APLIKASI KRIPTOGRAFI RC4 UNTUK PENGAMANAN EMAIL BERBASIS WEB PADA PT. TITAN INFRA ENERGY

Rizky Fajar[1)], **Subandi** [2)]
[1]Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
[1,2]Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : 1411500034@student.budiluhur.ac.id [1)], subandionline@gmail.com[2)]

Abstrak

PT. Titan Infra Energy adalah perusahan yang bergerak dibidang industri pertambangan, semua informasi mengenai proses negosiasi dan penjualan dengan perusahaan lain yang mebutuhkan supply dari PT.Titan Infra Energy didistribusikan melalui email dan dikelola sendiri oleh setiap divisinya. Berdasarkan hal tersebut perusahaan membutuhkan suatu metode untuk menjaga keamanan email yang mengandung data atau informasi yang bersifat rahasia. Salah satu cara yang dapat dilakukan untuk melindungi informasi atau data adalah dengan menggunakan teknik enkripsi dan dekripsi. Oleh karena itu aspek keamanan dalam pertukaran informasi data sangatlah penting Terutama pada bidang pertambangan, dimana banyak data yang penting dan bersifat rahasia seperti data penjualan dan laporan keuangan. Karena begitu pentingnya data tersebut, maka dibutuhkan suatu metode yang dapat menjaga keamanan isi email tersebut. Algoritma yang akan digunakan adalah algoritma RC4. Hasil dari penelitian ini akan diimplementasikan dalam sebuah program aplikasi berbasis web yang dapat memberikan kemudahan bagi setiap orang yang akan mengamankan file-file penting.

Kata kunci: Kriptografi, Enkripsi, Dekripsi, *RC4, Email*

1. PENDAHULUAN

Kemajuan teknologi saat ini sangat mempermudah manusia untuk berkomunikasi satu dengan yang lainnya walaupun berbeda negara sekalipun. Pada zaman dahulu manusia berkomunikasi secara jarak jauh menggunakan cara yang konvensional, yaitu dengan cara surat menyurat. Pada zaman modern seperti ini dengan adanya internet, manusia dapat berkomunikasi jarak jauh dengan mudah menggunakan *email*, Dengan adanya internet manusia banyak mendapatkan dampak positif dan disayangkan terdapat dampak negatifnya juga dari kemajuan teknologi internet yaitu dengan adanya pencurian data informasi penting.

Masalah *security* dan *privacy* adalah aspek yang sangat penting. Pengiriman suatu pesan, data dan informasi yang sangat penting membutuhkan tingkat keamanan yang tinggi.

PT.Titan Infra Energy adalah perusahan yang bergerak dibidang industri pertambangan. Semua informasi mengenai proses negosiasi dan penjualan dengan perusahaan lain yang mebutuhkan *supply* dari PT.Titan Infra Energy didistribusikan melalui *email* dan dikelola sendiri oleh setiap divisinya. Berdasarkan hal tersebut perusahaan membutuhkan suatu metode untuk menjaga keamanan *email* yang mengandung data atau informasi yang bersifat rahasia.

Berdasarkan uraian diatas dapat disimpulkan dengan membuat suatu aplikasi pengamanan isi pesan yang akan dikirim menggunakan media *email* pada PT.Titan Infra Energy sehingga hanya orang yang bersangkutan yang dapat mengetahui isi dari pada informasi tersebut.

2. METODE PENELITIAN

Metode yang digunakan dalam penulisan laporan Tugas Akhir ini adalah metode pengembangan SDLC (*System Development Life Cycle*). SLDC merupakan metodologi klasik yang digunakan untuk mengembangkan, memelihara dan menggunakan sistem informasi. Metode ini menggunakan pendeketanan sistem yang disebut pendekatan air terjun (*waterfall approach*), yang menggunakan beberapa tahapan dalam mengembangkan sistem (Supriyanto, 2015). Adapun tahapan dalam SLDC (*System Development Life Cycle*) adalah sebagai berikut:

a. Tahap Perencanaan

Pada tahap ini adalah tahap awal dimana penulis akan mengumpulkan data berkaitan dengan metode yang akan digunakan untuk mempermudah pembuatan aplikasi.

b. Tahap Analisis sistem

Pada tahap ini akan dianalisa fungsi-fungsi apa saja yang diperlukan untuk mengimplementasikan aplikasi ini.

c. Tahap Perancangan

Pada tahap ini dilakukan perancangan tampilan aplikasi yang akan dibangun sesuai dengan kebutuhan aplikasi sehingga mempermudah dalam proses implementasi.

d. Tahap Penerapan/Implementasi

Pada tahap ini aplikasi akan diimplementasikan berdasarkan analisis sistem dan rancangan yang sudah dibuat.

e. Tahap Pengujian

Pada tahap ini dilakukan pengujian dan pengecekan, supaya aplikasi yang dibuat dapat berjalan sesuai dengan rancangan

3. LANDASAN TEORI

3.1. Kriptografi

Kriptografi telah dikenal kurang lebih pada tahun 2000 sebelum masehi oleh bangsa Mesir. Berbentuk tulisan *heiroglyphic* pada monumen. Bangsa *Mesopotania* telah menggunakan kriptografi pada tahun 1500 sebelum masehi, selanjutnya dikenal juga oleh bangsa Yahudi dan bangsa Yunani. Teknik kriptografi pada awalnya dilakukan dengan cara menggunakan simbol tertentu untuk mengganti simbol yang telah digunakan dan dikenal secara umum oleh masyarakat. Kriptografi merupakan ilmu dan seni untuk menjaga pesan agar aman [1].

3.2. Definisi Kriptografi

Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang hanya memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan. Dalam kriptografi, data atau pesan yang dikirimkan melalui jaringan akan disamarkan sedemikian rupa. Sehingga seandainya data tersebut bisa diperoleh dan dibaca oleh orang lain, maka pihak yang tidak berhak atau berwenang tersebut tidak akan bisa mengerti arti dari data tersebut [2].

Dalam bidang kriptografi terdapat dua konsep yang sangat penting atau utama yaitu enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi atau data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Sebuah pesan atau data yang masih asli dan belum mengalami penyandian dikenal dengan istilah *plaintext*. Kemudian setelah disamarkan dengan suatu cara penyandian, maka *plaintext* ini disebut sebagai *ciphertext*. Proses penyamaran dari *plaintext* ke *ciphertext* disebut enkripsi (*encryption*), dan proses pengembalian dari *ciphertext* menjadi *plaintext* kembali disebut dekripsi (*decryption*) [3]

Kekuatan algoritma yang digunakan untuk proses enkripsi dan dekripsi berhubungan erat dengan penggunaan persamaan matematika. Semakin banyak dan rumit perhitungan dari persamaan matematika yang digunakan maka data sandi semakin aman. Pemanfaatan kecepatan dan ketelitian dari kerja komputer sangat membantu untuk proses ini. Kerahasiaan kunci adalah bagaimana cara kunci tersebut disimpan dan didistribusikan kepada pihak yang berhak menerima data, karena kunci ini akan digunakan untuk melakukan dekripsi. Semakin rapih kunci disimpan dan didistribusikan maka data sandi semakin aman [4].

3.3. Tujuan Kriptografi

Untuk meningkatkan keamanan informasi (*information security*) setelah dilakukan proses pengiriman dan penerimaan informasi maka dapat dilakukan tindakan-tindakan berikut ini:

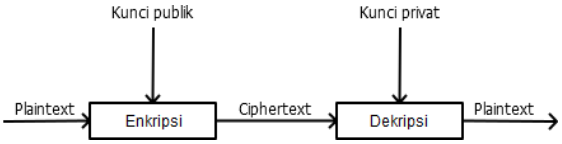
1) Membuktikan keaslian (*authentication*) yaitu proses yang memungkinkan penerima informasi untuk mengetahui asal atau pengirim informasi yang sebenarnya. Bertujuan mencegah pengacau yang mengirimkan informasi menggunakan identitas orang lain.
2) Menjaga integritas data (*data integrity*) yaitu proses yang menjamin penerima informasi dapat memeriksa apakah informasi telah berubah sebelum diterimanya. Berubah karena secara sengaja dipalsukan oleh pihak lain atau secara tidak disengaja karena terjadi kerusakan pada proses pengiriman informasi.
3) Membuktikan seseorang telah mengirimkan pesan (*nonrepudiation*) yaitu proses untuk menjamin pengirim informasi tidak dapat menyangkal bahwa dia telah mengirim informasi tersebut. Sebaliknya dapat juga digunakan untuk melindungi seseorang dari tuduhan yang menyatakan bahwa dia telah mengirimkan informasi padahal tidak.
4) Menjaga kerahasiaan (*confidentiality*) yaitu proses untuk menjamin informasi yang dikirimkan tidak dapat dipahami isinya oleh orang yang tidak berhak.

3.4. Algoritma RC4

RC4 didesain oleh Ron Rivest yang berasal dari *RSA Security* pada tahun 1987. RC4 sendiri mempunyai singkatan resmi yaitu "*Rivest Cipher*", namun juga dikenal sebagai "*Ron's Code*" RC4 sebenarnya dirahasiakan dan tidak dipublikasikan kepada khalayak ramai, namun ternyata ada orang yang tidak dikenal menyebarkan RC4 ke *mailing list Cypherpunks*. Kemudian berita ini dengan cepat diposkan ke *sci.crypt newsgroup*, dan kemudian menyebar luas diinternet. Kode yang dibocorkan tersebut dipastikan keasliannya karena *output* yang dikeluarkan sama dengan software-software yang menggunakan RC4 yang berlisensi. Nama RC4 sudah dipatenkan, sehingga RC4 sering disebut juga *ARCFOUR* atau *ARC4* (*Alleged RC4*) untuk menghindari masalah pematenan. *RSA Security* tidak pernah secara resmi merilis algoritma tersebut, namun Rivest secara pribadilah yang merilisnya dengan menghubungkan *Wikipedia* Inggris ke catatan-catatan yang ia punya. RC4 telah menjadi bagian dari protokol enkripsi yang standard dan sering digunakan, termasuk *WEP* dan *WPA* untuk *wireless card*, serta *TLS*. Faktor utama yang menjadi kesuksesan dari RC4 adalah kecepatannya dan kesederhanaannya dalam menangani banyak aplikasi, sehingga mudah untuk mengembangkan implementasi yang efisien ke *software* dan *hardware* [5].

3.5. Kriptografi Kunci Asimetris

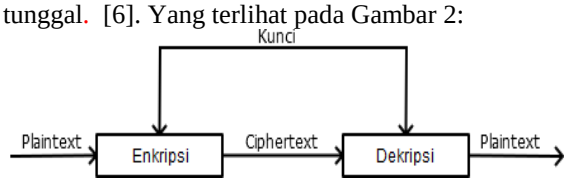
Kriptografi kunci asimetris yang sering disebut juga kriptografi kunci. Algoritma asimetri ini disebut kunci publik karena kunci untuk enkripsi dapat dibuat publik yang berarti semua orang boleh mengetahuinya. Sembarang orang dapat menggunakan kunci enkripsi tersebut untuk mengenkrip pesan namun hanya orang tertentu yaitu calon penerima pesan dan sekaligus pemilik kunci dekripsi yang merupakan pasangan kunci publik, yang dapat melakukan dekripsi terhadap pesan tersebut. Dalam sistem ini, kunci enkripsi disebut kunci publik, sementara kunci dekripsi sering disebut kunci privat [6]. Yang terlihat pada Gambar 1:



Gambar 1. Kunci Asimetris

3.6. Kriptografi Kunci Simetris

Disebut juga sebagai kriptografi konvensional. Kriptografi simetris adalah algoritma kriptografi yang menggunakan kunci enkripsi yang sama dengan kunci dekripsinya. Kriptografi simetris sering disebut sebagai algoritma kunci rahasia, algortima kunci tunggal. [6]. Yang terlihat pada Gambar 2:



Gambar 2. Kunci Simetris

Algoritma simetris terbagi menjadi 2, yaitu:

a) *Stream Cipher*

Secara garis besar *stream cipher* adalah yang unit atau data pada umumnya sebuah *byte* atau bahkan terkadang *bit*. Dengan cara ini enkripsi atau dekripsi dapat dilaksanakan pada variable panjang.

b) *Block Cipher*

Block cipher beroperasi dengan rangkaian bit-bit plaintext yang dibagi menjadi blok-blok bit dengan besar yang sama. Algoritma enkripsi menghasilkan blok *ciphertext* yang berukuran sama dengan blok plaintextnya. Blok *plaintext* akan menghasilkan blok *ciphertext* yang sama apabila dienkripsi menggunakan kunci yang sama. Hal ini berbeda dengan *stream cipher* dimana bit-bit *plaintext* akan menghasilkan bit-bit *ciphertext* yang berbeda setiap kali dienkripsi.

4. HASIL DAN PEMBAHASAN

4.1. Hardware dan Software

Dalam pembuatan aplikasi ini, perangkat keras (*hardware)* dan lunak (*software*) yang digunakan adalah:

Tabel 1. Perangkat keras *(Hardware)*

No	Perangkat	Kebutuhan
1	Processor	Intel® Core™ i3-6006U 2.0GHz
2	Ram	DDR3 4GB
3	Harddisk	SATA 1TB
4	Display	14.0” 1366 x 768

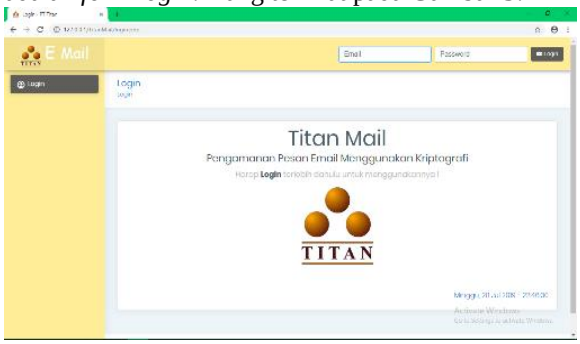
Tabel 2. Perangkat lunak *(Software)*

No	Kebutuhan
1	Microsoft Windows 10 Pro
2	Microsoft Office 2013
3	Notepad ++ v7.6.4
4	Google Chrome v75.0.3770.100
5	XAMPP v3.2.2
6	Balsamiq Mockups v3.5.15
7	Microsoft Visio v14.0

4.2. Tampilan Program

1) Tampilan Layar *Form Login*

Tampilan layar yang pertama kali akan muncul adalah *form login.* Yang terlihat pada Gambar 3:



Gambar 3. Tampilan Layar Form Login

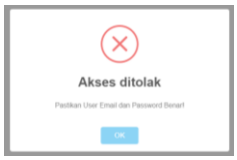
Jika *email* dan *password* tidak diisi, maka akan muncul pesan seperti Gambar 4:

Gambar 4. Tampilan Layar Form Login

Jika *email* dan *password* yang digunakan valid dan sudah diizinkan maka akan tampil pesan seperti Gambar 5, kemudian pengguna akan diarahkan ke *form* selanjutnya.

Gambar 5. Tampilan Pesan Berhasil Login

Jika *email* atau *password* yang digunakan salah atau belum diizinkan maka akan tampil pesan seperti Gambar 6:



Gambar 6. Tampilan Pesan Gagal Login

2) Tampilan Layar *Form Home*

Tampilan layar *form home* ini merupakan tampilan menu utama dari aplikasi setelah pengguna berhasil *login*. Didalam *form home* terdapat terdapat beberapa *form* seperti *form send mail, form inbox, form help* dan *form about,* yang terlihat pada Gambar 7:

Gambar 7. Tampilan Layar Form Home

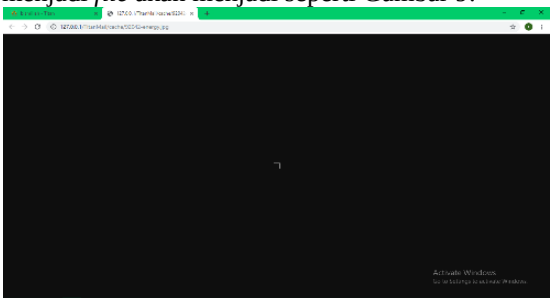
4.3. Pengujian Aplikasi

Dalam melakukan pengujian penulis memanfaatkan beberapa berkas *file* dokumen sebagai data yang akan disisipkan dalam *file*. Berkas – berkas yang akan digunakan tersebut adalah:

1) Proses Enkripsi pada *File *.jpg*

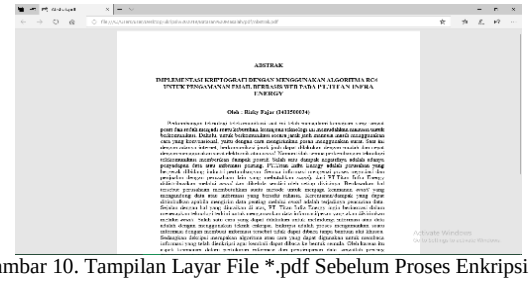
Gambar 8. Tampilan Layar File *.jpg Sebelum Proses Enkripsi

Setelah dilakukan proses enkripsi maka *file* akan menjadi *file* akan menjadi seperti Gambar 9:



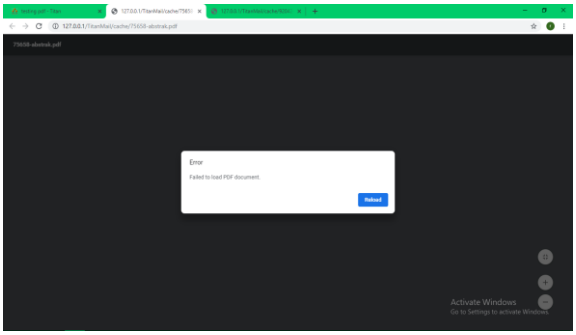
Gambar 9. Tampilan Layar File *.jpg Hasil Proses Enkripsi

2) Proses Enkripsi pada *File *.pdf*



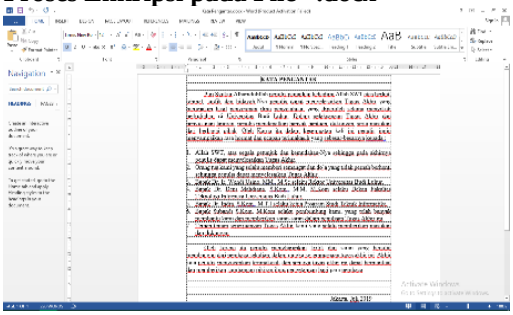
Gambar 10. Tampilan Layar File *.pdf Sebelum Proses Enkripsi

Setelah dilakukan proses enkripsi maka *file* akan menjadi tidak terbaca karena file extensi sudah berubah, *file .pdf* tersebut dibuka dengan menggunakan *pdf reader*, yang terlihat pada Gambar 11:



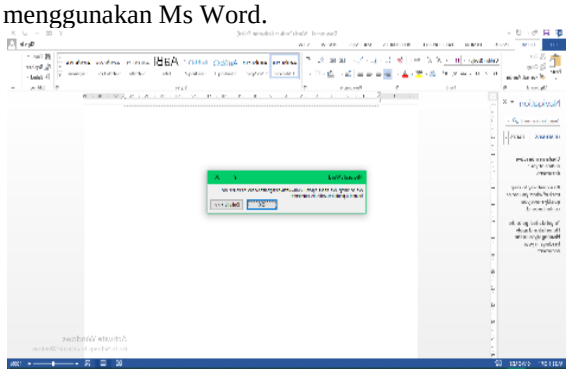
Gambar 11. Tampilan Layar File *.pdf Sesudah Proses Enkripsi

3) Proses Enkripsi pada File *.docx



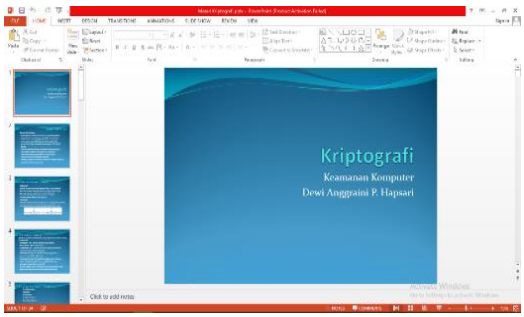
Gambar 12. Tampilan Layar File .docx Sebelum Proses Enkripsi

Setelah dilakukan proses enkripsi maka *file* akan menjadi tidak terbaca karena file extensi sudah berubah, *file .docx* tersebut dibuka dengan menggunakan Ms Word.



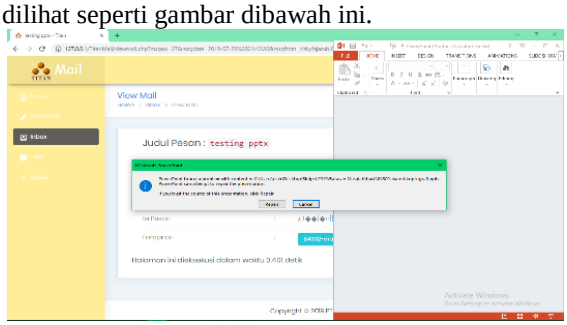
Gambar 13. Tampilan Layar File .docx Sesudah Proses Enkripsi

4) Proses Enkripsi pada File *.pptx



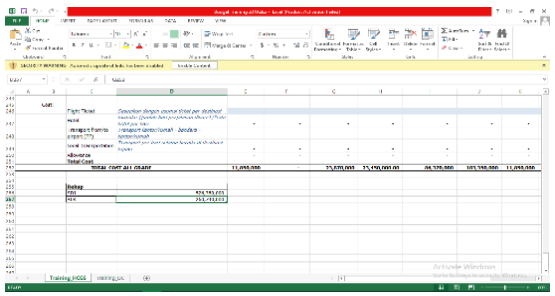
Gambar 14. Tampilan Layar File .pptx Sebelum Proses Enkripsi

Setelah dilakukan proses enkripsi maka *file* akan berubah ekstensi dan tidak bisa di baca, *file .pptx* yang telah dienkripsi tersebut dibuka dengan menggunakan *ms. Power Point*. Hasil nya dapat dilihat seperti gambar dibawah ini.



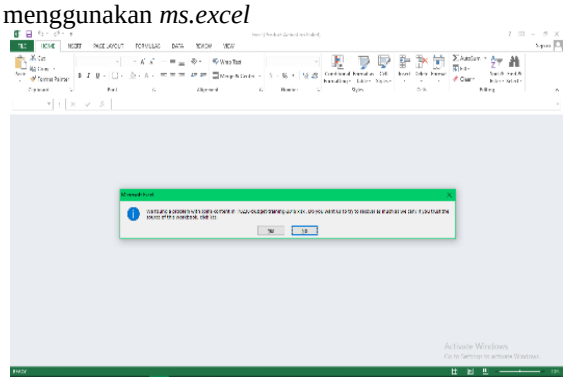
Gambar 15. Tampilan Layar File .pptx Hasil Proses Enkripsi

5) **Proses Enkripsi pada Dokumen *File *.xlsx***



Gambar 16. Tampilan Layar File .xlsx Sebelum Proses Enkripsi

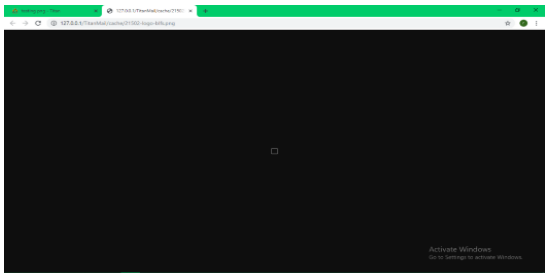
Setelah dilakukan proses enkripsi maka *file* akan menjadi teracak dan sulit dipahami, *file .xlsx* yang telah dienkripsi tersebut dibuka dengan menggunakan *ms.excel*



Gambar 17. Tampilan Layar File .xlsx Setelah di Enkripsi

6) Proses Enkripsi pada File *.png

Gambar 18. Tampilan Layar File .png Sebelum Proses Enkripsi



Gambar 19. Tampilan Layar File .png Sesudah Proses Enkripsi

4.4. Tabel Hasil Uji Coba Program

Tabel 3. Hasil Proses Enkripsi dan Dekripsi pada file .Docx

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	Kata Pengantar.docx	15	5.548	0.709	15	15
2	Proposal.docx	116	7.456	1.064	116	116
3	Abstrak.docx	3567	9.798	2.745	3567	3567

Tabel 4. Hasil Proses Enkripsi dan Dekripsi pada file .Xlsx

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	Budget Training 2019	76	9.128	2.995	76	76
2	Budget TMDP II Program 2019	37	7.348	1.185	37	37
3	Budget Training SLR SDJ 2019 Final	81	9.879	3.154	81	81

Tabel 5. Hasil Proses Enkripsi dan Dekripsi pada file .Pptx

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	Materi Kriptografi	139	13.304	5.563	139	139
2	dokumen.tips_ppt-kebersihan-lingkungan	1702	20.567	7.278	1702	1702
3	TEKNOLOGI INFORMASI	62	5.568	2.311	62	62

Tabel 6. Hasil Proses Enkripsi dan Dekripsi pada file .Pdf

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	Kata Pengantar	108	11.149	4.337	108	108
2	DAFTAR PUSTAKA	283	14.667	5.556	283	283
3	Abstrak	63	7.344	2.112	63	63

Tabel 7. Hasil Proses Enkripsi Dan Dekripsi .Jpg

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	energy	25	37.537	1.148	25	25
2	Logo Budi Luhur	20	35.678	1.087	20	20
3	Logo Budi Luhur	18	32.334	1.053	18	18

Tabel 8. Hasil Proses Enkripsi dan Dekripsi pada file .Png

No	Nama	Ukuran File (kb)	Waktu Proses		Ukuran File Setelah (kb)	
			Enkrip	Dekrip	Enkrip	Dekrip
1	logo BLFS	231	19.662	5.906	231	231
2	Logo BL	113	15.413	4.678	113	113
3	PT. Titan	37	7.543	2.678	37	37

5. DAFTAR PUSTAKA

[1] Elka. L. H, Khairil, & Ferry, H, U. (2014). Aplikasi Enkripsi Dan Deskripsi Data Menggunakan Algoritma RC4. *Jurnal Media Infotama*, 10(1), pp. 1–7.

[2] Harni K., Satya D., et al. (2018). Penerapan Algoritma Rivert Code 4 (RC4) Pada Aplikasi kriptografi Dokumen. *PETIR(Jurnal dan Penerapan Teknik Informatika)*, 11(1), pp. 38–47.

[3] Jumrin, Sutardi, S (2016). Aplikasi Sistem Keamanan Basis Data Dengan Teknik Kriptografi RC4. *semanTIK*, 2(1), pp.59–64.

[4] Dani, I. (2018). *Pengamanan Data Teks Dengan Algoritma Modifikasi RC4*. Pelita Informatika: Informasi dan Informatika, 6(3), pp. 309–312.

[5] Rizal, Y. R.,Yuli C, & Imam. S. (2016). Shamir Adleman, dan Metode Steganografi Untuk Pengamanan Pesan Rahasia Pada Berkas Teks Digital, Transient, 5(1), pp. 86-91.

[6] Halim, A & Budiman (2015). *Implementasi affine Chiper dan RC4 Pada Enkripsi File Tunggal*. *Prosiding SNATIF Ke*-2, Fakultas Teknik Universitas Maria Kudus, (September), pp. 243-250.

[7] Aldi, Y, dan Noni, J. (2018). Aplikasi kriptografi menggunakan algoritma RC4 dan des untuk mengamankan pesan email. *Jurnal Skanika*, 1(2), pp. 491–497.

[8] Hendrawati, Hamdani, Awang, H, K. (2014). Keamanan Data Dengan Menggunakan Algoritma Rivest Code 4 (RC4) dan Steganografi Pada Citra Digital. *Informatika Mulawarman: Jurnal Ilmiah Ilmu Komputer*, 9(1), pp. 6-12.

[9] Kurniadi, Irwansyah, F. (2015). Penerapan Algoritma RC4 Untuk Enkripsi Keamanan Data (Studi Kasus: Dinas Pendidikan dan Kebudayaan Kota Sekayu), *Jurnal Ilmiah R & B*, (12), pp.1-13

[10] Murni. M. (2015). Implementasi Sistem Pengamanan Data Barang Pada PT.Matahari Putra Prima, *Jurnal Mantik Penusa*, 18(2), pp. 1-10.