IMPLEMENTASI ALGORITMA KRIPTOGRAFI *RIVEST CODE* 4 (RC4) BERBASIS *WEB* PADA PT. PUTRI MAHARANI MEDIKAL

Daffa Arya[1*], Dolly Virgian Shaka Yudha Sakti[2]

[1,2]Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email: [1*]daffasimatauw21@gmail.com, [2]dolly.virgianshaka@budiluhur.ac.id
(* : corresponding author)

Abstrak- Keamanan merupakan hal yang sangat penting untuk sebuah data, demi menjaga kerahasiaan informasi yang terdapat dalam basis data tersebut. Salah satu kasus penyalahgunaan data pribadi terjadi di dalam PT. Putri Maharani Medikal yang dimana perusahaan ini adalah perusahaan yang bergerak dibidang medis, yaitu terjadinya penyalahgunaan data untuk digunakan sebagai pinjaman online oleh orang yang tidak bertanggung jawab. Untuk itu sangat diperlukan pengamanan data agar data pribadi kita atau data yang bersifat penting tidak dicuri atau disadap oleh orang yang tidak bertanggung jawab. Banyak data yang bersifat rahasia dan tidak bisa di salah gunakan oleh pihak yang tidak berhak menggunakannya. Kriptografi merupakan seni dan ilmu untuk memproteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang mempunyai kunci untuk mengubah kode itu Kembali yang berfungsi untuk menjaga kerahasiaan data atau pesan. Algoritma RC4 adalah algoritma yang membangkitkan keystream yang kemudian di-XOR-kan dengan plaintext pada waktu enkripsi atau di-XOR-kan dengan bit-bit ciphertext pada waktu dekripsi. Hasil penelitian, aplikasi ini dapat mengamankan database yang berisikan data pasien dan file penting.

Kata Kunci: kriptografi RC4, PT. putri maharani medikal, data

IMPLEMENTATION OF RIVEST CODE 4(RC4) CRYPTHOGRAPHY ALGORITHM AT PT. PUTRI MAHARANI MEDIKAL

Abstract- *Security is very important for a data, in order to maintain the confidentiality of the information contained in the database. One of the cases of misuse of personal data occurred in PT. Putri Maharani Medikal, where this company is a company engaged in the medical field, namely the misuse of data to be used as online loans by irresponsible people. For this reason, data security is very necessary so that our personal data or important data is not stolen or tapped by irresponsible people. A lot of data is confidential and cannot be misused by parties who are not entitled to use it. Crypthography is the art and science of protecting data transmission by converting it into a certain code and is only intended for people who have the key to change the code. Back which serves to maintain the confidemtiality of data or messages. The RC4 algorithm is an algorithm that generates a keystream which is then XORed with plaintext at the time of encryption or XORed with bits of ciphertext at the time of decryption. The results of the study, this application can secure a database containing patient data and important files.*

Keywords*: crypthography RC4, PT. putri maharani medikal, data*

1. PENDAHULUAN

Keamanan adalah hal yang cukup penting untuk sebuah data dalam bentuk *file* demi menjaga kerahasiaan informasi yang terdapat dalam file tersebut. Untuk itu sangat diperlukan pengamanan data agar data pribadi kita atau data yang bersifat penting tidak dicuri atau disadap oleh pihak yang tidak bertanggung jawab.

Kriptografi adalah salah satu solusi atau metode pengamanan data yang cukup tepat untuk menjaga kerahasiaan serta keamanan informasi, dan juga dapat meningkatkan keamanan suatu data ataupun informasi. Diterapkannya metode ini agar informasi yang bersifat rahasia yang akan dikirim melalui suatu jaringan, seperti dalam jaringan Internert ataupun LAN, tidak dapat diketahui atau disalahgunakan oleh orang atau pihak yang tidak memiliki kepentingan di dalamnya[1].

Pada dasarnya data rahasia perlu disimpan atau disampaikan melalui suatu cara tertentu agar tidak diketahui oleh pihak asing yang tidak berhak. Dan untuk mengatasi masalah tersebut maka terciptalah ilmu kriptografi[2][3].

Seiring dengan perkembangan teknologi, tidak hanya perangkat keras dan perangkat lunak saja namun sistem keamanan data juga semakin berkembang. Pada saat ini sering terjadi pencurian data yang disebabkan kurang nya sistem keamanan data pada *file*. *File* dokumen yang bersifat rahasia tidak boleh diketahui pihak luar karena akan menimbulkan kerugian materi. Untuk mengamankan data tersebut menggunakan *Rivest Code* 4 (RC4), karena metode ini menghasilkan ukuran Panjang karakter kunci (*ciphertext*) yang sama dengan pesan aslinya (*plaintext*).

Metode ini memiliki 3 tahap utama yaitu, KSA (*Key Scheduling Algorithm*), PRGA (*Psuedo Random Generation Algorithm*), dan proses XOR[3][4][5].

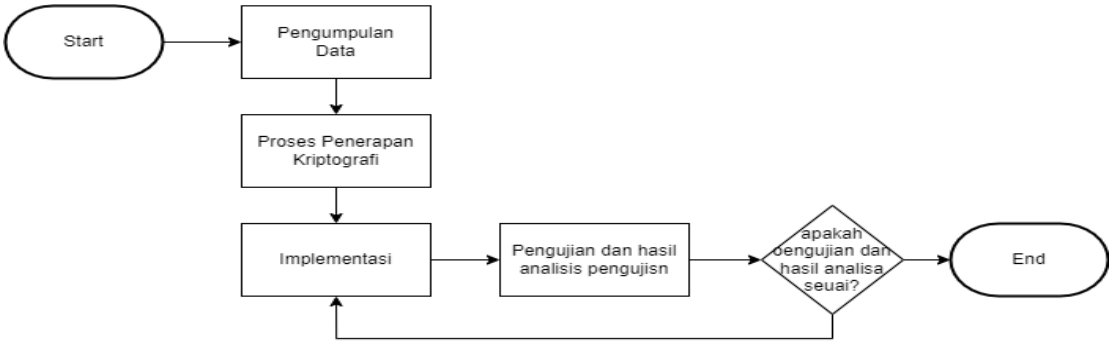
Pada penelitian sebelumnya juga telah dibuat aplikasi keamanan dengan menggunakan algoritma Kriptografi RC4 dan juga ada yang memakai algoritma lebih dari satu seperti kompresi LZW, *Playfair cipher, Caesar cipher*, dan BASE 64[6][7].

Dengan adanya sistem kriptografi sistem enkripsi dan dekripsi diharapkan dapat menjaga data yang bersifat rahasia. Kriptografi terdiri dari enkripsi dan dekripsi. Enkripsi yang dimaksud adalah mengubah pesan asli menjadi pesan sandi, sedangkan dekripsi adalah proses pengembalian pesan sandi menjadi pesan asli Kembali[8][9][10].

2. METODE PENELITIAN

Di dalam metode penilitian ini data yang akan digunakan adalah *database* pasien yang di dalamnya terdapat NIK, Nama, Alamat, Nomor Telfon, dan Alamat.

Metode penelitian ini digunakan sebagai pedoman dalam menjalankan penelitian agar hasil yang dicapai sesuai dengan tujuan yang telah dilakukan sebelumnya. Gambar di bawah ini merupakan tahapan yang dilakukan dalam penerapan metode penelitian yang akan dilakukan pada penelitian ini.



Gambar 1. Penerapan Metode

Lalngkalh pengumpulaln daltal digunalkaln sebalgali Lalngkalh untuk menentukaln permalsallalhaln yalng bisal dijaldikaln balhaln dallalm penelitialn ini. Beberalpal lalngkalh yalng dilalkukaln alntalral lalin :

a. Wawancara

Proses wawancara dilakukan langsung dengan pemilik dari perusahaan dan beberapa karyawan, dengan proses tanya jawab untuk membahas permasalahan dan solusi agar mendapatkan informasi untuk membangun aplikasi yang diharapkan.

b. Observasi

Observasi adalah cara mengumpulkan data yang efektif dan juga efisien untuk mempelajari suatu sistem yang akan dibangun. Ini dilakukan dengan pengamatan langsung dari permasalahan yang ada.

c. Studi Pustaka

Dilakukan dengan pengumpulan data dengan jurnal dan buku serta referensi lain yang berkaitan dengan kriptografi, *Rivest Code* 4 (RC4), dan teori-teori lainnya yang berkaitan dengan pembuatan program pada aplikasi ini.

Implementalsi sistem alkaln diimplementalsikaln kedallalm pembualtaln alplikalsi paldal penelitialn ini sesuali dengaln kebutuhaln berdalsalrkaln sistem yalng telalh dilalkukaln. Dallalm hall ini alplikalsi yalng alkaln digunalkaln alntalral lalin :

a. *Software* yang digunakan dalam penerapan pengamanan data menggunakan Bahasa pemrograman PHP dan penyimpanan data menggunakan MySQL.
b. *Hardware* yang akan digunakan Processor Intel Core i5, 1.2 GHz.

Berikut ini adalah tahap melalakukan pengujian pada aplikasii yang telah dibuat, dengan melakukan pengujian daftar file melalui menu enkripsi dan menu dekripsi pada aplikasi yang dibuat.

Tabel 1. Rancangan Pengujian

No	Skenario Pengujian	Hasil Yang Diharapkan
1.	*User* mengisi *form login*	Tampil halaman *menu home*
2.	*User* memilih sub *menu* enkripsi altalu dekripsi	Tampil halaman *menu* enkripsi atau dekripsi
3.	*User* menginput daftar pasien di *menu* enkripsi besertal *key* daln *submit*	Tampil Hasil data yang telah terenkripsi
4.	*User* ingin mendekripsikaln data yang telah dienkripsi dengan cara dekripsi daln memalsukaln *key*	Tampil halaman hasil daftar yang sudalh di dekripsikan Kembali menjadi normal
5.	*User* memilih menu tentang	Tampil halaman tentang

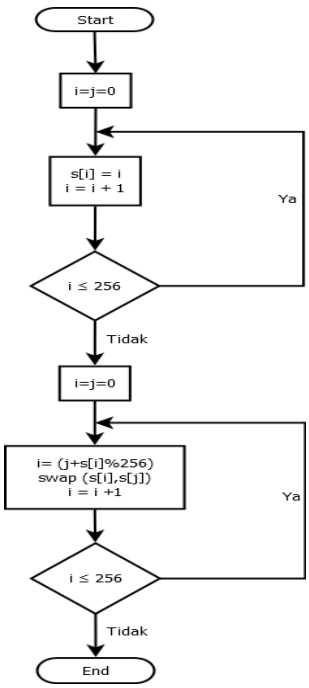
3. HASIL DAN PEMBAHASAN

Lingkungan percobaan pada penelitian ini menggunakan perangkat keras dan perangkat lunak yang digunakan penulis sebagai alat pendukung dalam melaksanakan penelitian dan merancang aplikasi. Adapun lingkungan percobaan yang digunakan pada penelitian adalah Processor Intel Core i5, 1.2 GHz dengan RAM/ Memory 8GB.

Pada penelitian ini penulis menggunakan metode Algoritma RC4, dan implementasi metode tersebut dapat dilihat pada gambar dibawah ini:

a. Implementasi Metode Enkripsi RC4

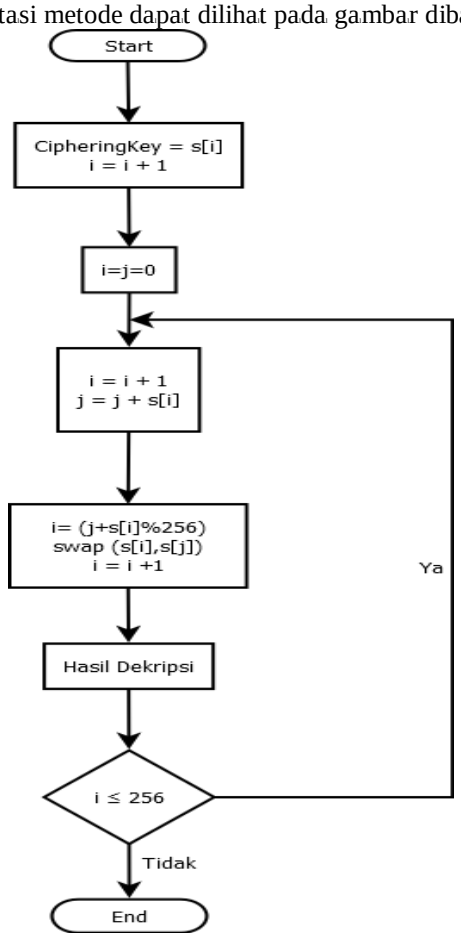
Pada gambar dibawah ini merupakan implementasi metode proses enkripsi menggunakan metode RC4. Pada bagian ini pertama setelah selesai data yang diinputkan akan pada bagian i dan selanjutnya variabel i akan penjumlahan dengan s(i) lalu setelah selesai selanjut nilai dari i akan dilakukan pengecekan i < 256, dan setelah i < dari 256 maka akan *false* dan nilai dari i langsung masuk ke proses *swap* yang dimana akan dilakukan proses pertukaran data dan setelah itu dilakukan pengecekan jika i sampai 256 dan setelah *false* maka akan tercetak hasil enkripsi yaitu *plaintext* Implementasi metode dapat dilihat pada gambar 2 dibawah ini:



Gaambar 2. Implementalsi Metode Enkripsi RC4

b. Implementasi Metode Dekripsi RC4

Pada gambar dibawah ini merupakan implementasi metode proses dekripsi menggunakan metode RC4, Pada bagian ini pertama setelah selesai data yang diinputkan akan pada bagian i dan selanjutnya variabel i akan penjumlahan dengan s(i) lalu setelah selesai selanjut nilai dari i akan dilakukan pengecekan i < 256, dan setelah i < dari 256 maka akan *false* dan nilai dari i langsung masuk ke proses *swap* yang dimana akan dilakukan proses pertukaran data dan setelah itu dilakukan pengecekan jika i sampai 256 dan setelah *false* maka akan tercetak hasil dekripsi yaitu *chipertext* implementasi metode dapat dilihat pada gambar dibawah ini:



Gambar 3. Implementasi Metode Dekripsi RC4

3.1 Hasil Rancangan Pengujian

Talbel 2. Hasil Rancangan Pengujian

No	Skenario Pengujian	Hasil Yang DiHarapkan	Hasil Pengujian
1.	*User* mengisi *form login*	Tampil halaman *menu home*	Sesuai Harapan
2.	*User* memilih *menu* enkripsi atau dekripsi	Tampil halaman *Menu* enkripsi atau dekripsi	Sesuai Harapan
3.	Memasukkan data dan menekan tombol untuk dienkripsi atau di dekripsi	Tampil halaman hasil proses enkripsi atau dekripsi	Sesuai Harapan
5.	*User* memilih menu Tentang	Tampil halaman *menu* Tentang	Sesuai Harapan
6.	*User* menekan tombol *logout*	Kembali kehalaman *login*	Sesuai Harapan

3.2 Analisa Hasil Uji Coba Program

Berdasarkan pengujian program yang dilakukan terhadap sistem aplikasi tersebut terdapat kelebihan dan kekurangan sebagai berikut:

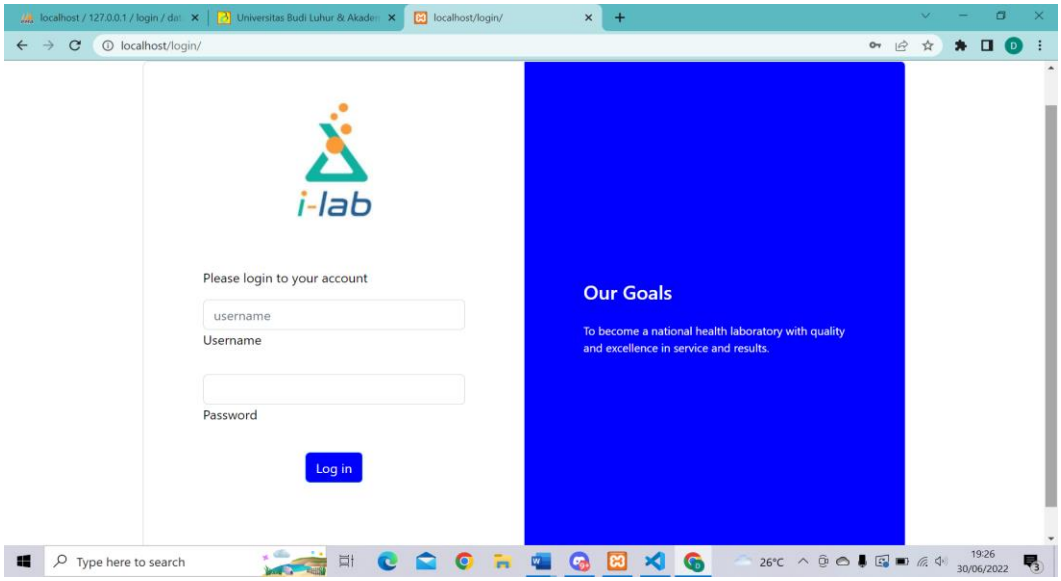
3.2.1 Kelebihan Program

a. Aplikasi ini mudah diakses karena berbasis *web*
b. Tampilan aplikasi *friendly* sehingga mudah dan nyaman untuk digunakan
c. Data yang dienkripsi tidak bisa dibaca sebelum di dekripsi

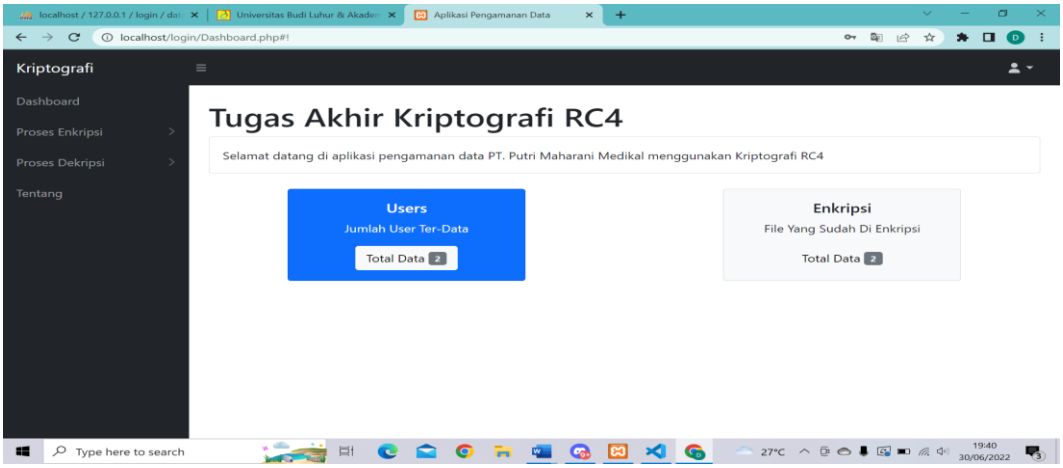
3.2.2 Kekurangan Program

a. Program masih menggunakan tampilan yang sederhana
b. Program hanya menggunakan satu algoritma untuk mengamankan data yakni metode RC4

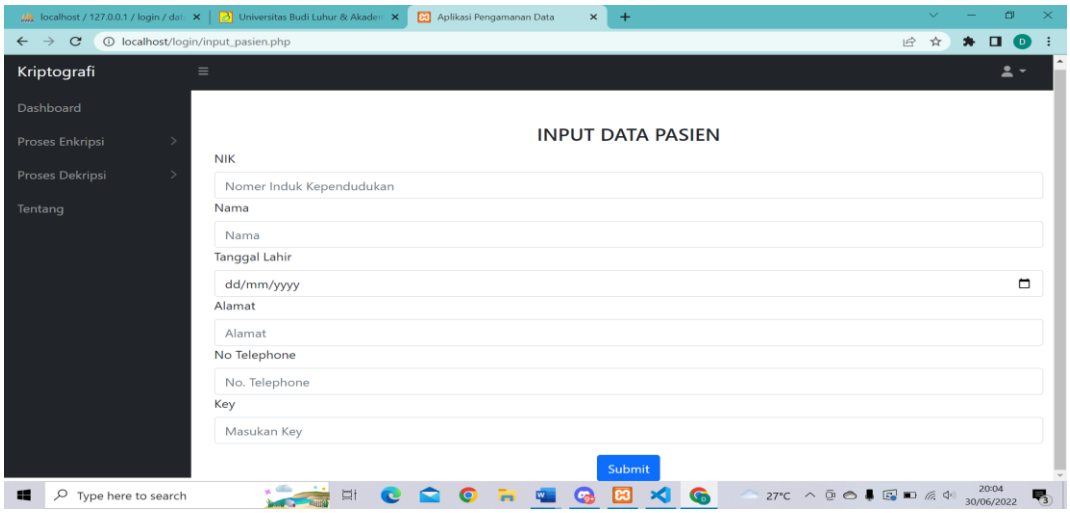
Berikut ini adalah gambar tampilan program aplikasi yang telah dibuat dimulai dari tampilan *login*, *dashboard*, proses enkripsi dan dekripsi. Berikut ini adalah gambar 4 menunjukan tampilan *menu login*, gambar 5 menunjukan tampilan *dashboard*, gambar 6 merupakan tampilan untuk input data untuk dienkripsi, dan terakhir pada gambar 7 merupakan tampilan hasil dekripsi.



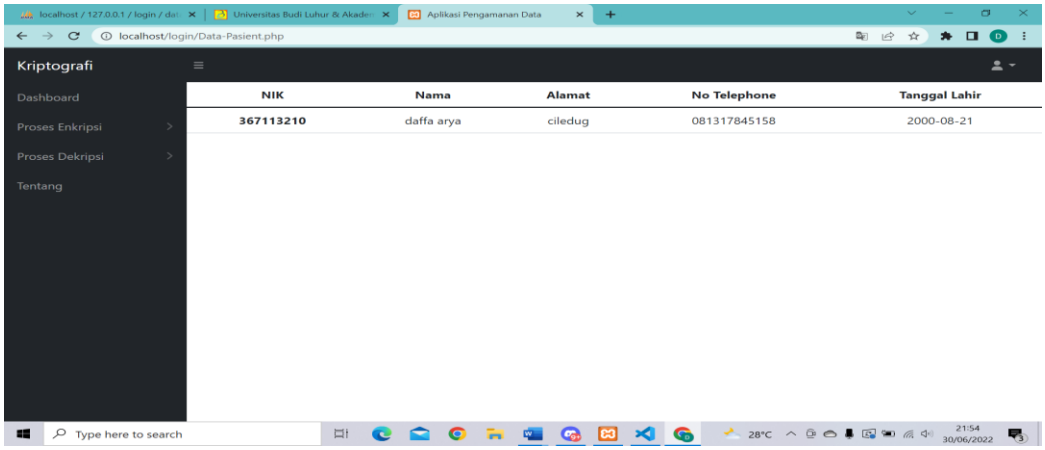
Gambar 4. Tampilan *Menu Login*



Gambar 5. Tampilan *Dashboard*



Gambar 6. Tampilan Input Data Untuk Di Enkripsi



Galmbalr 7. Tampilan Hasil Dekripsi

4. KESIMPULAN

Berdasarkan perumusan masalah dari program yang sudah dibuat maka dapat ditarik kesimpulan, sebagai berikut:

a. Dengan adanya aplikasi pengamanan data ini penyimpanan data atau informasi data diri menjadi lebih aman.
b. Dengan adanya aplikasi pengamanan data ini dapat menerapkan dan melakukan proses enkripsi atau dekripsi algoritma rivest code 4 (RC4) dengan baik dan dikhususkan untuk mengamankan file dan data di dalam basis data..
c. Aplikasi pengamanan data ini dapat menjamin keutuhan file dan data pada saat enkripsi maupun didekripsikan tanpa mengalami kerusakan atau perubahan data ketika di dekripsi.

Selain menarik beberapa kesimpulan, ada juga saran dan masukan yang diperlukan agar aplikasi ini dapat berjalan dengan lebih baik antara lain:

a. Dibutuhkan pengembangan sistem yang telah dibuat dan menambahkan fitur-fitur lain sesuai dengan kebutuhan.
b. Dapat menggunakan dua algoritms untuk melakukan proses enkripsi data agar dapat lebih aman seperti penggunaan dua algoritma simetris atau kombinasi antara algoritma simetris dan algoritma asimetris.

DAFTAR PUSTAKA

[1] Safwan Reza Dan Noni Juliasari, "Penerapan Kriptografi Pada Aplikasi Secure-Mail Berbasis Web Menggunakan Algoritma Caesar Cipher dan Rivest Code 4 (RC4)," *SKANIKA*, vol. 1, no. 1, pp.221-236, 2018.
[2] B. S. Hasugian, "Peranan Kriptografi Sebagai Keamanan Sistem Informasi Pada Usaha Kecil Dan Menengah," *Jurnal Warta Ed. 53*, 2017.
[3] R. Damanik, "Penyembunyian File Teks Menggunakan Algoritma RC4 dan End of File (Eof) Pada Citra Digital," *J. Isd*, vol. 3, no. 1, pp. 50–56, 2018.
[4] K. Kirman, "Implementasi Algoritma RC4 Untuk Proteksi File Mp3," *Pseudocode*, vol. 5, no. 1, pp. 80–86, 2018.
[5] D. P. O. Simamora, "Implementasi Algoritma RC4 dan Playfair Cipher Untuk Mengamankan Data Teks," *Jurnal Pelita Informatika*, vol. 6, no. 1, pp. 137-143, 2017.
[6] S. Susanto, "Implementasi Keamanan Data Menggunakan Algoritma Rivest Code 4 (RC4) Pada Sistem Informasi Inventory Stock Barang Pada Distributor PT. Wings Food," *Lontar Komputer*, vol. 8, no. 2, pp. 77-88, 2017.
[7] A. Kodir And W. Pramusinto, "Implementasi Kriptografi Dengan Menggunakan Metode Rc4 Dan Base64 Untuk Mengamankan Database Sekolah Pada Sdn Grogol Utara 10," *SKANIKA*, vol. 4, no. 1, pp. 7–14, 2021.
[8] W. E. Winanto And Mufti, "Aplikasi Keamanan Email Data Produksi Pt Kunyun Gravure Industries Indonesia Dengan Rc4 Dan Base64," *Skanika*, vol. 1, no. 1, pp. 303–308, 2018.
[9] A. R. Wahid And Syafrullah, "Implementasi Algoritma RC4 dan Kompresi Lzw Untuk Pengamanan Database Pada Pt . Mpp International," *Skanika*, vol. 1, no. 3, pp. 1045–1050, 2018.
[10] S. Susanto, "Implementasi Keamanan Data Sistem Informasi Inventory Stock Barang PT. Wings Food Menggunakan Algoritma Rivest Code 4 (RC4)," *Lontar Komputer*, vol. 8, no. 2, pp. 77-88, 2017.