EXPLORER
Journal of Computer Science and Information Technology
E-ISSN 2774-4647

Proteksi Keamanan Data dengan Menerapkan Algoritma Bacon Cipher dan ROT128

Indra Rahmatsyah[1], Yunita Sari Siregar[2], Khairunnisa[3]
Fakultas Teknik dan Komputer, Program Studi Teknik Informatika, Universitas Harapan Medan
Jalan H.M. Joni No. 70 Medan, Indonesia

Email: Indrarahmatsyah16@gmail.com, yunitasarisiregar1990@gmail.com, khairunnisajv2@gmail.com,

Abstrak-Aktivitas penyimpanan data dan pertukaran informasi secata digital mempunyai resiko dan tentunya harus disertai dengan keamanan informasi. Berbagai cara dilakukan untuk memproteksi data seperti menyembunyikan data dengan teknik steganografi atau dengan cara menyandikan data dengan teknik kriptografi. Jika pada umumnya teknik steganografi dilakukan dengan cara menyisipkan data kedalam media citra, audio ataupun video, akan tetapi dalam penelitian ini data akan disisipkan atau disembunyikan kedalam file text sebagai media (cover message) untuk menyembunyikan data. Sedangkan pengaman data dengan teknik kriptografi dilakukan dengan merubah data yang akan dirahasiakan (plaintext) menjadi data yang disandikan (ciphertext) sehingga data tersebut tidak dapat dipahami oleh orang yang tidak mempunyai legalitas pada data tersebut. Maka dari itu dengan metode ini pengamanan file penelitian menghasilkan sebuah pengujian dari blackbox testing enkripsi dan deskripsi serta ekstraksi. Dimana hasil enkripsi pada file teks terenkripsi dengan menggunakan algoritma ROT128 dengan waktu 1,82ms dan dimana hasil deskripsi pada file teks menghasilkan file teks terdekripsi dengan menggunakan algoritma ROT128 dengan waktu 1,47ms. Setelah melakukan proses ekstraksi pada file teks hasil deskripsi dengan menggunakan algoritma Bacon Cipher akan menghasilkan teks asli dengan waktu 13,95ms.

Kata Kunci: Steganografi, Kriptografi, Bacon Cipher, ROT128

Abstract-The data storage and information exchange activities digitally have risks and of course must be accompanied by information security. Various ways are done to protect data such as hiding data with steganography techniques or by encoding data with cryptographic techniques. If in general the steganography technique is done by inserting data into image, audio or video media, but in this study the data will be inserted or hidden into a text file as a media (cover message) to hide the data. While data security with cryptographic techniques is done by changing the data to be kept secret (plaintext) into encoded data (ciphertext) so that the data cannot be understood by people who do not have legality in the data. Therefore, with this method of securing research files, it produces a test of blackbox testing of encryption and description and extraction. Where is the result of the encryption on the encrypted text file using the ROT128 algorithm with a time of 1.82ms and where is the result of the description on the text file producing a decrypted text file using the ROT128 algorithm with a time of 1.47ms. After carrying out the extraction process on the resulting text file description using the Bacon Cipher algorithm, it will produce the original text with a time of 13.95ms.

Keywords: Steganography, Cryptography, Bacon Cipher, ROT128

1. PENDAHULUAN

Munculnya internet dan kemajuan pada bidang teknologi informasi, mengakibatkan informasi tidak hanya terdapat di media massa tradisional seperti televisi akan tetapi informasi bisa didapatkan oleh setiap orang yang memiliki akses terhadap internet. Kemajuan dalam bidang teknologi informasi memberikan banyak keuntungan bagi kehidupan manusia, tetapi keuntungan yang ditawarkan juga menimbulkan kejahatan seperti pencurian data [1]. Perkembangan ilmu pengetahuan untuk mengamankan data semakin ditingkatkan agar pengguna teknologi selalu merasa aman. Aktivitas penyimpanan data dan pertukaran informasi secata digital mempunyai resiko dan tentunya harus disertai dengan sistem keamanan informasi itu sendiri. Berbagai cara dilakukan bagaimana menjaga keamanan data seperti menyembunyikan data dengan teknik *steganografi* atau dengan cara menyandikan data menjadi suatu kode-kode yang tidak dimengerti, sehingga apabila dicuri atau disadap oleh orang lain akan kesulitan untuk mengetahui dan memahami informasi yang sebenarnya. Bacon Cipher merupakan salah satu teknik *steganografi*. Dasar dari *steganografi* menggunakan Bacon Cipher adalah dengan menggantikan atau melambangkan sebuah alphabet dengan sebuah deretan huruf [2], [3]. algoritma ROT128 merupakan pengembangan dari algoritma ROT13. Algoritma ROT13 merupakan salah satu algoritma kriptografi yang bekerja menyandikan pesan dengan cara mensubstitusikan sebuah karakter dengan 13 karakter sesudahnya sehingga abjad “A“ menjadi “N“ dan sebaliknya abjad “N“ menjadi “A“ ROT13 juga disebut monoalfabetik cipher karena memilki sifat yaitu satu huruf di plaintext diganti dengan tepat satu huruf ciphertext [2], [4], [5].

Penelitan ini menggabungkan teknik *steganografi* dan *kriptografi* dengan mengimplementasikan kombinasi algoritma Bacon Cipher dan algoritma ROT128 untuk memproteksi keamanan data berupa *file text* [3], [6]. Jika pada umumnya teknik *steganografi* dilakukan dengan cara menyisipkan data kedalam media citra, audio ataupun video, akan tetapi dalam penelitian ini data akan disisipkan atau disembunyikan kedalam *file text* sebagai media (*cover message*) untuk menyembunyikan data.
Kombinasi antara Bacon Cipher dan algoritma ROT128 dalam penelitan ini untuk mendapatkan *ciphertext* yang lebih kuat dan sulit untuk dipecahkan, sehingga dengan menggunakan perpaduan dua algoritma ini, maka dapat mengoptimalkan *proteksi* keamanan data [2], [7]. Kombinasi antara kedua algoritma ini juga akan mengatasi penggunaan *ciphertext* tunggal yang secara komparatif lemah.
Tujuan dilakukan penelitian ini adalah untuk mengimplementasikan kombinasi algoritma Bacon Cipher dan ROT128 dalam memberikan proteksi pada keamanan data guna menjaga dan meningkatkan keamanan data pada *file text* sehingga tidak dapat disebar luaskan oleh pihak yang tidak bertanggung jawab dan untuk mengatasi permasalahan ciphertext tunggal sehingga tidak mudah untuk dipecahkan.

2. METODE PENELITIAN

Penelitan ini akan mengimplementasikan kombinasi algoritma Bacon Cipher dan algoritma ROT128 yang merupakan pengembangan dari algoritma ROT13. Kombinasi antara kedua algoritma dalam penelitan ini bertujuan untuk mendapatkan *ciphertext* yang lebih kuat sehingga sulit untuk dipecahkan, sehingga dengan menggunakan perpaduan dua algoritma ini, dapat mengoptimalkan proteksi keamanan data. Kombinasia antara kedua algoritma ini juga akan mengatasi penggunaan *ciphertext* tunggal yang secara komparatif lemah [8], [9].

2.1 Algoritma Bacon Cipher

Bacon's cipher merupakan salah satu teknik steganografi yang klasik, unik, namun tidak terlalu umum diketahui orang. Walaupun namanya menyiratkan kriptografi (cipher), namun Bacon's cipher merupakan teknik steganografi. Bacon's cipher diciptakan oleh Sir Francis Bacon pada sekitar abad 16. Namun keberadaannya serta pembahasannya baru mencuat pada akhir abad 19. Bacon's cipher telah menyembunyikan banyak rahasia pada masanya. Pada dasarnya, teknik steganografi dengan menggunakan Bacon's cipher tidaklah terlalu rumit. Teknik steganografi menggunakan cara baconian berpusat pada tabel 1.

Tabel 1. Konversi Alphabet Pada Bacon Cipher

Karakter	Kode	Karakter	Kode	Karakter	Kode
A	AAAAA	j	ABAAB	S	BAABA
B	AAAAB	k	ABABA	T	BAABB
C	AAABA	l	ABABB	U	BABAA
D	AAABB	m	ABBAA	V	BABAB
E	AABAA	n	ABBAB	W	BABBA
F	AABAB	o	ABBBA	X	BABBB
G	AABBA	p	ABBBB	Y	BBAAA
H	AABBB	q	BAAAA	Z	BBAAB
I	ABAAA	r	BAAAB	Spasi	BBBAA

Dapat dilihat bahwa korespondensi dari huruf kolom karakter (a, b, c,) dengan kelompok huruf di kolom kode tidak terlalu menjelaskan apa makna Bacon's cipher. Tabel 1 ini akan lebih mudah dipahami bila dalam bentuk bilangan biner seperti yang disajikan pada tabel 2. Tabel 2 adalah tabel yang digunakan pada variasi Bacon's cipher [7].

Tabel 2. Konversi Alphabet ke Biner pada Bacon Cipher

Karakter	Biner	Karakter	Biner	Karakter	Biner
a	00000	J	01001	s	10010
b	00001	k	01010	t	10011

c	00010	l	01011	u	10100
d	00011	m	01100	v	10101
e	00100	n	01101	w	10110
f	00101	o	01110	x	10111
g	00110	p	01111	y	11000
h	00111	q	10000	z	11001
i	01000	r	10001	spasi	11100

Dasar dari steganografi menggunakan Bacon's cipher adalah dengan menggantikan atau melambangkan sebuah alphabet dengan sebuah deretan huruf yang dapat juga dianalogikan dengan bilangan biner 0 dan 1. Satu kelompok bilangan biner yang terdiri dari 5 digit angka ini akan merepresentasikan bagaimana huruf akan digambarkan, apakah huruf kapital atau huruf kecil [10], [11]. Berikut ini akan dicontohkan cara menyisipkan pesan dengan menggunakan Bacon's Cipher, misalkan terdapat sebuah pesan (plaintext) yang akan disamarkan, yaitu:

Pesan (plaintext): rahasia

Dengan menggunakan konversi alphabet pada tabel 3 akan diperoleh hasil yaitu dengan mengkodekan setiap huruf dari plaintext yang diganti dengan sekelompok lima huruf 'A' atau 'B' sehingga menjadi:

r = BAAAB
a = AAAAA
h = AABBB
a = AAAAA
s = BAABA
i = ABAAA
a = AAAAA

Secara normal maka plaintext "rahasia" akan disamarkan menjadi:
Ciphertext: BAAAB AAAAA AABBB AAAAA BAABA ABAAA AAAAA

2.2 Algoritma ROT128

ROT13 (Rotate 13) merupakan turunan dari algoritma Caesar Cipher yang ditemukan dan digunakan oleh Julius Caesar pada tahun 50 SM dengan menggunakan kunci=13 [2], [12] Algoritma ROT13 merupakan salah satu algoritma kriptografi yang bekerja menyandikan pesan dengan cara mensubstitusikan sebuah karakter dengan 13 karakter sesudahnya [10] sehingga abjad "A" menjadi "N" dan sebaliknya abjad "N" menjadi "A" [11] ROT13 juga disebut "monoalfabetik cipher" [12] karena memilki sifat yaitu satu huruf di plaintext diganti dengan tepat satu huruf ciphertext. Misalnya plaintext dengan huruf "A" diganti dengan ciphertext huruf "N".

Algoritma ROT13 adalah enkripsi substitution cipher yang umum digunakan di sistem operasi UNIX [4], [13] yang banyak digunakan di forum-forum online, berfungsi untuk melindungi isi artikel yang memungkinkan hanya orang yang mempunyai hak yang bisa membacanya [4], [5] Keunikan dari algoritmaROT13 ialah baik untuk mengenkripsi maupun deskripsi suatu pesan. ROT13 memang tidak didesain untuk keaman tingkat tinggi. Algoritma ROT13 digunakan untuk menyelubungi isi dari artikel (posting) di usenet news (sistem diskusi Internet yang terdistribusi secara global). Sehingga hanya orang yang betul-betul ingin membaca dapat melihat isinya. Contoh penggunaan lain adalah untuk menutupi jawaban dari sebuah teka teki (puzzle) [5].

Tabel 3. Substitusi ROT128

1	2	3	4	5	…	…	…	124	125	126	127	128
Ü	Ā	ā	Ă	ă	…	…	…	{	|	}	~	ĝ
⬍	⬍	⬍	⬍	⬍	…	…	…	⬍	⬍	⬍	⬍	⬍
Ğ	ğ	Ġ	ġ	Ģ	…	…	…	û	ü	ý	þ	ÿ
129	130	131	132	133	…	…	…	252	253	254	255	256

Tabel 3 menunjukan pergeseran huruf alphabet yang dirancang menggunakan algoritma ROT128 dimana $K = 128$ yang artinya index huruf di geser sejauh 128 ke depan [14], [15]. Adapun secara matematis algoritma ROT128 dalam penyandian plaintext menjadi *chipertext* adalah dengan menggunakan persamaan:

$$C_i = E(P_i) = (P_i + 128)\ mod\ 256$$

Keterangan:

C_i : Ciphertext
E : Enkripsi
P_i : Plaintext
13 : Kunci (K)
$mod\ 256$: Operasi Modulus 256

3. HASIL DAN PENGUJIAN

3.1 Implementasi Sistem

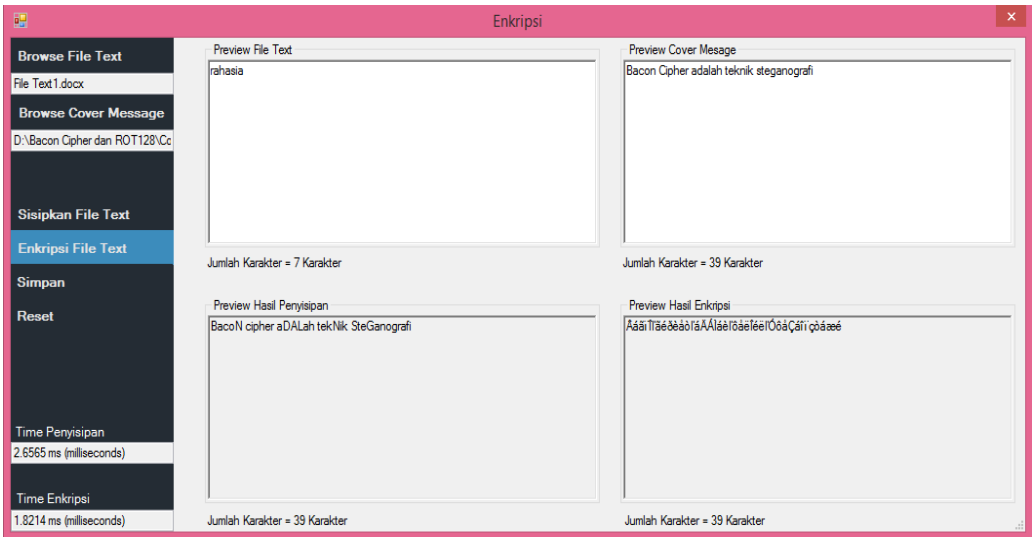
Implementasi sistem merupakan tahapan yang dilakukan setelah melewati tahapan analisis dan perancangan. Setelah selesai menganalisis dan membuat rancangan dari sistem yang akan dibangun, selanjutnya adalah mengimplementasikan hasil analisis dan perancangan ke dalam bentuk perangkat lunak dengan menggunakan bahasa pemrograman. Dalam penelitian ini bahasa pemrograman yang digunakan yaitu Visual C#.NET. Implementasi pada sistem ini dibuat berbasis desktop dalam lima halaman yaitu halaman awal halaman utama (home), halaman enkripsi, halaman dekripsi, halaman help, dan halaman about.

3.2 Pengujian Sistem

Tahap pengujian selanjutnya dilakukan dengan tujuan untuk menjamin sistem yang dibuat sesuai dengan hasil analisis dan perancangan serta menghasilkan satu kesimpulan apakah sistem tersebut sesuai dengan yang diharapkan. Untuk itu dibutuhkan sebuah metode pengujian yang menjadi ukuran atau parameter sehingga dapat ditarik kesimpulan bahwa sistem memang telah berjalan sesuai dengan tujuan. Metode pengujian yang digunakan adalah blackbox testing, yaitu sebuah metode yang digunakan untuk mendemonstrasikan fungsional aplikasi saat dioperasikan, apakah input diterima dengan benar dan output yang dihasilkan telah sesuai dengan yang diharapkan.

3.3 Pengujian Proses Penyisipan dan Enkripsi

Pengujian proses penyisipan dan enkripsi dilakukan untuk menguji apakah aplikasi yang telah dibuat dapat menyisipkan file text kedalam cover message menggunakan algoritma Bacon Cipher. Selanjutnya akan di enkripsi lagi dengan menggunakan algoritma ROT128 untuk memberikan proteksi ganda pada file text.



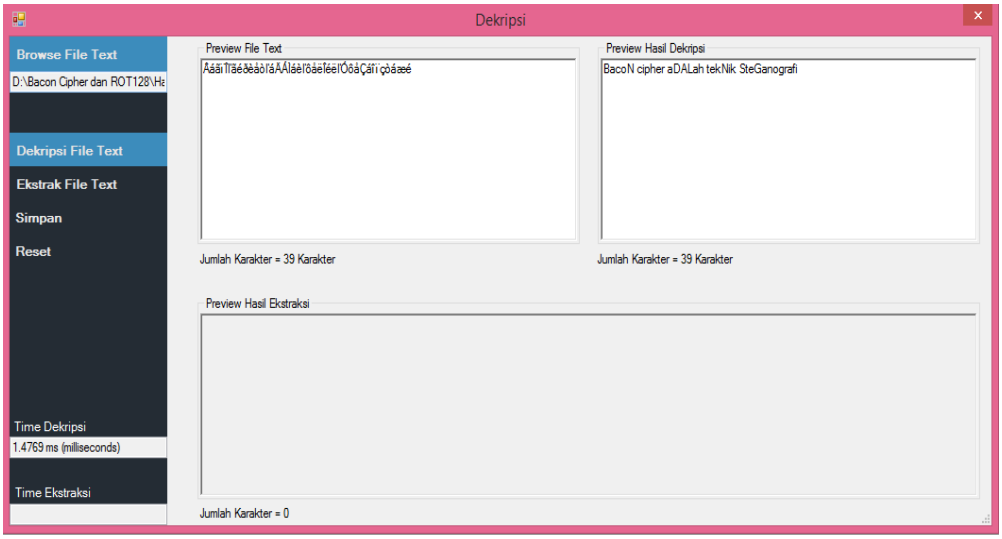
Gambar 2. Hasil Enkripsi File Text

Adapun proses hasil enkripsi masukkan file text dan masukkan cover massage lalu sisipkan file text ke dalam cover massage dan mengkenkripsi file text. Hasil penyisipan setelah melakukan proses enkripsi pada file text dari hasil penyisipan sebelumnya maka akan menghasilkan file text terenkripsi (ciphertext2) dengan menggunakan algoritma ROT128. Pada kasus pengujian ini, file text yang akan dienkripsi yaitu dengan rincian sebagai berikut:

Hasil penyisipan : BacoN cipher aDALah tekNik SteGanografi (39 karakter)
Hasil enkripsi : Âáãï Îľãéðèåòľá ÄÁÌáèľôåë Îéël'ÓôåÇáîïçòáæé
Waktu enkripsi : 1.82 ms (millisecond)

3.4 Pengujian Proses Dekripsi dan Ekstraksi

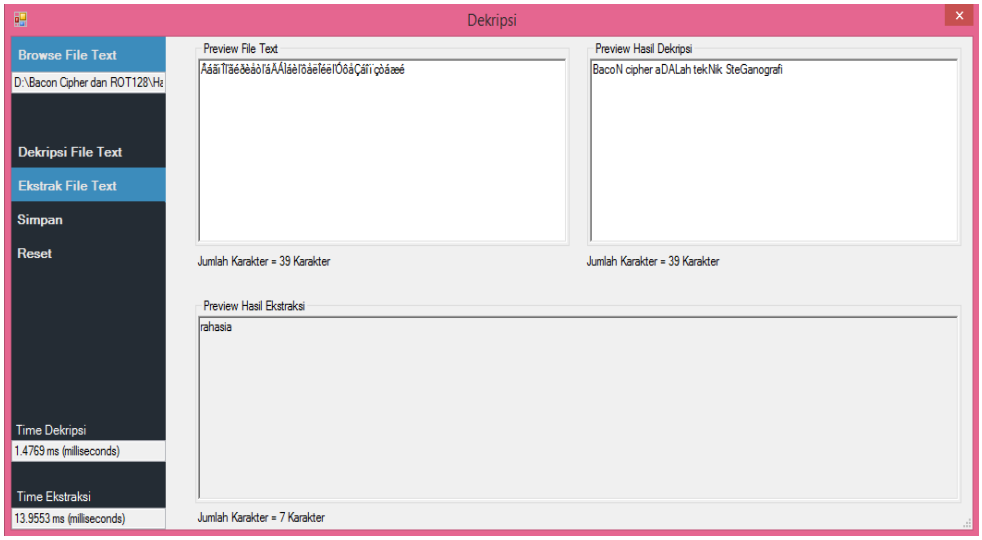
Pengujian proses dekripsi dan ekstraksi dilakukan untuk menguji apakah aplikasi yang telah dibuat dapat mengembalikan file text terenkripsi (ciphertext2) dengan algoritma ROT128. Selanjutnya akan diekstraksi lagi dengan algoritma Bacon Cipher untuk mendapatkan file text aslinya.



Gambar 3. Hasil Deskripsi File text

Adapun proses hasil Deskripsi masukkan file text hasil enkripsi lalu deskripsikan hasil enkripsi pada gambar 2. setelah melakukan proses dekripsi pada file text dari hasil penyisipan sebelumnya maka akan menghasilkan file text terdekripsi (ciphertext1) dengan menggunakan algoritma ROT128. Pada kasus pengujian ini, file text yang akan di dekripsi yaitu dengan rincian sebagai berikut:

File text : Âáãï Îľãéðèåòľá ÄÁÌáèľôåë Îéël'ÓôåÇáîïçòáæé
Hasil dekripsi : BacoN cipher aDALah tekNik SteGanografi (39 karakter)
Waktu dekripsi : 1.47 ms (millisecond)



Gambar 4. Hasil Ekstraksi File Text

Proses ekstraksi merupakan tahapan selanjutnya yang dilakukan setelah melakukan proses dekripsi dengan menggunakan algoritma ROT128. Proses ekstraksi berfungsi untuk mengekstraksi file text asli yang terdapat dalam file ciphertext1 dengan menggunakan algoritma Bacon Cipher. Pada halaman dekripsi, pilih tombol 'Ekstraksi File text' maka sistem akan menampilkan hasil ekstraksi beupa file text asli seperti terlihat pada gambar 4. Setelah melakukan proses ekstraksi pada file text hasil dekripsi (ciphertext1) dengan menggunakan algoritma Bacon Cipher akan menghasilkan file text asli dengan rincian sebagai berikut:

Hasil dekripsi : BacoN cipher aDALah tekNik SteGanografi (39 karakter)
Hasil ekstraksi : rahasia (7 karakter)
Waktu ekstraksi : 13.95 ms (millisecond)

3.5 Hasil Pengujian Sistem

Apabila dari input yang diberikan, proses dapat menghasilkan output yang sesuai dengan kebutuhan fungsionalnya, maka program yang dibuat sudah benar, tetapi apabila output yang dihasilkan tidak sesuai dengan kebutuhan fungsionalnya, maka masih terdapat kesalahan pada program tersebut, dan selanjutnya dilakukan penelusuran perbaikan untuk memperbaiki kesalahan yang terjadi. Adapun hasil dari pengujian sistem dengan menggunakan metode blackbox testing dapat diuraikan sebagai berikut:

a. Black Box Testing Penyisipan

Kasus dan hasil pengujian dari penyisipan file text pada halaman enkripsi dapat disajikan pada tabel 4. Pada tabel 4 berisi tabel blackbox testing penyisipan, kasus pengujian yang dilakukan antara lain "Input File Text", "Input Cover Message", dan "Sisipkan File Text". Hasil dari pengujian ini file text dapat disipkan kedalam cover message dan sistem akan menampilkan hasil penyisipan dengan status berhasil.

Tabel 4. Black Box Testing Penyisipan

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	*Input File Text*	menginputkan *file text* dengan memilih tombol "*Browse File Text*"	*file text* dapat di input sesuai dengan format file yang dipilih dan sistem akan menampilkan isi dan jumlah karakter *file text*	Valid
2	*Input Cover Message*	menginputkan *cover message* dengan memilih tombol "*Cover Message*"	*cover message* dapat di input sesuai dengan format file yang dipilih dan sistem akan menampilkan isi dan jumlah karakter dari *cover message*	Valid
3	Sisipkan *File Text*	menyisipkan *file text* kedalam *cover message* dengan memilih tombol "Sisipkan *File Text*"	*file text* dapat disisipkan kedalam *cover message* dan sistem akan menampilkan hasil penyisipan (*ciphertext1*) dan jumlah karakter dari *ciphertext1*	Valid

b. Black Box Testing Enkripsi

Kasus dan hasil pengujian dari enkripsi hasil penyisipan (ciphertext1) pada halaman enkripsi dapat disajikan pada tabel 5.

Tabel 5. Black Box Testing Enkripsi

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	Enkripsi *File Text*	mengenkripsi file hasil penyisipan (ciphertext1) dengan memilih tombol "Enkripsi File Text"	file ciphertext1 dapat dienkripsi dan sistem akan menampilkan hasil enkripsi (ciphertext2) dan juga jumlah karakter ciphertext2	Valid
2.	Simpan	menyimpan hasil enkripsi (ciphertext2) dengan memilih tombol "Simpan"	ciphertext2 dapat disimpan sesuai dengan format file yang ditentukan (.txt atau .docx)	Valid
3.	Reset	mereset inputan data dengan memilih tombol "Reset"	inputan data yang dimasukkan berhasil dikosongkan	Valid

Pada tabel 5 berisi tabel blackbox testing enkripsi, kasus pengujian yang dilakukan antara lain "Enkripsi File Text", "Simpan", dan "Reset". Hasil dari pengujian ini file text hasil penyisipan (ciphertext1) dapat dienkripsi dan sistem akan menampilkan hasil enkripsi (ciphertext2), ciphertext2 dapat disimpan sesuai dengan format file yang ditentukan (.txt atau .docx), dan inputan data yang dimasukkan berhasil dikosongkan dengan status berhasil.

c. Black Box Testing Dekripsi

Kasus dan hasil pengujian dari dekripsi hasil enkripsi (ciphertext2) pada halaman dekripsi dapat disajikan pada tabel 6.

Tabel 6. Black Box Testing Dekripsi

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	Input File Text	menginputkan file text dengan memilih tombol "Browse File Text"	file text dapat di input sesuai dengan format file yang dipilih dan sistem akan menampilkan isi dan jumlah karakter file text	Valid
2.	Dekripsi File Text	mendekripsi file hasil enkripsi (ciphertext2) dengan memilih tombol "Dekripsi File Text"	file ciphertext2 dapat didekripsi dan sistem akan menampilkan hasil dekripsi (ciphertext1) dan juga jumlah karakter ciphertext1	Valid

Pada tabel 6 berisi tabel blackbox testing dekripsi, kasus pengujian yang dilakukan antara lain "Input File Text" dan "Dekripsi File Text". Hasil dari pengujian ini file text hasil enkripsi (ciphertext2) dapat didekripsi dan sistem akan menampilkan hasil dekripsi (ciphertext1) dengan status berhasil.

d. Black Box Testing Ekstraksi

Kasus dan hasil pengujian dari ekstraksi hasil dekripsi (ciphertext1) pada halaman dekripsi dapat disajikan pada tabel 7.

Tabel 7. Black Box Testing Ekstraksi

No.	Kasus Uji	Langkah Uji	Hasil	Status
1.	Ekstraksi File Text	mengekstraksi file text hasil dekripsi (ciphertext1) dengan memilih tombol "Ekstraksi File Text"	ciphertext1 dapat di ekstraksi dan menampilkan hasil berupa file text asli dan jumlah karakter file text	Valid
2.	Simpan	menyimpan hasil ekstraksi dengan memilih tombol "Simpan"	file text asli dapat disimpan sesuai dengan format file yang ditentukan (.txt atau .docx)	Valid
3.	Reset	mereset inputan data dengan memilih tombol "*Reset*"	inputan data yang dimasukkan berhasil dikosongkan	Valid

Pada tabel 7 berisi tabel blackbox testing ekstraksi, kasus pengujian yang dilakukan antara lain "Ekstraksi File Text", "Simpan", dan "Reset". Hasil dari pengujian ini file text hasil dekripsi (ciphertext1) dapat ekstraksi dan sistem akan menampilkan hasil ekstraksi hasil berupa file text asli dan jumlah karakter file text serta dapat disimpan sesuai dengan format file yang ditentukan (.txt atau .docx), dan inputan data yang dimasukkan berhasil dikosongkan dengan status berhasil.

4. KESIMPULAN

Kombinasi Algoritma Bacon Cipher dan Algoritma ROT128 menghasilkan sebuah file teks yang berisi kata tersembunyi yang telah dienkripsi dan dideskripsi sehingga hanya pengguna dan penggirim saja yang dapat melihatnya. Kombinasi dua Algoritma ini menghasilkan kata acak untuk menyembunyikan file asli menggunakan tabel ASCII sehingga tidak mudah untuk dipecahkan. Penerapan kombinasi algoritma setganografi Bacon Cipher dan algoritma ROT128 dapat meningkatkan keamanan data dan mengatasi permasalahan pada penggunaan ciphertext tunggal.

DAFTAR PUSTAKA

[1] N. Wahyuningsih dan N. Janah, "Faktor-faktor Yang Mempengaruhi Kepuasan Nasabah Menggunakan Internet Banking Pada Bank Muamalat," *Al-Amwal J. Ekon. dan Perbank. Syari'ah*, vol. 10, no. 2, hal. 295, 2018, doi: 10.24235/amwal.v10i2.3596.

[2] R. M. Aresta, E. W. Pratomo, V. Geraldino, J. D. Santoso, dan S. Mulyatun, "Implementasi Multi Enkripsi Rot 13 Pada Symbol Whatsapp," *J. Inf. Syst. Manag.*, vol. 2, no. 1, hal. 1–5, 2020, doi: 10.24076/joism.2020v2i1.158.

[3] E. Sugiarto *dkk.*, "Securing Text Messages using the Beaufort-Vigenere Hybrid Method," *J. Phys. Conf. Ser.*, vol. 1577, no. 1, 2020, doi: 10.1088/1742-6596/1577/1/012032.

[4] E. R. Pramudya, M. B. Hatmi, A. Susanto, dan I. U. W. Mulyono, "Kombinasi Algoritma ROT13 Dan Vigenere Cipher Pada Alamat Directory File Untuk Keamanan Dokumen," *J. Semin. Nas. (SEMMNAS LPPM)*, hal. 548–555, 2020.

[5] F. Setiawan dan Fauziah, "Document Management System Menggunakan Kombinasi Algoritma ROT13 dan Algoritma String Matching," *J. Sains Komput. Inform.*, vol. 6, no. 1, hal. 126–135, 2022.

[6] D. R. I. M. Setiadi, C. Jatmoko, E. H. Rachmawanto, dan C. A. Sari, "Kombinasi Cipher Subtitusi (Beaufort Dan Vigenere) Pada Citra Digital," *Pros. SENDI_U*, vol. 7, no. 10, hal. 52–57, 2018, [Daring]. Tersedia pada: https://www.unisbank.ac.id/ojs/index.php/sendi_u/article/view/5960.

[7] Y. C. Milian dan W. Sulistyo, "Model Pengembangan Keamanan Data dengan Algoritma ROT 13 Extended Vernam Cipher dan Stream Cipher," *J. JTIK (Jurnal Teknol. Inf. dan Komunikasi)*, vol. 7, no. 2, hal. 208–216, 2023, doi: 10.35870/jtik.v7i2.716.

[8] Hendrik, "Kombinasi Algoritma Huffman dan Algoritma ROT 13 Dalam Pengamanan File Docx," *J. Inf. Syst. Res.*, vol. 2, no. 1, hal. 40–46, 2020.

[9] R. K. Hondro dan A. Fau, "PERANCANGAN APLIKASI PENYANDIAN TEKS DENGAN ALGORITMA ROT13 DAN TRIANGLE CHAIN CIPHER (TCC)," *J. Mahajana Inf.*, vol. 3, no. 2, hal. 41–56, 2018, [Daring]. Tersedia pada: http://e-journal.sari-mutiara.ac.id/index.php/7/article/view/416/393.

[10] M. Fadlan, S. Sinawati, Aida Indriani, dan Evi Dianti Bintari, "PENGAMANAN DATA TEKS MELALUI PERPADUAN ALGORITMA BEAUFORT DAN CAESAR CIPHER," *J. Tek. Inform.*, vol. 12, no. 2, 2019.

[11] N. A. Ramadhani dan I. Susilawati, "Penerapan Steganografi untuk Penyisipan Pesan Teks pada Citra Digital dengan Menggunakan Metode Least Significant Bit," *J. Multimed. Artif. Intell.*, vol. 4, no. 1, hal. 21–27, 2020.

[12] N. E. Saragih, "Aplikasi Pengamanan Pesan Dengan Algoritma Rot 13 Dan Steganografi End of File," *CSRID J.*, vol. 13, no. 3, hal. 13–22, 2021.

[13] D. Anggara, "Implementasi Metode Zig-Zag Chiper Dan ROT13 Untuk Kerahasiaan Basis Data," vol. 1, no. 3, 2023.

[14] M. M. Alnakhlani, Mukhtar, D. A. Himawanto, A. Alkurtehi, dan D. Danardono, "Effect of the bucket and nozzle dimension on the performance of a pelton water turbine," *Mod. Appl. Sci.*, vol. 9, no. 1, hal. 25–33, 2015, doi: 10.5539/mas.v9n1p25.

[15] M. Windriasari, M. Pd, S. P. Winarko, S. Pd, dan M. Ak, "JURNAL ANALISIS PENERAPAN METODE ACTIVITY BASED COSTING DALAM PENENTUAN HARGA POKOK PRODUKSI ROTI PADA UD . GANYSHA KEDIRI Oleh : Dibimbing oleh : SURAT PERNYATAAN ARTIKEL SKRIPSI TAHUN 2017," vol. 01, no. 01, 2017.