Megantara & Rafrastara, 2019). Contoh lain dalam kriptografi teknik transposisi adalah transposisi Rail Fence (Ratna, 2018), Transposisi Route (Kusumaningtyas, 2018), Transposisi ganda (Priyam, 2015), dan Transposisi Myszkowski (Bhowmic & Geetha, 2015). Teknik transposisi cara kerjanya dengan membuat pesan bersandi (chipertext) dengan menggantikan posisi objek – objek pesan asli (plaintext) tanpa mengganti atau merubah pesan asli (plaintext) tersebut. Pada teknik transposisi kolom ini pembacaan matrix dilakukan dengan cara membaca kolom perkolom sesuai dengan kunci yang digunakan. Pengurutan pada proses enkripsi diurutkan juga berdasarkan kuncinya (Sinaga & Umam, 2018). Penomoran pada kunci dilakukan sesuai dengan urutan huruf abjad. Yang kemudian membuat sebuah tabel dengan baris dan kolom sebanyak panjang kunci. Selanjutnya, pesan asli (plaintext) dimasukkan kedalam tabel tersebut. Setelah semua pesan asli (plaintext) memenuhi tabel yang telah dibuat maka proses enkripsi bisa dilakukan.

ISBN: 978-602-6697-66-0

METODE

Beaufort Cipher

Beaufort cipher merupakan salah satu jenis dari polyalphabetic cipher. Seperti namanya beaufort chipper ditemukan oleh Sir Francis Beaufort. Beaufort cipher hampir sama dengan vigenere cipher, yang membedakan adalah beaufort cipher memiliki urutan alphabet B~Z dalam ciphertext yang terbalik. Enkripsi dengan beaufort dapat diselesaikan dengan tabel tabula recta. Untuk menyelesaikan sebuah persoalan tentang mengenkripsi dengan beaufort cipher kita harus membuat sebuah kolom dimana header atas diisi dengan huruf abjad, kemudian header samping diisi dengan kunci (key) dengan penghilangan huruf yang kembar (Sari & Hayati, 2018). Kunci (key) dijabarkan sepanjang huruf plaintext seperti pada Gambar 1.

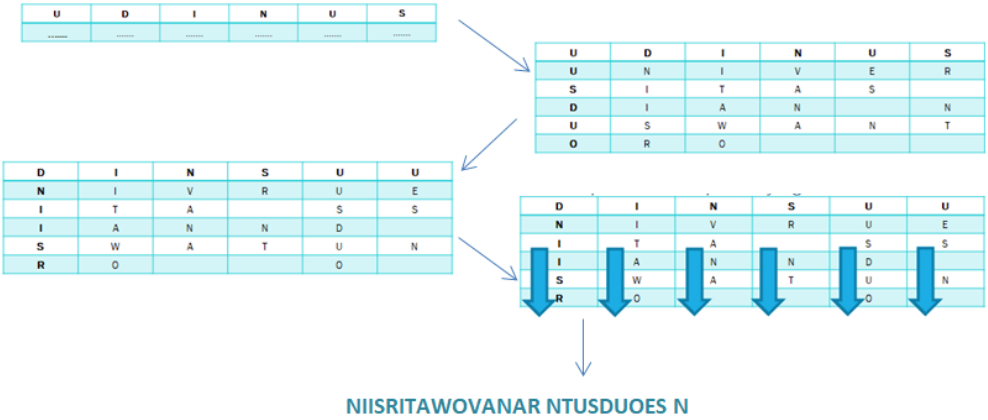
P	D	I	A	N	N	U	S	W	A	N	T	O	R	O
K	P	O	L	K	E	P	O	L	K	E	P	O	L	K

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

Gambar 1. Proses enkripsi pada Beaufort Cipher

Transposisi Kolom

Penyandian transposisi kolom dituliskan dengan sebaris seperti biasanya dengan panjang kunci yang telah ditentukan sebelumnya. Kemudian kunci yang telah ditentukan dinomori sesuai urutan huruf abjad, jika huruf a maka urutan nomornya adalah 1 dan kemudian seterusnya seperti ditunjukkan pada Ganbar 2.

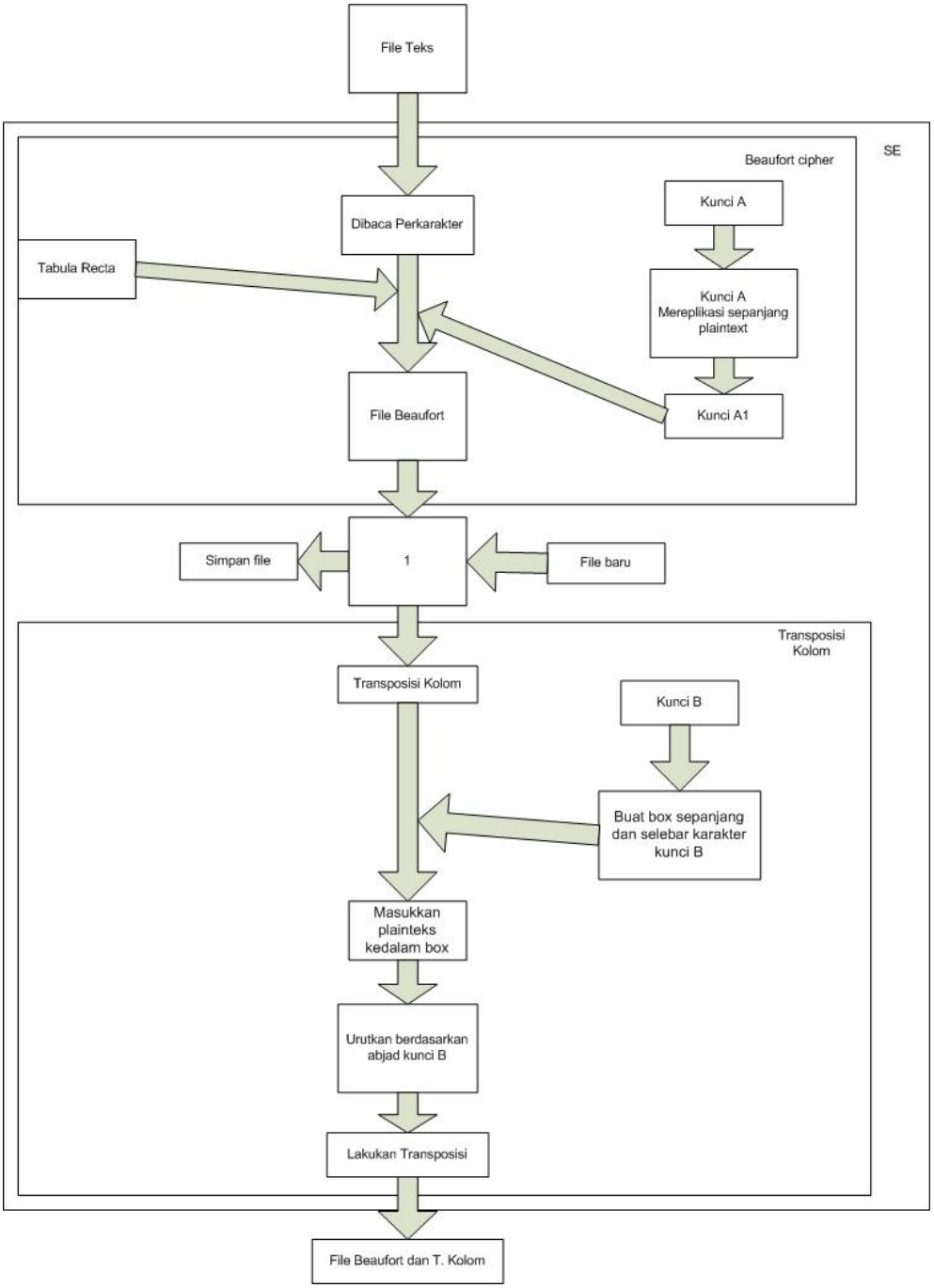


Gambar 2. Proses enkripsi pada Transposisi Cipher

Proses enkripsi dan dekripsi file

Berdasarkan Gambar 3, proses enkripsi file dimulai dengan melakukan proses input dan pembacaan bit karakter dari file tersebut. Hasilnya adalah file tidak bisa dibuka karena bit karakter telah diacak. Kemudian, pada kotak yang bernomor 1, pengguna akan diberi pilihan apakah akan meneruskan mengenkripsi dengan beaufort saja atau dengan transposisi kolom juga. Pada tahap transposisi kolom, seteleah kunci diinputkan maka dibuatlah box sepanjang kunci yang diinputkan.

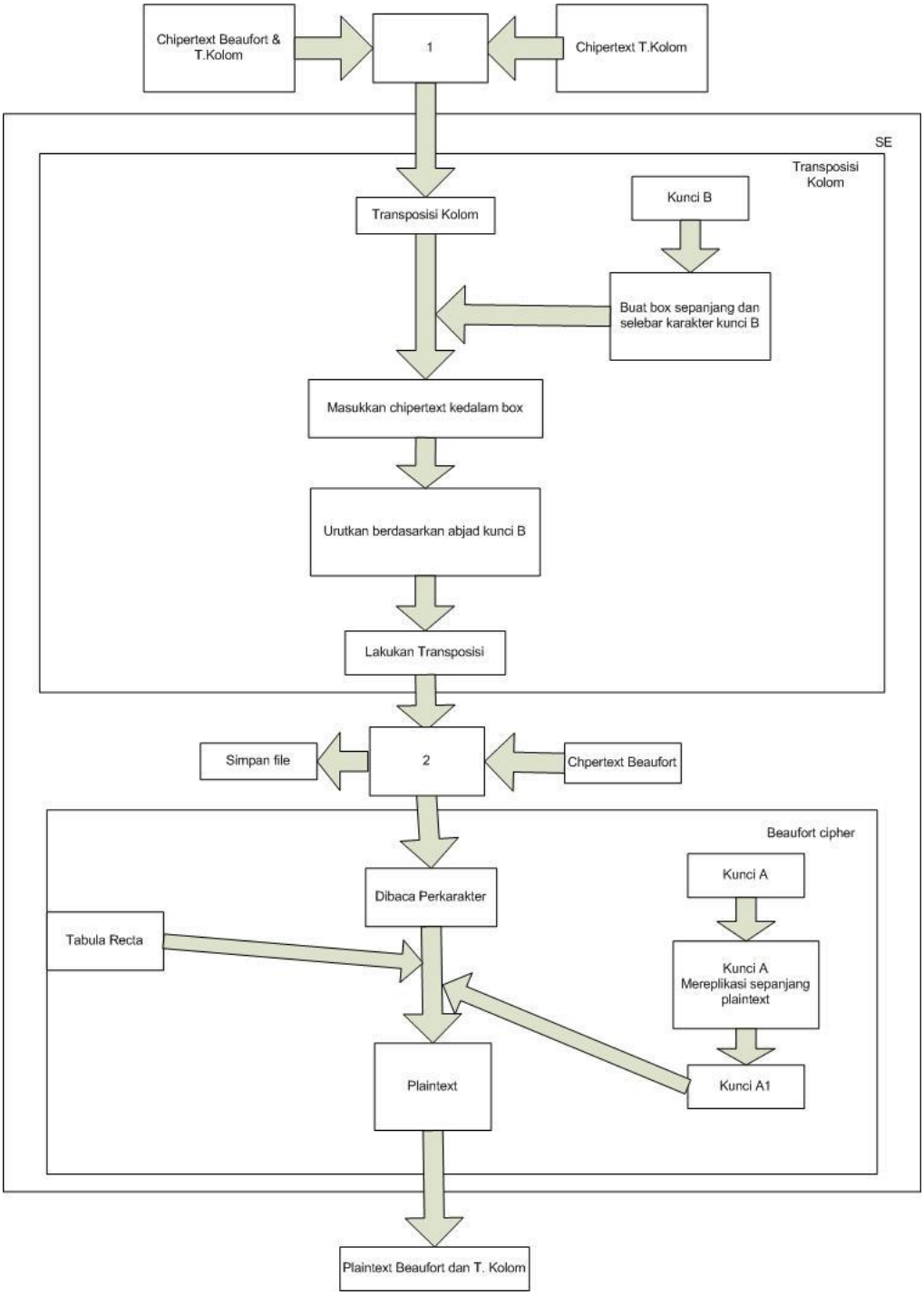
ISBN: 978-602-6697-66-0



Gambar 3. Proses Enkripsi File

Pada Gambar 4, proses dekripsi file dimulai saat pengguna memilih kotak yang memiliki nomor 1 didalamnya, pengguna memilih file mana yang akan didekripsi. Jika ciphertext beaufort saja maka langsung saja ketahap kotak bernomor 2. Proses dekripsi adalah mengembalikan cipherteks ke plainteks, jadi prosesnya kebalikan dari proses enkripsi. Dimana metode transposisi kolom dilakukan terlebih dahulu.

ISBN: 978-602-6697-66-0



Gambar 4. Proses Dekripsi File

Pengukuran Hasil

Entropi adalah konsep acak dimana terdapat kemungkinan yang tidak pasti (Emy, 2015). Hubungan entropi dengan informasi adalah ukuran yang menyatakan jumlah informasi didalam pesan. Besaran entropi biasanya dinyatakan dalam satuan bit. Didalam kriptografi entropi berguna untuk memperkirakan jumlah bit rata-rata dalam mengkodekan elemen pesan (Emy, 2015). Entropi dapat dihitung menggunakan rumus berikut.

$$H_e = -\sum_{k=0}^{n} P(k)\log_2(P(k))$$

Dengan $H_e$sebagai entropi, n menyatakan jumlah simbol yang berbeda didalam pesan, pada citra n adalah nilai keabuan dari citra, kemudian untuk P(k) adalah probabilitas kejadian simbol k. Jika sebuah pesan

ISBN: 978-602-6697-66-0

dienkripsi dengan kondisi teracak, nilai dari entropi yang ideal adalah ≈ 8. Yaitu setiap simbol dalam pesan tersebut dikodekan sebanyak ≈ 8 bit. Dengan demikian, sistem enkripsi yang dibuat aman dari serangan entropi. Jika sebuah sistem enkripsi diuji dan mendapat nilai lebih kecil dari 8, maka data disebut sistem enkripsi tersebut masih dapat ditebak (Emy, 2015).

Avalanche Effect (AE)

Algoritma kriptografi akan memenuhi nilai avalanche effect jika satu buah bit input mengalami perubahan, maka probabilitas semua bit berubah adalah setengahnya yaitu 50%. Apabila nilai AE lebih dari 50%, dapat dikatakan bahwa skema kriptografi tersebut adalah aman. Rumus AE adalah sebagai berikut.

$$\text{Avalanche Effect} = \frac{\text{jumlah bit yang berubah}}{\text{jumlah bit total}} \text{ x } 100\%$$

Bit Error Rate (BER)

BER digunakan untuk menguji hasil pesan yang telah diekstraksi dengan bentuk berupa prosentase bit yang salah dibandingkan dengan total bit pada saat dilakukan penyisipan sesuai rumus berikut. Nilai BER yang baik yaitu mendekati 0, dengan demikian tidak terdapat perbedaan antara hasil eklstraksi dan data asli.

$$\text{BER} = \frac{\text{jumlah bit error}}{\text{jumlah bit seluruhnya}} \text{ x } 100\%$$

HASIL DAN PEMBAHASAN

Pada penelitian ini digunakan yaitu 30 file dengan berbagai ukuran dari 1 kb sampai 500 kb, sedangkan format file yang digunakan *.txt, *.pdf, *.doc, *docx, dan lain lain dimana masing – masing format file diuji menggunakan ukuran file yang berbeda-beda. Pada Tabel 1, kami telah menguji coba lama waktu enkripsi dan dekripsi menggunakan instrument dengan RAM Intel® Core ™ i5-8400 CPU @ 2.80GHz (6 CPUs) 16 GB.

Tabel 1. Lama Waktu Enkripsi, Dekipsi, Entropy, dan BER

Tipe	Ukuran (kb)	Enkripsi	Dekripsi	Entropy	BER
Jpg	1	0.0003	0.0004	6.0064	0
Bmp	3	0.0005	0.0005	7.2350	0
Txt	6	0.0005	0.0006	7.2215	0
Pdf	10	0.0006	0.0006	6.9924	0
Doc	12	0.0007	0.0007	6.0140	0
Docx	15	0.0008	0.0009	6.0154	0
Rtf	17	0.0008	0.0012	7.0654	0
Png	25	0.0008	0.0012	7.2115	0
Pdf	50	0.0009	0.0014	7.2852	0
Pdf	75	0.0010	0.0015	7.2554	0
Txt	85	0.0010	0.0016	6.2154	0
Wav	100	0.0011	0.0018	7.5568	0
Wav	110	0.0013	0.0018	7.8665	0
Bmp	125	0.0014	0.0019	7.7754	0
Jpg	140	0.0019	0.0021	6.0254	0
Pdf	170	0.0019	0.0024	6.5244	0
Pdf	250	0.0019	0.0025	7.2265	0
Bmp	270	0.0020	0.0025	7.3365	0
Png	300	0.0021	0.0026	7.3356	0
Bmp	330	0.0026	0.0034	7.1554	0
Rtf	376	0.0027	0.0037	7.3665	0
Bmp	400	0.0027	0.0037	7.5614	0
Wav	408	0.0029	0.0038	7.2350	0
Mp3	440	0.0040	0.0038	6.9556	0

ISBN: 978-602-6697-66-0

Mp3	450	0.0040	0.0038	6.8755	0
Pdf	471	0.0041	0.0038	7.2664	0
Pdf	480	0.0041	0.0038	7.7781	0
Doc	490	0.0042	0.0038	7.8612	0
Docx	492	0.0043	0.0038	7.2651	0
Pdf	500	0.0044	0.0038	6.6625	0

Tabel 2. Nilai AE pada beberapa pesan berbeda

Data Teks	Algoritma		
	Beaufort	Transposisi Kolom	Beaufort + Transposisi Kolom
Percobaan	48 %	42 %	53 %
Seminar nasional	47 %	41 %	56 %
Universitas Dian Nuswantoro	45 %	42 %	54 %
Aplikasi Kriptografi Super Enkripsi	45 %	43 %	54 %

Dengan menggunakan password software remover sesuai Gambar 4, file acak terpilih telah menunjukkan bahwa aplikasi tidak dapat membaca file yang diinputkan.

a) Pdf password remover file normal b) Pdf password remover file enkripsi

Gambar 4. Uji dengan aplikasi password remover

Berdasarkan Gambar 4 point a, dijelaskan bahwa file berformat *.pdf tersebut merupakan file yang belum dienkripsi, tandanya adalah pada kolom event bertuliskan *"File is not encrypted"*. Sedangkan untuk membuktikan bahwa file pdf tersebut betul-betul telah dienkripsi seperti tampak pada Gambar 4 point b memperlihatkan bahwa aplikasi tiba tiba terhenti, ini dikarenakan aplikasi tidak bisa membaca file pdf yang teracak isinya karena telah dienkripsi. Kemudian untuk membuka file tersebut bisa didekripsi dengan aplikasi penyandian file menggunakan metode super enkripsi yang diusulkan oleh peneliti.

KESIMPULAN

Berdasarkan percobaan yang telah dilakukan menggunakan 30 dataset yang berasal dari berbagai macam jenis file dengan ukuran mulai dari 1 kb hingga 500 kb, diperoleh nilai avalanche effect terbesar yaitu 56% menggunakan hybrid beaufort dan transposisi kolom. Perolehan nilai AE beaufort saja maupun transposisi kolom saja terbukti lebih rendah dibanding usulan metode pada makalah ini. Seluruh data menghasilkan nilai BER = 0 yang berarti file hasil ekstraksi sama persis dengan file asli sebelum proses enkripsi. Pada perhitungan entropy, diperoleh nilai mendekati 8. Pada 30 percobaan, tidak terdapat nilai entropy kurang dari 6 dan beberapa nilai entropy mendekati nilai maksimal.

DAFTAR PUSTAKA

Bhowmic, A., & Geetha, M. (2015). Enhancing resistance of hill cipher using columnar and Myszkowski transposition. International Journal of Computer Sciences and Engineering, 20-25.

Emy, S. (2015). Kriptografi & Implementasinya menggunakan MATTLAB. Yogyakarta: ANDI Yogyakarta.

Ginting, A., Isnanto, R., & Windasari, I. (2015). Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. Jurnal Teknologi dan Sistem Komputer, 253-258.

ISBN: 978-602-6697-66-0

Kusumaningtyas, J. (2018). Analisa Algoritma Ciphers Transposition: Study Literature. Multimatrix, 1-12.

Megantara, R., & Rafrastara, F. (2019). SUPER ENKRIPSI TEKS KRIPTOGRAFI MENGGUNAKAN ALGORITMA HILL CIPHER DAN TRANSPOSISI KOLOM. Prosiding SENDI_U 2019 (pp. 85-92). Semarang: Universitas Stikubank.

Natsir, M. (2016). Pengembangan Prototype Sistem Kriptografi Untuk Enkripsi Dan Dekripsi Data Office Menggunakan Metode Blowfish Dengan Bahasa Pemrograman Java. Jurnal Format, 87-105.

Permana, T., Sari, C., Rachmawanto, E., & Subhiyakto, E. (2017). Implementasi Pengamanan Citra Digital Berbasis Metode Kriptografi Vernam Cipher. Techno. Com, 337-347.

Priyam, A. (2015). Extended Vigenère using double Transposition. Intl J Engg Sci Adv Research, 62-65.

Ratna, D. (2018). IMPLEMENTASI ALGORITMA RAIL FENCE CHIPER DALAM KEAMANAN DATA GAMBAR 2 DIMENSI. Jurnal Pelita Informatika, 38-42.

Rosyadi, A. (2012). IMPLEMENTASI ALGORITMA KRIPTOGRAFI AES UNTUK ENKRIPSI DAN DEKRIPSI EMAIL. Transient: Jurnal Ilmiah Teknik Elektro, 63-67.

Sari, C., Rachmawanto, E., Astuti, Y., & Umaroh, L. (2016). OPTIMASI PENYANDIAN FILE MENGGUNAKAN KRIPTOGRAFI SHIFT CIPHER. Proceeding SENDI_U ke 2. Semarang: Universitas Stikubak.

Sari, R., & Hayati, R. (2018). Beaufort Cipher Algorithm Analysis Based on the Power Lock-Blum Blum Shub in Securing Data. 6th International Conference on Cyber and IT Service Management (CITSM) (pp. 1-4). Parapat: IEEE.

Sinaga, D., & Umam, C. (2018). IMPLEMENTASI KRIPTOGRAFI VIGENERE CIPHER PADA MEDIA TEKS DENGAN KOMBINASI TRANSPOSISI KOLOM. Prosiding SENDI_U 2018 (pp. 136-139). Semarang: Universitas Stikubank.

Widyastuti, N. (2014). PENGEMBANGAN METODE BEAUFORT CIPHER MENGGUNAKAN PEMBANGKIT KUNCI CHAOS. Jurnal Teknologi, 73-82.