SISTEM ENKRIPSI DOKUMEN MENGGUNAKAN METODE RC4 DAN BASE64 PADA JUSTICIA LAW FIRM & ASSOCIATES

Rizky Tegar Fahruroji[1], Dyah Rhetno Wardhani[2], Fery Rahmawan[3]

Universitas Indraprasta PGRI
Jl. Raya Tengah Kelurahan Gedong, Pasar Rebo, Jakarta Timur 13760
[1]tegar@gar.my.id, [2]dyahrhetno@gmail.com, [3]ferytijany489@gmail.com

ABSTRAK

Justicia Law Firm & Associates menyimpan semua dokumen digital termasuk yang bersifat rahasia pada *network file sharing* dengan protokol *Server Message Block* (SMB). Menyebarnya ancaman WannaCry Ransomware pada tahun 2017 menyebabkan protokol SMB menjadi kurang aman, oleh sebab itu data perlu disimpan menggunakan enkripsi agar lebih aman. Metode yang digunakan adalah Rivest Cipher 4 (RC4) dan Base64 sebagai encode/decode. Pada penelitian ini dihasilkan sistem enkripsi menggunakan metode RC4 dan Base64 sebagai solusi dari permasalahan keamanan data Justicia Law Firm & Associates. Sistem enkripsi mendukung hampir semua ekstensi yang umum digunakan untuk dokumen perusahaan oleh Justicia Law Firm & Associates, yaitu .xlsx, .xls, .doc, .docx, .zip, .rar, .pdf, .jpg, .jpeg, dan .png. Karena menggunakan basis web, maka sistem ini dapat diakses menggunakan sistem operasi apapun selama memiliki GUI *(Graphical User Interface)* dan akses internet. File yang dienkripsi mengalami peningkatan ukuran sebesar 33% karena melalui proses encoding Base64, dan setelah didekripsi ukuran file menjadi semula seperti file asli.
Kata Kunci : kriptografi, Rivest Cipher 4 (RC4), enkripsi, keamanan data.

ABSTRACT

Justicia Law Firm & Associates stores all digital documents, including confidential ones, on a network file sharing using the Server Message Block (SMB) protocol. The spread of the WannaCry Ransomware threat in 2017 resulted in the SMB protocol becoming less secure; therefore, data needs to be stored using encryption for increased security. The methods utilized are Rivest Cipher 4 (RC4) and Base64 for encoding/decoding. This research yields an encryption system using RC4 and Base64 as a solution to Justicia Law Firm & Associates' data security issues. The encryption system supports nearly all common file extensions used for company documents, such as .xlsx, .xls, .doc, .docx, .zip, .rar, .pdf, .jpg, .jpeg, and .png. Since it operates on a web-based platform, the system can be accessed using any operating system with a Graphical User Interface (GUI) and internet access. Encrypted files experience a 33% increase in size due to the Base64 encoding process, but after decryption, the file size returns to its original state as the original file.
***Key Word** : cryptograph, Rivest Cipher (RC4), encryption, data security.*

PENDAHULUAN

Setiap perusahaan memiliki dokumen digital yang bersifat rahasia. Karena sifatnya yang rahasia, maka dokumen digital tersebut haruslah dijaga dan diamankan sehingga meminimalisir terjadinya kebocoran data. Berdasarkan hasil observasi peneliti secara langsung terungkap bahwa Justicia Law Firm & Associates menyimpan semua dokumen digital termasuk yang bersifat rahasia pada network file sharing dengan protokol *Server Message Block* (SMB). SMB adalah protokol client-server yang digunakan untuk berbagi *file* dan direktori, mengekspor printer dan port serial, serta menyediakan abstraksi komunikasi untuk *named pipe* dan *mail slo*t yang dapat diakses secara remote di berbagai komputer (Arjun Shajit dkk., 2016:22). Protokol SMB dipilih sebagai metode *sharing file* dengan alasan kemudahan dalam operasionalnya. Walaupun mudah, adanya ancaman pada protokol SMB seperti WannaCry Ransomware yang pada tahun 2017 menyebabkan protokol SMB menjadi kurang aman. WannaCry Ransomware adalah jenis perangkat lunak berbahaya yang mengunci perangkat menggunakan enkripsi hingga korban membayar uang tebusan sebagai tebusan untuk kunci dekripsi agar dapat mengakses kembali data yang dikunci (Mohurle & Patil, 2017: 1938). Selain itu, dokumen yang tersimpan tidak memiliki pengamanan apapun, sehingga hanya dengan mengetahui alamat file sharing maka siapapun dapat mengaksesnya. Hal ini yang mendorong peneliti untuk meneliti dan juga mengembangkan sistem enkripsi dokumen

menggunakan metode enkripsi RC4 dan Base64 pada Justicia Law Firm & Associates. Justicia Law Firm & Associates adalah firma hukum yang memfokuskan diri dalam penanganan hukum perusahaan, terutama untuk foreign direct investment di Indonesia. Mereka menyajikan informasi yang akurat dan dapat diandalkan untuk klien demi memastikan bahwa mereka terinformasi dengan benar saat membuat keputusan untuk praktik bisnis dan operasi mereka. Justicia Law Firm & Associates juga menyediakan layanan litigasi dan hukum perusahaan berkualitas tinggi, serta memberikan nasihat hukum untuk perusahaan patungan/joint venture ataupun merger/akuisisi.

Justicia Law Firm & Associates memiliki pengalaman mendalam dalam memberikan nasihat hukum untuk perusahaan skala menengah dan besar dalam bidang hukum perusahaan (seperti diantaranya lisensi bisnis dan juga *merger* & akuisisi), hukum karyawan, dan penyelesaian sengketa dengan firma hukum internasional terkemuka, serta perusahaan nasional besar. Meskipun sistem dan regulasi hukum di Indonesia sangat dinamis dan agresif terutama pada bidang hukum perusahaan, Justicia Law Firm & Associates akan memberikan panduan bagi klien mereka melalui sistem hukum Indonesia (Justicia Law Firm & Associates, 2023).

Penelitian mengenai sistem enkripsi menggunakan metode RC4 sudah pernah dilakukan oleh peneliti-peneliti sebelumnya. Pada penelitian Uli Sholihah Saragih tahun 2017 dengan judul Implementasi Enkripsi Dan Dekripsi Dengan Metode RC4 Untuk Pengamanan Data Sistem Informasi menghasilkan sistem yang dapat mengenkripsi *database* pada sistem informasi mahasiswa Jurusan Ilmu Komputer Fakultas MIPA Universitas Lampung (Uli Sholihah Saragih, 2017). Penelitian lain dilakukan oleh Muhammad Rifki Adnan pada tahun 2022 dengan judul Pengamanan Data Laporan Keuangan Menggunakan Metode RC4 Pada Reddog Cabang Gading Serpong. Pada penelitian tersebut menghasilkan sistem enkripsi dokumen berbasis web menggunakan PHP dan MySQL.

Berdasarkan uraian di atas, peneliti memutuskan untuk merancang sistem enkripsi dokumen menggunakan metode RC4 dan Base64 pada Justicia Law Firm & Associates. RC4 sendiri merupakan kepanjangan dari Ronald Code atau Rivest's Cipher. Menurut Sumarno (dalam Adnan, 2022:10), RC4 *stream cipher* ini merupakan salah satu jenis algoritma yang mempunyai S-Box dan menggunakan variabel yang panjang kuncinya 1 sampai 256 bit yang digunakan untuk menginisialisasikan tabel sepanjang 256 bit. Algoritma Base64 merupakan salah satu algoritma untuk *encoding* dan *decoding* dengan bilangan dasar 64 (Afrianto & Taliasih, 2020). Dengan keberadaan sistem ini diharapkan masalah yang berhubungan dengan keamanan dokumen akan tertangani.

METODE PENELITIAN

Peneliti memilih Justicia Law Firm & Associates sebagai lokasi penelitian. Adapun alasan peneliti memilih Justicia Law Firm & Associates adalah karena Justicia Law Firm & Associates merupakan perusahaan tempat peneliti pernah bekerja sebelumnya. Hal ini memudahkan peneliti untuk melaksanakan penelitian karena peneliti mendalami keadaan lokasi penelitian. Meskipun begitu, informasi yang dikumpulkan dan diolah harus tetap obyektif dan tidak dipengaruhi oleh pendapat peneliti sendiri. Waktu yang dipakai adalah bulan Maret sampai dengan Juni tahun 2023.
Peneliti melakukan tahap persiapan mulai minggu ke-3 April sampai dengan minggu ke-2 Mei 2023 dengan menyusun proposal, pengurusan perizinan dan menyusun instrumen yang dibutuhkan. Kemudian dilanjutkan dengan tahap pelaksanaan dengan melakukan pengumpulan data, analisis data yang didapat dan merumuskan hasil penelitian. Lalu tahap penyelesaian dengan menyelesaikan kerangka laporan, penulisan laporan, revisi dan penyuntingan laporan dan penyelesaian laporan.

Peneliti dalam mengumpulkan data melakukan observasi secara langsung pada Justicia Law Firm & Associates. Selain itu peneliti juga melakukan wawancara tidak terstruktur kepada karyawan Justicia Law Firm & Associates.
Berdasarkan data yang diperoleh, peneliti mendapat fakta bahwa :

a. Dokumen perusahaan disimpan pada file sharing menggunakan protokol SMB.

b. Dokumen tersimpan tanpa keamanan berarti.
c. Kekhawatiran akan pencurian dan penguncian data seperti pada kasus WannaCry pada tahun 2017.
d. Siapapun yang mengetahui alamat file sharing dapat mengaksesnya.

Untuk mengatasi permasalahan di atas, peneliti melakukan studi kepustakaan mengenai enkripsi dokumen. Studi kepustakaan dilakukan dengan membaca penelitian terdahulu yang terkait dengan enkripsi dokumen. Peneliti kemudian memilih 3 penelitian terdahulu sebagai penelitian yang relevan, yaitu skripsi oleh Muhamad Rifki Adnan dengan judul pengamanan data laporan keuangan menggunakan metode RC4 Pada reddog cabang Gading Serpong pada tahun 2022, skripsi oleh Uli Sholihah Saragih dengan judul implementasi enkripsi dan dekripsi dengan metode RC4 untuk pengamanan data sistem informasi pada tahun 2017 dan jurnal oleh Nurhikmah Taliasih dan Irawan Afrianto dengan judul sistem keamanan basis data klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 dan base64 yang diterbitkan jurnal nasional teknologi dan sistem informasi Vol. 06 No. 01 (2020) 009-018.

HASIL DAN PEMBAHASAN

Scope Definition

Ruang lingkup penelitian ini adalah perancangan sistem enkripsi dokumen menggunakan metode RC4 dan Base64 pada Justicia Law Firm & Associates.

Nama Proyek : Perancangan Sistem Enkripsi Dokumen Menggunakan Metode RC4 dan Base64 pada Justicia Law Firm & Associates.

Ruang Lingkup : Mengatasi permasalahan keamanan data perusahaan Justicia Law Firm & Associates.

Problem Analysis

Menghindari pencurian dan bocornya dokumen sensitif yang disimpan pada sistem *sharing files* Justicia Law Firm & Associates dengan merancang sistem enkripsi dokumen menggunakan metode RC4 dan Base64.

Requirement Analysis

a. Tingkatan pengguna

1) *Blocked* adalah tingkatan yang digunakan untuk mengunci akun agar tidak dapat masuk ke sistem enkripsi.
2) *Guest* adalah tingkatan yang digunakan untuk akun yang hanya diperbolehkan untuk mengunduh file yang dibagikan kepadanya. Akun ini tidak dapat mengunggah file dan melakukan manajemen pengguna.
3) *User* adalah tingkatan untuk akun biasa. Dengan level ini, pengguna dapat mengunggah file dan membagikannya kepada pengguna lain pada sistem.
4) *Administrator* adalah tingkatan tertinggi pada sistem enkripsi ini. Pengguna dengan level *Administrator* mendapatkan akses penuh atas sistem seperti pembuatan, penghapusan dan penyuntingan akun.

b. Spesifikasi *server*

Tabel 1. Spesifikasi server

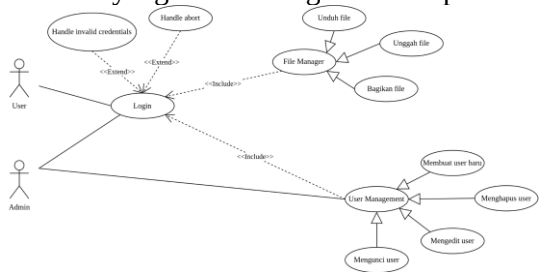
No	Perangkat	Kebutuhan Minimum
1.	CPU	1 *core*
2.	*Memory*	1 GB
3.	*Storage*	10 GB
4.	*Operation System*	Ubuntu 20.04
5.	Internet	Upload 20 Mbps

Sumber : Dokumen Pribadi (2023)

Logical Design

a. *Use Case Diagram*

Gambar 1 menjelaskan *use case diagram* dari sistem yang dirancang oleh peneliti.

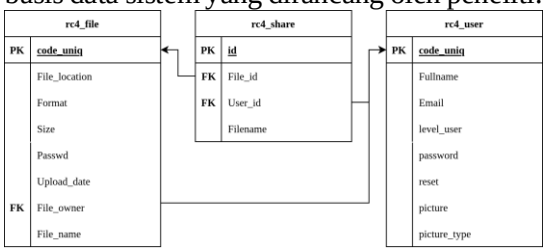


Gambar 1. *Use case diagram*
Sumber: Dokumen Pribadi (2023)

p-ISSN:2527-5321
e-ISSN:2527-5941

b. *Class Diagram*

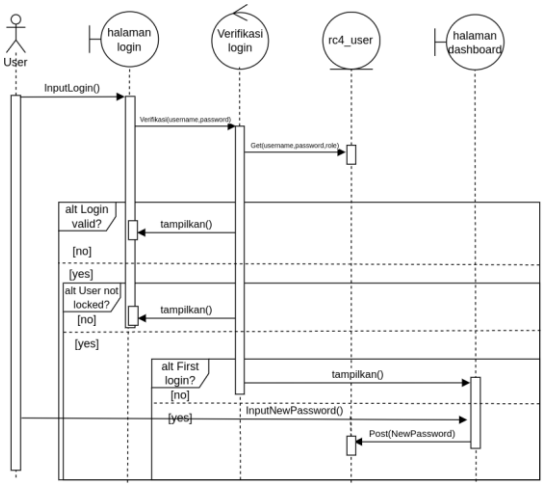
Gambar 2 menjelaskan class diagram dari basis data sistem yang dirancang oleh peneliti.



Gambar 2. ***Class diagram***
Sumber: Dokumen Pribadi (2023)

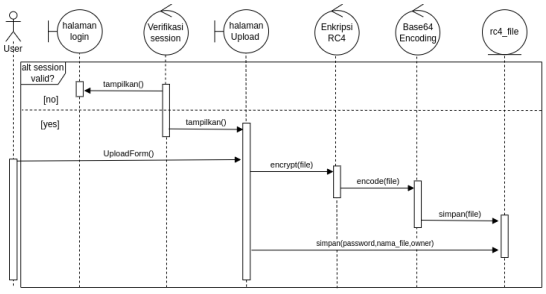
c. *Sequence Diagram*

Gambar 3 *sequence diagram login* dari basis data sistem yang dirancang oleh peneliti.



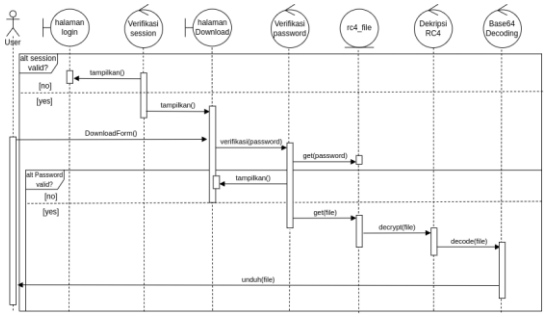
Gambar 3. ***Sequence diagram login***
Sumber: Dokumen Pribadi (2023)

Gambar 4 *sequence diagram upload* pada sistem yang dirancang oleh peneliti.



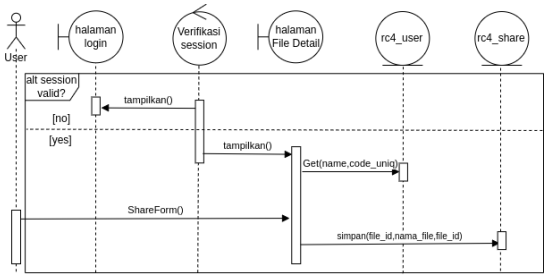
Gambar 4. ***Sequence diagram upload***
Sumber: Dokumen Pribadi (2023)

Gambar 5 menjelaskan *sequence diagram upload* pada sistem yang dirancang oleh peneliti.



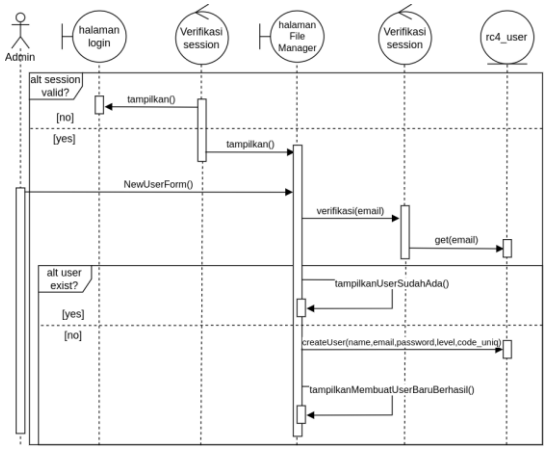
Gambar 5. ***Sequence diagram download***
Sumber: Dokumen Pribadi (2023)

Gambar 6 menjelaskan *sequence diagram share* pada sistem yang dirancang oleh peneliti.



Gambar 6. ***Sequence diagram share***
Sumber: Dokumen Pribadi (2023)

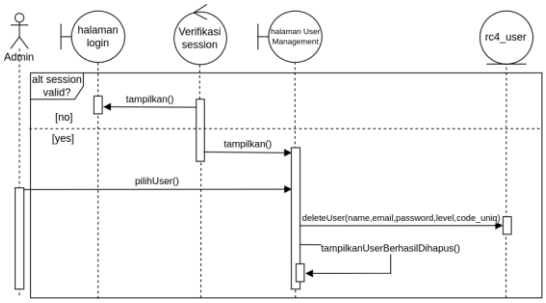
Gambar 7 menjelaskan *sequence diagram create user* pada sistem yang dirancang oleh peneliti.



Gambar 7. ***Sequence diagram create user***
Sumber: Dokumen Pribadi (2023)

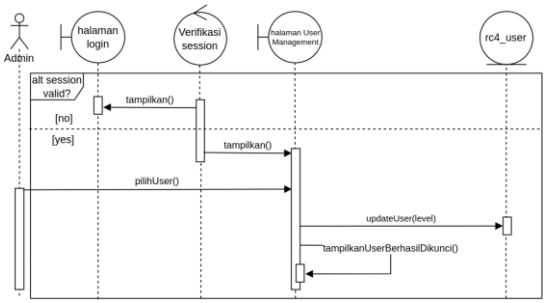
Gambar 8 menjelaskan *sequence diagram delete user* pada sistem yang dirancang oleh peneliti.

p-ISSN:2527-5321
e-ISSN:2527-5941



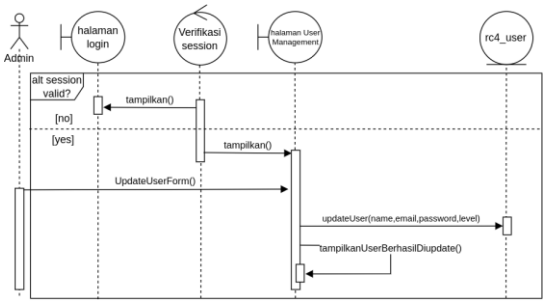
Gambar 8. *Sequence diagram delete user*
Sumber: Dokumen Pribadi (2023)

Gambar 9 menjelaskan *sequence diagram lock user* pada sistem yang dirancang oleh peneliti.



Gambar 9. *Sequence diagram lock user*
Sumber: Dokumen Pribadi (2023)

Gambar 10 menjelaskan *sequence diagram edit user* pada sistem yang dirancang oleh peneliti.



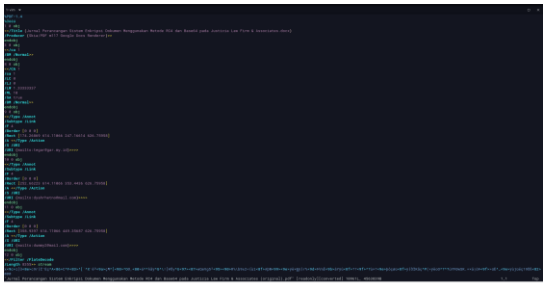
Gambar 10. *Sequence diagram edit user*
Sumber: Dokumen Pribadi (2023)

System Test

Gambar 11 menunjukkan isi file dokumen yang peneliti gunakan sebagai sampel untuk pengujian sistem enkripsi.

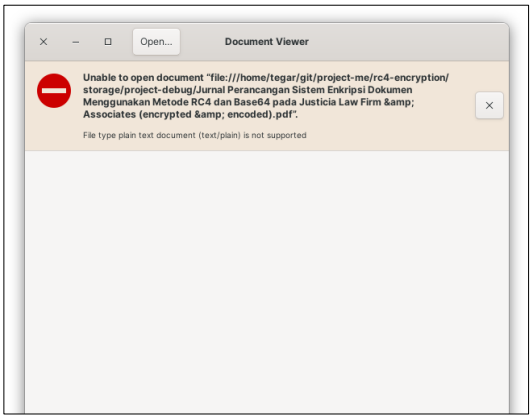
Gambar 11. Dokumen jurnal berekstensi pdf sebagai sampel
Sumber: Dokumen Pribadi (2023)

Gambar 12 menunjukkan isi file dokumen yang peneliti gunakan sebagai sampel untuk pengujian sistem enkripsi jika dibuka menggunakan Vim.



Gambar 12. Membuka dokumen sampel
Sumber: Dokumen Pribadi (2023)

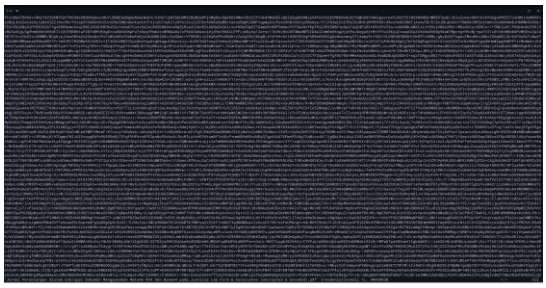
Gambar 13 pengujian membuka dokumen jurnal setelah melalui proses enkripsi dan *encoding* menunjukkan bahwa file tidak dapat dibuka setelah melalui proses enkripsi dan *encoding*.



Gambar 13. Pengujian membuka dokumen jurnal setelah melalui proses enkripsi dan *encoding*
Sumber: Dokumen Pribadi (2023)

Gambar 14 pengujian membuka dokumen jurnal menggunakan vim setelah melalui proses enkripsi dan *encoding* menunjukkan isi file setelah melalui proses enkripsi dan *encoding*.

p-ISSN:2527-5321
e-ISSN:2527-5941

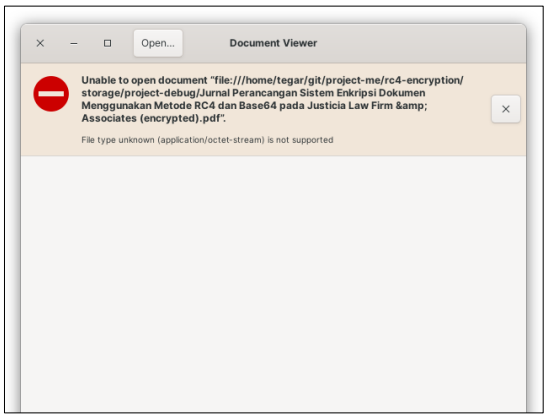


Gambar 14. Pengujian membuka dokumen jurnal menggunakan vim setelah melalui proses enkripsi dan *encoding*
Sumber: Dokumen Pribadi (2023)

Gambar 15 pengujian membuka dokumen jurnal terenkripsi menggunakan vim setelah melalui proses *decoding* menunjukkan isi file terenkripsi setelah melalui proses *decoding*.

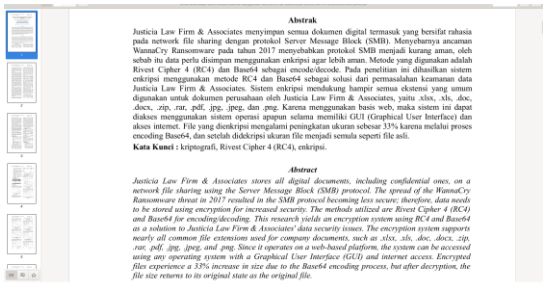
Gambar 15. Pengujian membuka dokumen jurnal terenkripsi menggunakan vim setelah melalui proses *decoding*
Sumber: Dokumen Pribadi (2023)

Gambar 16 pengujian membuka dokumen jurnal terenkripsi setelah melalui proses *decoding* menunjukkan bahwa file terenkripsi tidak dapat dibuka setelah melalui proses *decoding* dikarenakan file masih dalam keadaan terenkripsi.



Gambar 16. Pengujian membuka dokumen jurnal terenkripsi menggunakan vim setelah melalui proses *decoding*
Sumber: Dokumen Pribadi (2023)

Gambar 17 Pengujian Membuka Dokumen Jurnal Setelah Melalui Proses Dekripsi dan *Decode* menunjukkan bahwa file tidak rusak setelah melalui proses Dekripsi dan *Decode*.



Abstrak

Justicia Law Firm & Associates menyimpan semua dokumen digital termasuk yang bersifat rahasia pada network file sharing dengan protokol Server Message Block (SMB). Menyebarnya ancaman WannaCry Ransomware pada tahun 2017 menyebabkan protokol SMB menjadi kurang aman, oleh sebab itu data perlu disimpan menggunakan enkripsi agar lebih aman. Metode yang digunakan adalah Rivest Cipher 4 (RC4) dan Base64 sebagai encode/decode. Pada penelitian ini dihasilkan sistem enkripsi menggunakan metode RC4 dan Base64 sebagai solusi dari permasalahan keamanan data Justicia Law Firm & Associates. Sistem enkripsi mendukung hampir semua ekstensi yang umum digunakan untuk dokumen perusahaan oleh Justicia Law Firm & Associates, yaitu .xlsx, .xls, .doc, .docx, .zip, .rar, .pdf, .jpg, .jpeg, dan .png. Karena menggunakan basis web, maka sistem ini dapat diakses menggunakan sistem operasi apapun selama memiliki GUI (Graphical User Interface) dan akses internet. File yang dienkripsi mengalami peningkatan ukuran sebesar 33% karena melalui proses encoding Base64, dan setelah didekripsi ukuran file menjadi semula seperti file asli.

Kata Kunci : kriptografi, Rivest Cipher 4 (RC4), enkripsi.

Abstract

Justicia Law Firm & Associates stores all digital documents, including confidential ones, on a network file sharing using the Server Message Block (SMB) protocol. The spread of the WannaCry Ransomware threat in 2017 resulted in the SMB protocol becoming less secure; therefore, data needs to be stored using encryption for increased security. The methods utilized are Rivest Cipher 4 (RC4) and Base64 for encoding/decoding. This research yields an encryption system using RC4 and Base64 as a solution to Justicia Law Firm & Associates' data security issues. The encryption system supports nearly all common file extensions used for company documents, such as .xlsx, .xls, .doc, .docx, .zip, .rar, .pdf, .jpg, .jpeg, and .png. Since it operates on a web-based platform, the system can be accessed using any operating system with a Graphical User Interface (GUI) and internet access. Encrypted files experience a 33% increase in size due to the Base64 encoding process, but after decryption, the file size returns to its original state as the original file.

Gambar 17. Pengujian membuka dokumen jurnal setelah melalui proses dekripsi dan *decode*
Sumber: Dokumen Pribadi (2023)

Gambar 18 menunjukkan bahwa ukuran file yang hanya melalui proses enkripsi tidak berbeda dengan file asli. Adapun ukuran file yang telah melalui proses enkripsi juga *encoding* mengalami kenaikan sebesar 33% dikarenakan setiap digit Base64 merepresentasikan 6 bit data. Karena itu, 3 8-bit bytes dari input berbentuk string maupun file biner (3x8 bits = 24 bits) dapat direpresentasikan oleh empat digit 6-bit Base64 (4x6 = 24 bits) (Mozilla, 2023).

Gambar 18. Perbandingan ukuran file
Sumber: Dokumen Pribadi (2023)

SIMPULAN DAN SARAN

Berdasarkan penelitian yang telah dilakukan, dapat ditarik kesimpulan bahwa sistem enkripsi yang peneliti rancang menggunakan metode RC4 dan Base64 berhasil mengamankan dokumen perusahaan Justicia Law Firm & Associates sesuai dengan tujuan penelitian. Sistem ini mendukung hampir semua ekstensi yang umum digunakan oleh perusahaan, yaitu .xlsx, .xls, .doc, .docx, .zip, .rar, .pdf, .jpg, .jpeg, dan .png. Karena menggunakan basis web, maka sistem ini dapat diakses menggunakan sistem operasi apapun selama memiliki GUI (Graphical User Interface) dan akses internet. File yang dienkripsi mengalami peningkatan ukuran sebesar 33% karena melalui proses encoding Base64, dan setelah didekripsi ukuran file menjadi semula seperti file asli. File hasil enkripsi terbukti menjadi acak sehingga tidak dapat digunakan sebelum didekripsi oleh sistem.

UCAPAN TERIMAKASIH

Peneliti ucapkan terima kasih kepada Justicia Law Firm & Associates yang telah memberi izin untuk melakukan penelitian dan meluangkan waktu untuk melakukan wawancara, Universitas Indraprasta PGRI dan juga pihak Semnas Ristek yang telah memberikan kesempatan peneliti untuk menyusun dan menerbitkan artikel Sistem Enkripsi Dokumen Menggunakan Metode Rc4 Dan Base64 Pada Justicia Law Firm & Associates yang merupakan artikel pertama peneliti untuk diterbitkan pada jurnal.

DAFTAR PUSTAKA

Adnan, M. R. (2022). *Pengamanan Data Laporan Keuangan Menggunakan Metode RC4 Pada Reddog Cabang Gading Serpong*. (Skripsi). Program Studi Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur, Jakarta Selatan.

Afrianto, I., & Taliasih, N. (2020). Sistem Keamanan Basis Data Klien P.T. Infokes Menggunakan Kriptografi Kombinasi RC4 Dan Base64. *Jurnal Nasional Teknologi dan Sistem Informasi*, *6*(1), 9–18. https://doi.org/10.25077/teknosi.v6i1.2020.9-18

Arjun Shajit, B., Kantola, R. A., & Szakacsits, S. (2016). *Developing an In-kernel File Sharing Server Solution Based on Server Message Block Protocol*. (Tesis). Aalto University School of Electrical Engineering.

Justicia Law Firm & Associates. (2023). *Justicia Law Firm & Associates - Fiat Justitia Ruat Caelum*. Diakses 26 Maret 2023, dari https://justicia.attorney

Mohurle, S., & Patil, M. (2017). A brief study of Wannacry Threat: Ransomware Attack 2017. *International Journal of Advanced Research in Computer Science*, *8*(5), 1938–1940. www.ijarcs.info

Mozilla. (2023). *Base64*. Diakses 14 Agustus 2023, dari https://developer.mozilla.org/en-US/docs/Glossary/Base64

Saragih, U. S. (2017). *Implementasi Enkripsi Dan Dekripsi Dengan Metode Rc4 Untuk Pengamanan Data Sistem Informasi*. (Skripsi). Program Studi Ilmu Komputer, Fakultas Matematika Dan Ilmu Pengetahuan Alam, Universitas Lampung Bandar, Lampung.

Shallal, Q. M., Bokhari, M. U., & Shallal, Q. M. (2016). A Review on Symmetric Key Encryption Techniques in Cryptography. International Journal of Computer Applications (Vol. 147, Nomor 10), 43–48. https://www.researchgate.net/publication/333118027

Sumartono, I., Putera, A., Siahaan, U., & Mayasari, N. (2016). An Overview of the RC4 Algorithm. 18(6), 67–73. https://doi.org/10.9790/0661-1806046773