

Penerapan Algoritma Vertical Bit Rotation Dalam Pengamanan Data Sekolah

Rachmat Aulia*, Haida Dafitri, Bayu Irwandi, Rizko Liza

Fakultas Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia

Email: ^{1,*}jackm4t@gmail.com, ²aida.stth@gmail.com, ³bbayu7068@gmail.com, ⁴risko.liza@gmail.com

Email Penulis Korespondensi: jackm4t@gmail.com

Submitted: 15/02/2022; Accepted: 31/03/2022; Published: 31/03/2022

Abstrak—Kriptografi merupakan ilmu yang berdasarkan pada teknik matematika yang berkaitan dengan keamanan dan informasi seperti kerahasiaan, keutuhan data dan otentikasi entitas. Definisi lain terkait kriptografi adalah melakukan proses pengkodean pustaka (dokumen-dokumen/data) yang berperan sebagai cipher, dan mengkonversikan teks asli menjadi teks yang tidak beraturan. Penerapan proses enkripsi memerlukan kunci publik dan kunci rahasia. Salah satu teknik kriptografi yang diaplikasikan pada penelitian ini adalah Algoritma *Vertical Bit Rotation* (VBR). Teknik VBR adalah teknik yang mengimplementasikan kunci asimetri, yang mana kunci tersebut bernilai sama dalam hal enkripsi maupun dekripsi data. Teknik dimaksud juga diterapkan dalam bentuk aplikasi yang dirancang pada penelitian ini, untuk dapat mendukung proses enkripsi dan dekripsi file berformat teks, sehingga memberikan keamanan data agar terhindar dari penyadapan dan akses ilegal dari pihak yang tidak bertanggung jawab. Hasil penelitian yang telah dilakukan menggunakan teknik VBR adalah proses enkripsi dan dekripsi data dalam bentuk dokumen teks dapat berjalan dengan baik sehingga mampu mengembalikan kondisi data dalam bentuk plaintext dan sebagai informasi tambahan, data yang sudah terenkripsi tidak dapat dikembalikan ke dalam bentuk aslinya tanpa menggunakan kunci yang sama.

Kata Kunci: Kriptografi; Vertical Bit Rotation; Enkripsi; Dekripsi; Kunci Publik

Abstract—Cryptography is a science based on mathematical techniques related to security and information such as confidentiality, data integrity and entity authentication. In other words, it means to conduct the process of encoding libraries that act as ciphers, and converting the original text into illegal it. The implementation of encryption process requires a public and a secret key. One of the cryptography techniques applied in the research is the Algorithm of Vertical Bit Rotation (VBR). The VBR is a technique that implements an asymmetric key, which it has a same value in term of data encryption and decryption. The technique is also applied in the shape of an application designed in this research, then have ability to run encryption and decryption process in the format of text file, that providing data security to avoid eavesdropping and illegal access from irresponsible parties. The result done by using VBR is it may run well so have ability to restore the condition of the data in plaintext, then in addition information, encrypted data cannot be returned to its pure form without using a valid key.

Keywords: Cryptography; Vertical Bit Rotation; Encryption; Decryption; Public Key

1. PENDAHULUAN

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatannya. Banyaknya proses yang dikomputerisasikan, menyebabkan keamanan sangat diperlukan pada semua aspek, terutama info dan data krusial demi menjaga kerahasiaan info data tersebut. Keamanan adalah aspek penting dalam menjaga suatu informasi maupun data dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi. Keamanan merupakan aspek penting dari suatu data atau informasi, dimana pengiriman data atau informasi membutuhkan keamanan yang tinggi terdapat beberapa cara melakukan pengamanan data ataupun pesan, antara lain ialah menggunakan teknik penyamaran data yang dianggap menggunakan kriptografi [1].

Kriptografi ialah seni serta ilmu buat memproteksi pengiriman data menggunakan mengubahnya sebagai kode eksklusif serta hanya ditujukan buat orang yang hanya mempunyai sebuah kunci buat mengganti kode itu kembali yang berfungsi pada saat menjaga kerahasiaan data atau pesan [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 [3].

Dalam dunia kriptografi ternyata huruf yang sama pada pesan mempunyai photograph huruf yang sama juga. Hal ini mempunyai tingkat resiko yang tinggi karena mudah ditebak. Untuk menuntaskan hal ini maka pesan haruslah disandikan (encoding)[4]. Tujuan membuat penyandian adalah mengamankan sandi dari para pembongkar sehingga hanya penerima saja yang mengetahui isinya [5].

Keamanan informasi merupakan prioritas utama di era saat ini. Dokumen–dokumen ataupun catatan–catatan kecil namun penting dapat menyebabkan kerugian yang cukup besar jika tidak diberikan keamanan tambahan[6]. Untuk mengatasi itu dibutuhkan mekanisme keamanan digital yang tergolong ke dalam bidang kriptografi. Kriptografi (cryptography) awalnya diadopsi dari bahasa Yunani yang memiliki dua suku kata: *kryptos* (tersembunyi) dan *graphein* (tulisan), jadi apabila digabungkan menjadi “tulisan tersembunyi” [7]. Kriptografi tidak hanya mencakup teknik-teknik menyandikan informasi, tetapi juga teknik untuk membongkar sandi. Terdapat dua proses utama dalam kriptografi: enkripsi dan dekripsi. Enkripsi adalah teknik yang mengubah plaintext menjadi ciphertext. Sedangkan deskripsi sebaliknya[8].

Penelitian sebelumnya dinyatakan bahwa, metode Vertical Bit Rotation akan berfungsi dengan baik apabila hasil enkripsi berupa nilai ASCII dapat direpresentasikan ke dalam karakter sehingga saat proses dekripsi dapat berjalan dengan sebagaimana mestinya dan dalam proses enkryp dan dekryp untuk setiap operasinya menggunakan 64-bit kunci dan 32 putaran [9].

Pada pembahasan latar belakang ini berkaitan dengan data sekolah yang dapat diamankan menggunakan teknik kriptografi menggunakan metode algoritma VBR (Vertical Bit Rotation) di SMA Negeri 8 Medan yang beralamat di Jalan Sampali no 23. SMA Negeri 8 Medan ialah sekolah Menengah Atas Negeri yang berada di provinsi Sumatera Utara, Indonesia.

Sama juga pada SMA biasanya yang ada di Indonesia masa pendidikan sekolah di SMAN 8 Medan ditempuh dalam waktu tiga tahun pelajaran, mulai dari kelas X sampai kelas XII. SMAN 8 merupakan sekolah yang mengembangkan prestasi akademik dan non-akademik pada siswanya, seperti memiliki kualitas ekstrakurikuler yang sangat baik. Banyak diantaranya ekstrakurikuler SMAN 8 Medan yang sudah terkenal di kota Medan sebagai ekstrakurikuler yang diakui. Pada tanggal 22 November 2011 akreditasi yang dimiliki sekolah ini yaitu akreditasi A dengan nilai sangat baik yaitu 98,45.

Fasilitas yang ada dalam sekolah ini sendiri adalah ruangan kelas, lab biologi, aula dan lapangan basket dengan ekstrakurikuler karate, cheerleaders, PMR, paduan suara, pasbrata, basket, futsal, dan pramuka dengan berbagai macam prestasi. Sekolah sebagai salah satu instansi atau organisasi yang juga menggunakan data adalah tujuan pengamanan data yang diajukan oleh penulis. Sekolah SMA Negeri 8 Medan di Jl. Sampali No.23, Pandau Hulu II, Kec. Medan Area, Kota Medan, Sumatera Utara adalah sekolah yang juga menggunakan data untuk penyimpanan data penting dan data internal mereka, sehingga implementasi kriptografi menggunakan algoritma VBR pada kasus ini dapat dilaksanakan dengan baik. Adapun manfaat diperoleh pada penelitian ini dapat merancang sebuah sistem dengan memberikan keamanan data pada pengarsipan data sekolah dengan menggunakan Vertical Bit Rotation (VBR).

2. METODOLOGI PENELITIAN

2.1 Pengumpulan Data

Teknik pengambilan data pada penelitian ini adalah sebagai berikut[10] :

1. Studi Literatur

Pada tahapan ini dalam pemahaman serta penjelasan konsep didapat dari buku-buku referensi, jurnal penelitian ataupun artikel yang didapat dari internet. Setelah materi yang dibutuhkan untuk pembuatan sistem ini telah terkumpul dan terdeteksi, maka dapat dilakukan pembelajaran materi.

2. Wawancara

Wawancara dilakukan untuk mendapatkan data atau informasi tentang sistem yang ingin penulis buat secara rinci. Data yang didapat diperoleh dari proses tanya jawab.

3. Observasi

Proses memperoleh data yang akurat dilakukan dengan mensinkronkan hasil wawancara yang didapat dengan melakukan observasi secara langsung.

2.2 Analisa

Analisa merupakan bentuk penelitian yang dilakukan secara terorganisir dalam melihat suatu peristiwa atau kejadian, untuk menentukan tema apa yang akan dipakai dalam pembuatan sistem agar dapat tersampaikan dan menjadi solusi sesuai dengan permasalahan yang ada [11].

2.3 Algoritma Kriptografi VBR (Vertical Bit Rotation)

Algoritma VBR merupakan yang mempunyai 32 putaran yang digunakan sebagai proses enkrip dan dekrip pada setiap operasinya, algoritma ini menggunakan 64 bit dan merupakan algoritma simetrik [12]. Encryp adalah suatu langkah yang dilakukan proses agar kode tersebut yang awalnya tidak dapat diketahui sehingga kode tersebut dapat diketahui dan dibaca[13]. Dekryp dapat diartikan sebuah chipper atau kode yang menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi cryptogram yang tidak dimengerti.

2.4 Perancangan Sistem

Perancangan sistem yang dibuat merupakan perancangan awal bentuk sistem yang akan diterapkan dan dibahas permasalahan, dimana sistem yang dibuat harus benar-benar sesuai dengan permasalahan dan harus mampu diterapkan pada program[14].

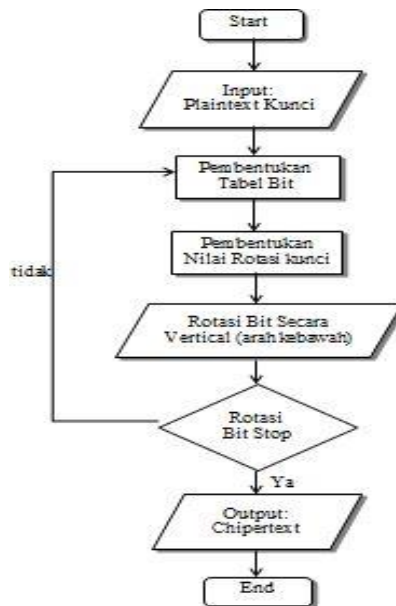
2.5 Flowchart Sistem

Langkah-langkah penyelesaian *flowchart* sistem dalam proses enkripsi serta proses dekripsi algoritma kriptografi VBR (Vertical Bit Rotation)[15]:

1. Flowchart enkripsi.

Pada penjelasan proses terjadinya enkripsi terhadap mengamankan pesan dimana dimulai plaintext yang mana dapat dimasukkan langsung ke dalam sistem dari dari yang berupa text yang dapat dibaca oleh sistem. Setelah itu

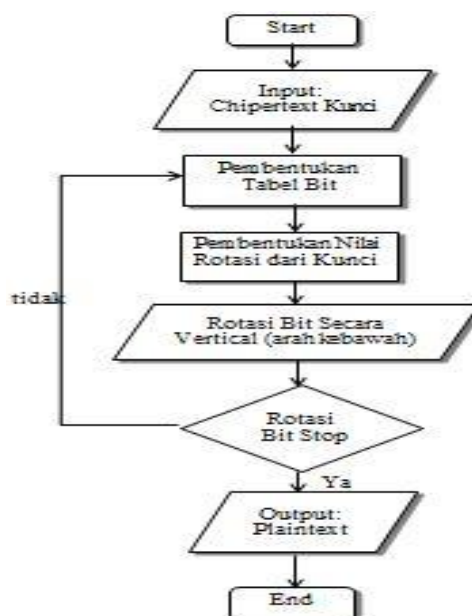
melakukan proses enkripsi kedalam algoritma VBR terhadap plaintext [16]. Setelah itu, masukkan kunci dengan kunci yaitu 1,2,3,4,5,6,7,8 untuk proses melakukan enkripsi.



Gambar 1. Flowchart Proses Enkripsi

2. Flowchart Dekripsi

Menjelaskan tentang proses terjadinya dekripsi pesan yang dimulai dari memasukkan chipertext kedua, selanjutnya dilakukan proses dekripsi dengan kunci yang sudah dimasukkan algoritma VBR (Vertical Bit Rotation)[13]. Sebelum dilakukan proses yang terlebih dahulu memeriksa kunci yaitu dengan kunci 1,2,3,4,5,6,7,8 apakah sama dengan hasil sebelumnya melakukan enkripsi. Untuk selanjutnya adalah memulai dari memasukkan hasil enkripsi chipertext, kemudian masukkan kunci dan proses dekripsi untuk mejalankannya [17].



Gambar 2. Flowchart Proses Dekripsi

3. HASIL DAN PEMBAHASAN

3.1 Penerapan Algoritma VBR

Dengan menerapkan algoritma Vertical Bit Rotation dalam satu buah sistem yang akan mengamankan data teks maka diperlukan langkah-langkah yang diperlukan dalam teknik Bit Vertical Bit Rotation ini untuk bekerja. Langkah awal yaitu karakter yang sudah diambil dari teks dilakukan proses enkripsi dan dekripsi, nilai ASCII-nya akan di proses sehingga akan di ganti dalam bentuk bit. Selanjutnya nilai bit akan diproses secara vertikal berdasarkan karakter



pembangkitnya. Dapat diproses dari sebuah sampel dari sebuah file yang bernama TES.doc, yang berisi data dari file tersebut adalah “tabel Organisasi”.

Langkah-langkah penelitian adapun langkah pertama dalam proses enkripsi dan dekripsi kriptografi dengan menggunakan metode VBR.

Tabel 1. Organisasi

Nama Oraganisasi	Jumlah
PMR	25

Dalam proses menjalankan dari file yang diambil dari data Organisasi diatas dapat dilakukan sebagai berikut:

Kunci awal adalah 1,2,3,4,5,6,7,8

Selanjutnya kunci awal konversi kunci ke *Byte Decimal* ASCII : 49,50,51,52,53,54,55,56

Dan selanjutnya proses Enkripsi :

Kunci Ke - 1 [49]:

Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 49 kali pada *bit* diposisi 1, *Bit* karakter sebelum geser *vertical* :

```
01010000 01001101 01010010 00001001 00110010 00110101 00001101 00001010
00001101 00001010 00001101 00001010 00001101 00001010
```

Hasil data Organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci -1 :

```
01010000 01001101 01010010 00001001 00110010 00110101 00001101 00001010
00001101 00001010 00001101 00001010 00001101 00001010
```

Setelah melakukan pergeseran kunci 1, tahap selanjutnya adalah melakukan pergeseran ke kunci - 2 [50]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 50 kali pada bit diposisi 2, *Bit* karakter sebelum geser *vertical* :

```
01010000 01001101 01010010 00001001 00110010 00110101 00001101 00001010
00001101 00001010 00001101 00001010 00001101 00001010
```

Hasil data Organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 2 :

```
00010000 00001101 00010010 00001001 00110010 00110101 00001101 00001010
01001101 01001010 01001101 00001010 00001101 00001010
```

Setelah melakukan pergeseran kunci 2, tahap selanjutnya adalah melakukan pergeseran ke kunci - 3 [51]: Data siswa melakukan pergeseran *Bit Vertical* sebanyak 51 kali pada bit di posisi 3, *Bit* karakter sebelum geser *vertical* :

```
00010000 00001101 00010010 00001001 00110010 00110101 00001101 00001010
01001101 01001010 01001101 00001010 00001101 00001010
```

Hasil data Organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 3 :

```
00110000 00001101 00010010 00001001 00010010 00010101 00001101 00001010
01001101 01001010 01001101 00001010 00001101 00101010
```

Setelah melakukan pergeseran kunci 3, tahap selanjutnya adalah melakukan pergeseran ke kunci - 4 [52]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 52 kali pada bit di posisi 3, *Bit* karakter sebelum geser *vertical* :

```
00110000 00001101 00010010 00001001 00010010 00010101 00001101 00001010
01001101 01001010 01001101 00001010 00001101 00101010
```

Hasil data Organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 4 :

```
00110000 00011101 00000010 00001001 00000010 00010101 00001101 00001010
01001101 01001010 01011101 00001010 00011101 00101010
```

Setelah melakukan pergeseran kunci 4, tahap selanjutnya adalah melakukan pergeseran ke kunci - 5 [53]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 53 kali pada bit di posisi 5, *Bit* karakter sebelum geser *vertical* :

```
00110000 00011101 00000010 00001001 00000010 00000101 00001101 00001010
01001101 01001010 01011101 00001010 00011101 00101010
```

Hasil data organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 5 :

```
00111000 00010101 00000010 00001001 00001010 00001101 00001101 00001010
01001101 01001010 01011101 00000010 00011101 00100010
```

Setelah melakukan pergeseran kunci 5, tahap selanjutnya adalah melakukan pergeseran ke kunci - 6 [54]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 54 kali pada bit di posisi 6, *Bit* karakter sebelum geser *vertical* :

```
00111000 00010101 00000010 00001001 00001010 00001101 00001101 00001010
01001101 01001010 01011101 00000010 00011101 00100010
```

Hasil data organisasi *bit* karakter setelah melakukan pergeseran *vertical* kuci ke - 6:

```
00111000 00010001 00000010 00001101 00001110 00001001 00001101 00001010
01001101 01001010 01011101 00000010 00011001 00100110
```

Setelah melakukan pergeseran kunci 6, tahap selanjutnya adalah melakukan pergeseran ke kunci - 7 [55]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 55 kali pada *bit* di posisi 7, *Bit* karakter sebelum geser *vertical* :



00111000 00010001 00000010 00001101 00001110 00001001 00001101 00001010
 01001101 01001010 01011101 00000010 00011001 00100110

Hasil data organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 7:

00111000 00010011 00000000 00001111 00001100 00001001 00001111 00001000
 01001111 01001000 01011111 00000000 00011011 00100100

Setelah melakukan pergeseran kunci 7, tahap selanjutnya adalah melakukan pergeseran ke kunci - 8 [56]: Data Organisasi melakukan pergeseran *Bit Vertical* sebanyak 56 kali pada bit di posisi 8, *Bit* karakter sebelum geser *vertical* :

00111000 00010011 00000000 00001111 00001100 00001001 00001111 00001000
 01001111 01001000 01011111 00000000 00011011 00100100

Hasil data Organisasi *bit* karakter setelah melakukan pergeseran *vertical* kunci ke - 8:

00111000 00010011 00000000 00001111 00001100 00001001 00001111 00001000
 01001111 01001000 01011111 00000000 00011011 00100100

Hasil yang didapat dari keseluruhan data Organisasi yang telah dilakukan maka *byte* akhir diperoleh setelah melakukan pergeseran *vertical* 1 sampai 8 bit karakter setelah data diinput ke menu halaman, sebelum melakukan proses enkripsi : 15,8,79,72,95,0,27,36,56,19,0,15,12,9,15,8

Dan selanjutnya adalah hasil data Organisasi setelah melakukan enkripsi yaitu dengan kunci 1,2,3,4,5,6,7,8 hasil enkripsi : __OH_

3.2 Tabel Pengujian Algoritma VBR (Vertical Bit Rotation)

Pengujian algoritma VBR (*Vertical Bit Rotation*) dalam proses keamanan pesan dilakukan percobaan pada beberapa *plaintext* dengan menggunakan kunci yang sama pada pembangkit kunci, seperti yang tampak pada tampilan berikut:

Tabel 2. Pesan Text

No	Pesan text	VBR
1	Nabila Nasywa 0042441002 082163709559 Islam Perempuan Medan, 31 Desember 2004	12345678
2	Drs. Maryono, M.Si. PNS 081396844442 LAKI – LAKI ISLAM	12345678
3	IPA 5 0 0 0 5	12345678
4	PMR 25	12345678

Tabel 3. Hasil Enkripsi dan Dekripsi

No	Enkripsi	Dekripsi	Keterangan
1	0640_!828102436;1TMiya)G !aqe`• t!EH mkd%),wP` (= #71pR` ldc(kDahur8_%;11 14	Nabila Nasywa 0042441002082163709559 Islam Perempuan Medan, 11Okt 2005	Berhasil
2	tpi+,oOf9\$HK]__%:291083=344TDhj\$ihk m%IHkya)_ __OHo07`Jfk	Drs. Maryono, M.Si. PNS 081396844442 LAKI – LAKI ISLAM	Berhasil
3	__!_!_ALM__ __!_	IPA 5 0 0 0 5	Berhasil
4	__OH_	PMR 25	Berhasil

4. KESIMPULAN

Berdasarkan penelitian dengan judul Implementasi Kriptografi Untuk Pengamanan Data Sekolah Menggunakan Algoritma VBR (*Vertical Bit Rotation*) Pada SMA Negeri 8 Medan. Dengan menggunakan software visual basic 10, dengan menggunakan data yang sudah dipakai untuk proses enkripsi dan dekripsi maka dalam proses penerapan algoritma VBR dapat di implementasikan dengan baik, dan penerapan VBR terbukti mampu memberikan keamanan. Pembuatan *system* keamanan file menggunakan VBR tidak menyebabkan kerusakan pada data, dimana hasil enkripsi dapat di dekripsi dengan baik dan mampu mengembalikan kondisi data kembali pada bentuk *plaintexts*. Informasi yang sudah terenkripsi tidak dapat dikembalikan ke dalam bentuk aslinya, jika pembangkit kuncinya tidak sama. Aplikasi pada penelitian ini dikembangkan untuk mengenkripsi pesan agar terjaga kerahasiannya sekaligus

mendeskripsikannya ke dalam bentuk aslinya agar dapat diketahui maknanya. Untuk penelitian selanjutnya disarankan menggunakan metode pengujian yang berbeda atau menggunakan metode yang sama dengan menggunakan studi kasus yang baru.

REFERENCES

- [1] D. J. E. Prihanto and M. I. Pakereng, "Perancangan Teknik Kriptografi Block Cipher Berbasis Pola Tarian Sajojo Papua," *Ultim. Comput. J. Sist. Komput.*, vol. 11, no. 2, pp. 71–80, 2020, doi: 10.31937/sk.v11i2.1454.
- [2] S. Agustini and M. Kurniawan, "Peningkatan Keamanan Teks Menggunakan Kriptografi Dan Steganografi," *SCAN - J. Teknol. Inf. dan Komun.*, vol. 14, no. 3, pp. 33–38, 2019, doi: 10.33005/scan.v14i3.1685.
- [3] R. Aulia, A. Zakir, and D. A. Purwanto, "Penerapan Kombinasi Algoritma Base64 Dan Rot47 Untuk Enkripsi Database Pasien Rumah Sakit Jiwa Prof. Dr. Muhammad Ildrem," *InfoTekJar (Jurnal Nas. Inform. dan Teknol. Jaringan)*, vol. 2, no. 2, pp. 146–151, 2018, doi: 10.30743/infotekjar.v2i2.300.
- [4] J. T. Elektro and P. N. Bandung, "Algoritma Labeling Citra Biner Dengan Performansi Optimal Processor-Time," *elektro*, vol. 4, no. 1, p. pp.18-26, 2003, doi: 10.9744/informatika.4.1.pp.18-26.
- [5] E. N. Citra, "Penerapan Algoritma Vertical Bit Rotation (VBR) Dalam Penyimpanan File Online," *MEANS (Media Inf. Anal. dan Sist.*, vol. 3, no. 1, pp. 16–23, 2018.
- [6] S. Tri, C. Kurniawan, T. Informatika, and S. Informasi, "Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android," vol. 2, no. 2, pp. 102–109, 2017, doi: 10.15575/join.v2i2.113.
- [7] I. Print, R. Aulia, A. Zakir, and M. Zulfahiz, "InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Penerapan Algoritma One Time Pad & Linear Congruential Generator Untuk Keamanan Pesan Teks," *J. Nas. Inform. Dan Ilmu Komput.*, vol. 1, 2019.
- [8] M. R. Rambe, E. V. Haryanto, and A. Setiawan, "Aplikasi Pengamanan Data dan Disisipkan Pada Gambar dengan Algoritma RSA Dan Modified LSB Berbasis Android," pp. 8–9, 2018.
- [9] S. Indonesia, J. P. Hidayatullah, and T. Wa, "Jurnal Sains Komputer dan Teknologi Informasi Page Yeffriansjah Salim . Implementasi Algoritma Vertical Bit Rotation (Vbr) Pada File Teks .," vol. 3, no. 1, pp. 41–51, 2020.
- [10] A. Utama and R. F. Siahaan, "Penerapan Kriptografi untuk Pengamanan Data Transaksi Deposito pada Easy Tronik dengan Metode RC-5," *J. Ilmu Komput. dan Sist. ...*, vol. 3, no. 3, pp. 29–39, 2021, [Online]. Available: <http://ejournal.sisfokomtek.org/index.php/jikom/article/view/86>.
- [11] F. Azmi and W. Erika, "Analisis Keamanan Data Pada Block Cipher Algoritma Kriptografi Rsa," *CESS (Journal Comput. Eng. Syst. Sci.*, vol. 2, no. 1, pp. 27–29, 2017.
- [12] R. Nuari and N. Ratama, "Implementasi Algoritma Kriptografi AES (Advanced Encryption Standard) 128 Bit Untuk Pengamanan Dokumen Shipping," *J. Artif. Intell. Innov. Appl.*, vol. 1, no. 2, pp. 2716–1501, 2020, [Online]. Available: <http://openjournal.unpam.ac.id/index.php/JOAIIA>.
- [13] Y. Reswan, U. Juhardi, B. T. Yuliansyah, and U. M. Bengkulu, "Implementasi Kompilasi Algoritma Kriptografi Transposisi Columnar Dan Rsa Untuk Pengamanan Pesan Rahasia," vol. 4, no. 2, 2018.
- [14] M. Y. Simargolang, "IMPLEMENTASI KRIPTOGRAFI RSA DENGAN PHP," vol. 1, pp. 1–10, 2017.
- [15] S. Waluyo and D. V. Kanahebi, "SISTEM PENGAMANAN FILE MENGGUNAKAN ALGORITMA RC4 BERBASIS WEBBASE STUDI KASUS : PT . TJIPTA JAYA BERSAMA," pp. 803–808, 2021.
- [16] O. Dakhi, M. Masril, R. Novalinda, J. Jufrinaldi, and A. Ambiyar, "Analisis Sistem Kriptografi dalam Mengamankan Data Pesan Dengan Metode One Time Pad Cipher," *INVOTEK J. Inov. Vokasional dan Teknol.*, vol. 20, no. 1, pp. 27–36, 2020, doi: 10.24036/invotek.v20i1.647.
- [17] F. Alfonita, "F. alfonita," *Comput. Ind. Eng.*, vol. 2, no. January, p. 6, 2018, [Online]. Available: <http://ieeauthorcenter.ieee.org/wp-content/uploads/IEEE-Reference-Guide.pdf%0Ahttp://wwwlib.murdoch.edu.au/find/citation/ieee.html%0Ahttps://doi.org/10.1016/j.cie.2019.07.022%0Ahttp://github.com/ethereum/wiki/wiki/White-Paper%0Ahttps://tore.tuhh.de/hand>.