

PENERAPAN KRIPTOGRAFI CAESAR CIPHER DAN BASE64 UNTUK MENGAMANKAN DATABASE DISTRIBUTOR BARANG PADA PT. SEKAWAN

Kholik Nurzaman^{1*}, Sri Mulyati²

^{1,2}Fakultas Teknologi Informasi, Teknik Informatika, Universitas Budi Luhur, Jakarta, Indonesia

Email : ^{1*}kholik.nz@gmail.com, ²sri.mulyati@budiluhur.ac.id

(* : corresponding author)

Abstrak-Dengan berkembangnya teknologi informasi saat ini, komunikasi mengalami kemajuan yang sangat pesat, mengakses suatu data atau informasi melalui bermacam-macam media salah satunya melalui media *website* dalam internet. Seseorang dengan mudah menyimpan, mengunduh, dan mengakses suatu data atau informasi. Keamanan dalam menyimpan dsuatu data atau sangatlah penting. Salah satu pengaruh negatif perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk mencegah kejahatan tersebut dalam penyimpanan data yang dianggap penting untuk mencegah kejahatan teknologi informasi. PT Sekawan menjadi khawatir jika akan menggunakan aplikasi tersebut tidak aman dan saat tersimpan kedalam *database*. Hal ini dikarenakan data dan informasi merupakan hal yang penting dan tetap rentan terhadap pencurian dan penyalahgunaan oleh pihak tertentu, yang dapat mengakibatkan kerugian yang besar. Oleh karena itu, dibuatlah aplikasi keamanan teks yang terenkripsi dalam *database* berbasis web yang dapat menjaga dan melindungi kerahasiaan data informasi. Dengan merancang aplikasi ini, penulis membuat suatu metode dengan cara proses enkripsi. Penulis akan menggunakan 2 (dua) algoritma kriptografi yaitu *Caesar Cipher* dan *Base64*. Kriptografi *Caesar Cipher* menggunakan kunci angka untuk enkripsi dan *Base64* sistem untuk mewakili data byte sebagai karakter *ASCII*. *Base64* menyediakan 6-bit *encoding* 8-bit *ASCII* karakter. Aplikasi ini dibuat menggunakan bahasa program *PHP*. Dan aplikasi kriptografi ini, mengharapkan informasi data barang, supplier, customer dan data transaksi akan aman dan tidak tersebar oleh pihak yang tidak bertanggung jawab. Berdasarkan implementasi dan pengujian program, dan mampu menjaga, melindungi kerahasiaan data informasi. Serta dapat memberikan manfaat bagi pihak PT. Sekawan dalam menjalankan tugas pokoknya, fungsi, dan peran dalam keamanan tekonologi.

Kata Kunci: *base64 decoding, base64 encoding, caesar cipher, database, kriptografi*

APPLICATION OF CAESAR CIPHER AND BASE64 CRYPTOGRAPHICTO SECURE GOODS DISTRIBUTOR AT PT. SEKAWAN

Abstract-Nowadays, the development of information and communication technology is growing fast. Access data or information through various media, one of which is through websites on the internet. Anyone can save, download, and access data or information. Security in the storage of data or information is a crucial thing. One of the negative impacts of technological developments is data theft. Data theft can make the owner lose. To avoid these crimes, security is needed in data storage, which is considered important to avoid information technology crimes. PT Sekawan is worried that using the application is not safe and when it is stored in the database, this is because data and information are important and remain vulnerable to theft and misuse by certain parties, which can cause huge losses. Therefore, an encrypted text security application is made in a web-based database that can maintain and protect the confidentiality of information. In designing this application, the author makes a method using the encryption process. The author will use 2 (two) cryptographic algorithms, namely *Caesar Cipher* and *Base64*. *Caesar Cipher* cryptography uses numeric keys for encryption and the *Base64* system to represent byte data as *ASCII* characters. *Base64* provides 6-bit encoding for 8-bit *ASCII* characters. This application is made using the *PHP* programming language. In this cryptographic application, it is expected information on goods, suppliers, customers, and transaction data will be safe and not spread by eavesdroppers or irresponsible parties. Based on program implementation and testing, and being able to maintain and protect the confidentiality of data and information. And can provide benefits for PT. Sekawan to carry out their main duties, functions, and roles in technology security.

Keywords: *base64 decoding, base64 encoding, caesar cipher, database, cryptography.*

1. PENDAHULUAN

Dengan berkembangnya teknologi informasi saat ini, komunikasi mengalami kemajuan yang sangat pesat, mengakses suatu data atau informasi melalui bermacam-macam media salah satunya melalui media *website* dalam internet. Seseorang dengan mudah menyimpan, mengunduh, dan mengakses suatu data atau informasi. Keamanan dalam menyimpan data atau informasi sangat penting dan tidak bisa diabaikan. Salah satu pengaruh negatif

perkembangan teknologi adalah pencurian data. Pencurian data ini tentunya merugikan bagi pemilik data, untuk mencegah kejahatan tersebut maka dibutuhkan pengamanan dalam penyimpanan data yang dianggap penting untuk mencegah kejahatan teknologi informasi.

Semua perusahaan didirikan dengan tujuan menghasilkan keuntungan dalam jangka panjang. Namun, perusahaan cenderung mengabaikan pentingnya keamanan data untuk mencapai tujuan mereka, itu sebabnya banyak perusahaan tidak terlalu memperhatikan keamanan data. Perusahaan harus memperhatikan apa yang dianggap penting oleh penggunanya, karena memperhatikan keamanan data adalah faktor penting dan sangat besar bagi kelangsungan hidup suatu perusahaan dalam persaingan. PT Sekawan merupakan perusahaan distributor barang textile yang didirikan pada tahun 1956. PT. Sekawan bergerak di bidang distributor menyalurkan barang textile untuk keperluan pabrik – pabrik textile di Indonesia. PT. Sekawan telah melayani berbagai customer di beberapa provinsi di Indonesia, sistem keamanan aplikasi dan keamanan data juga harus dijaga untuk memastikan bahwa data yang dimiliki perusahaan tidak dapat dibaca atau disalahgunakan oleh pihak yang tidak diinginkan. Maka dari itu, supaya tidak ada pihak yang berkepentingan yang dapat mengubah data yang telah tersimpan atau dapat mencuri data yang telah ada, diperlukan suatu metode yang dapat mengamankan data yang ada pada *database*. Penerapan kriptografi pada tugas akhir ini berfokus pada bagaimana kriptografi dapat mengamankan data yang tersimpan melalui sistem *database* yang aman hingga data tersebut dibuka oleh pihak yang berkepentingan.

Banyak cara yang dapat digunakan untuk mengamankan data, termasuk diantaranya kriptografi. Teknik- teknik tersebut memiliki fungsi yang berbeda, kriptografi dimaksudkan untuk menyamarkan sebuah pesan (*plaintext*) menjadi pesan (*chipertext*) susah dibaca atau di pahami.

Berdasarkan data di atas, pada saat memasukkan data ke dalam database, harus ada sistem keamanan informasi. Untuk melakukan ini, ada metode yang biasa dikenal sebagian penyajian data. Dalam penelitian ini, penulis akan mencoba mengimplementasikan ilmu matematika yang disebut kriptografi. Dengan kriptografi, data dapat diubah menjadi kata sandi yang tidak dipahami oleh siapa pun dan mengembalikannya ke bentuk aslinya, sebuah proses yang di kenal sebagai enkripsi dan dekripsi. Algoritma enkripsi sangat beragam. Dalam laporan tugas akhir ini, penulis menggunakan dua metode yaitu algoritma *Caesar Cipher* dan *Base64* untuk melakukan enkripsi dan dekripsi data pada sistem *database*.

2. METODOLOGI PENELITIAN

2.1 Data Penelitian

Data Penelitian berupa nama pelanggan, barang, transaksi, vendor diperoleh melalui tempat penelitian PT. Sekawan Data barang terdiri dari nama barang, satuan barang, kode vendor dan harga barang, seperti Tabel 3.2:

Tabel 3. 2 Data Barang

No.	Barang	Satuan	Supplier
1.	MINO WDG DRUM 665-5.01-C96X2.5/3.5 ALM	Pcs	NITTO SHOJI,LTD
2.	BRUSH SP-S-34-3	Pcs	SPAZZOLIFICIOBUSTESE S.A. S
3.	SPRING 13 110R	Pcs	MESDAN S.P.A.
4.	DIODA ZENER 18V	Pcs	IRO AB
5.	GUIDE 110 114	Pcs	MESDAN S.P.A.
6.	RING FLANGE	Pcs	KANAI JUYO
	KS2 45.0MMIDX54.0MM SD PC3 BF		KOGYO CO, LTD
7.	TRAVELLER TMYS-2/HF NO.1/0 (10.000PCS)	Box	KANAI JUYO KOGYO CO, LTD
8.	TRAVELLER OYHHINI NO.3 (10.000PCS)	Box	KANAI JUYO KOGYO CO., LTD
9.	STRIPPING FILLET HL 13M	Set	KANAI JUYO KOGYO CO., LTD
10.	WAX ROLL 15.2 X38 X 43MM 684 WHITE (2554)	Kgs	RESEDA BINDERGMBH & CO
11.	COVER GUIDE 3064941A	Pcs	MESDAN S.P.A.
12.	LEVER 80 4923B	Pcs	MESDAN S.P.A.
13.	O RING 64 4923B	Pcs	MESDAN S.P.A
14.	PISTON SEAL 11690	Pcs	CV DIZINDOANUGERAH
15.	CAP GRIPPER	Pcs	YUIL MULSAN

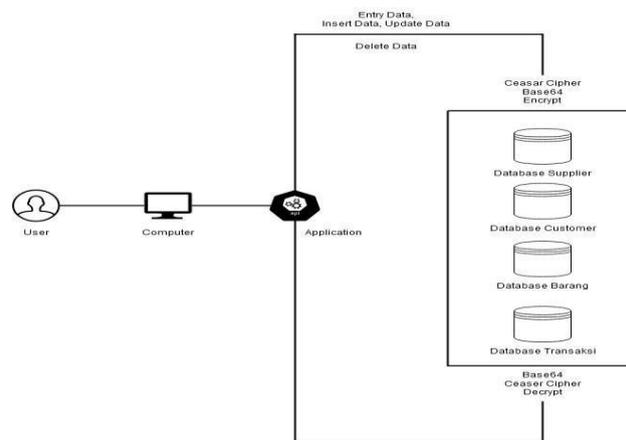
2.2 Metode Pembeding

Hasil tinjauan pustaka dapat disimpulkan perbedaan penelitian dengan penelitian sebelumnya, yaitu:

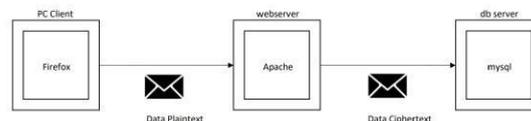
- Penelitian sebelumnya menerapkan data file dokumen dan email proses enkripsi dan dekripsi, sedangkan penelitian saat ini hanya enkripsi dan dekripsi data teks
- Penelitian sebelumnya hanya menggunakan kata kunci yang sama terhadap enkripsi dan dekripsi, sedangkan penelitian saat ini menggunakan kunci berbeda-beda pada saat enkripsi dan dekripsi
- Penelitian sebelumnya tidak menggunakan waktu enkripsi dan dekripsi, penelitian saat ini menggunakan waktu enkripsi dan dekripsi untuk mengetahui kecepatan proses.

2.3 Penerapan Metode

Dalam penerapan metode peneliti akan menjelaskan langkah penyelesaian metode dan arsitektur kerja sistem. Seperti yang di perlihatkan pada Gambar 2.1 dan 2.2 berikut ini:



Gambar 2.1 Cara Kerja Sistem Algoritma Caesar Cipher dan Base64

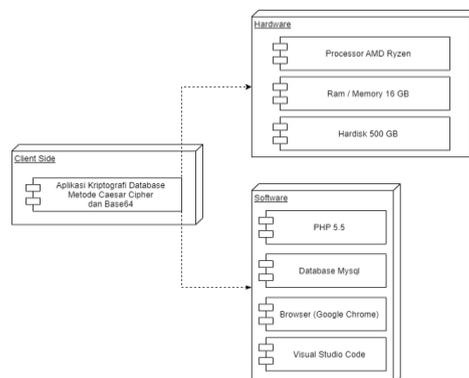


Gambar 2.2 Arsitektur Kerja Sistem Sederhana

3. HASIL DAN PEMBAHASAN

3.1 Lingkungan Percobaan

Pengimplementasian aplikasi ini memerlukan kelengkapan *hardware* dan *software* pendukung. Pembahasannya meliputi, terlihat pada Gambar 3.1:

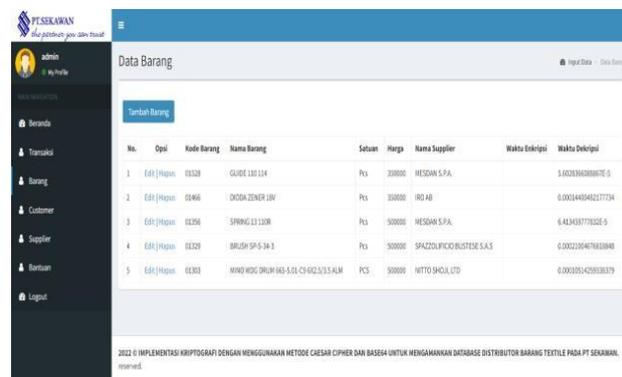


Gambar 3.1 Lingkungan Percobaan


```
|  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- |
| ```  <?php $i = 1; $db->connect(); $db->sql('SELECT A.*, B.*, A.time_encrypt as b_time_encrypt, A.time_decrypt as b_time_decrypt FROM barang A LEFT JOIN supplier B ON A.supplier_id = B.id_supplier ORDER BY id_barang DESC');  $res = $db->getResult();  foreach ($res as $k => $val) { $time_start = microtime(true); $decrypt_kode = base64_decode($cipher->decrypt($val['barang_kode'], $val['barang_key'])); $decrypt_nama = base64_decode($cipher->decrypt($val['barang_nama'], $val['barang_key'])); $decrypt_satuan = base64_decode($cipher->decrypt($val['barang_satuan'], $val['barang_key'])); $decrypt_harga = base64_decode($cipher->decrypt($val['barang_harga'], $val['barang_key'])); $decrypt_s_nama = base64_decode($cipher->decrypt($val['supplier_nama'], $val['supplier_key'])); }  <tr> <td> <?=$i> </td> <td> <a href=?=$helpers->base_url()->template.php?pb=barang-edit&id=?=$val['id_barang']?>Edit</a> <a onClick="return confirm('Apakah anda yakin ingin menghapus data ?>=$decrypt_nama?)" href=?=$helpers->base_url()->proses/delete.php?param=barang-delete&id=?=$val['id_barang']?> Hapus</a>  ``` | | | | | | | |

```

Gambar 3. 4 Layar Proses Dekripsi Barang



The screenshot shows a web application interface for 'PESEKURAN'. The main content area is titled 'Data Barang' and contains a table with the following data:

No.	Opis	Kode Barang	Nama Barang	Satuan	Harga	Nama Supplier	Waktu Enkripsi	Waktu Dekripsi
1	Edit/Hapus	0020	GLIDE 120 114	Pcs	30000	HESSIAN S.P.A.	5.00239408087E-5	
2	Edit/Hapus	0040	DODAZ ZENER 10V	Pcs	30000	IRO AB	0.000440442277734	
3	Edit/Hapus	0050	SPRING 11 110R	Pcs	50000	HESSIAN S.P.A.	6.413453777022E-5	
4	Edit/Hapus	0020	BRUSH SP-3 14-3	Pcs	50000	SPAZZOLPICO BUSIESTE S.A.S	0.0002204476830840	
5	Edit/Hapus	0030	WIND WDC DRUM 045-S-01-CV-02-S15-ALM	Pcs	50000	WITTO SINGU LTD	0.0003051425930379	

Gambar 3.5 Tampilan Data Barang yang telah Menjadi Teks Asli

a. Algoritma Proses Sistem Enkripsi Algoritma Caesar Cipher

Algoritma proses enkripsi ini menerangkan bagaimana cara kerja *Caesar Cipher* melakukan proses enkripsi sehingga menghasilkan *ciphertext*. Selama proses ini, *plaintext* diinterpretasikan menjadi *chiphertext* dan di proses menggunakan *Caesar Cipher*.

1. Masukkan plaintext
2. len = Panjang plaintext
3. P = Plaintext; S = Shift; C = Ciphertext4. i
4. = 0
5. for (i < len) do
6. ((P[i]+S) mod26)
7. i++
8. End For
9. write (ciphertext)

b. Algoritma Proses Sistem Dekripsi Algoritma Caesar Cipher

Algoritma dekripsi ini menerangkan bagaimana cara kerja sistem *Caesar Cipher* melakukan proses dekripsi sehingga menghasilkan teks asli atau *plaintext*.

```
1. Masukkan kunci
2. len = Panjang ciphertext
3. P = Plaintext; S = Shift; C = Ciphertext
4. for (I < len) do
5.     P[i] = ((C[i]-S) mod26)
6.     i++
7. end for
8. write (plaintext)
```

c. Algoritma Proses Sistem Enkripsi *Base64*

Algoritma alur kerja enkripsi ini menerangkan bagaimana cara kerja *Base64* melakukan proses enkripsi sehingga menghasilkan *ciphertext*. Selama proses ini, dilakukan implementasi *plaintext* menjadi *chipertext* yang kemudian akan diproses oleh *Base64*.

```
1. Start
2. Input Karakter ASCII
3. Konversi Index ASCII ke BINARY
4. Hitung Jumlah Keseluruhan Bit BINARY
5. If "Jumlah Bit" <= 24 Bit Then
6. Tambahkan dengan Bit 0 Hingga Berjumlah 24
7. Bagi Byte Menjadi Per Group Dengan Jumlah Bit 6 tiap Group
8. Konversi dari BINARY menjadi ASCII dengan Tabel Base 64
9. Tampilkan Hasil Encoding
10. Else
11. Bagi Bit Menjadi Per Group Dengan Jumlah Bit 6 tiap Group
12. If "Jumlah Bit" tidak bias dibagi 6 Then
13. Tambahkan dengan Bit 0 Hingga Dibagi 6
14. Konversi dari BINARY menjadi ASCII Dengan Tabel Base64
15. Else
16. Konversi dari BINARY menjadi ASCII dengan Tabel Base64
17. End If
18. End If
```

d. Algoritma Proses Sistem Dekripsi Algoritma *Base64*

Algoritma proses dekripsi ini menerangkan bagaimana cara kerja dekripsi *base64* melalui proses dekripsi sehingga berhasil menghasilkan teks asli atau *plaintext*.

```
1. Start
2. Input Karakter ASCII hasil Encoding Base64
3. Konversi Index ASCII ke BINARY dengan Tabel Base64
4. If Karakter = "=" Then
5. Kembalikan nilai Bit menjadi 0
6. Bagi Bit menjadi 8 Bit per kelompok
7. Konversi dari BINARY menjadi ASCII
8. Tampilkan Hasil Decoding
9. Else
10. Bagi bit menjadi 8 bit per kelompok
11. Konversi dari Binary menjadi ASCII
12. Tampilkan Hasil Decoding
13. End If
```

3.3 Analisa dalam Penjabaran Pengujian

Pengujian di lakukan menggunakan memastikan semua fitur enkripsi dan dekripsi sudah berjalan dengansesuai:

1. Fitur enkripsi di proses pada saat melakukan tambah data dan ubah data
2. Fitur dekripsi di proses pada saat melakukan tampil data
3. Semua fitur tambah tampil ubah dan hapus pada menu transaksi, barang, supplier, dan customer padapengujian enkripsi dan dekripsi berjalan sesuai

3.3.1 Tampilan Layar Login

Berikut adalah Tampilan Layar Halaman Login saat pertama user akses aplikasi, terlihat di Gambar 3.6:



Gambar 3.6 Tampilan Login

3.3.2 Tampilan Layar Beranda

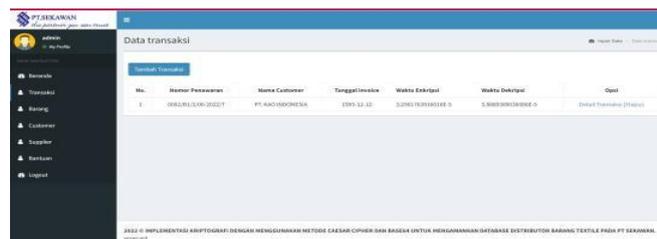
Berikut adalah Tampilan Layar Halaman Barang yaitu Halaman utama setelah *user* berhasil login, diperlihatkan pada Gambar 3.7 dibawah ini:



Gambar 3. 7 Beranda

3.3.3 Tampilan Layar Tampil Transaksi

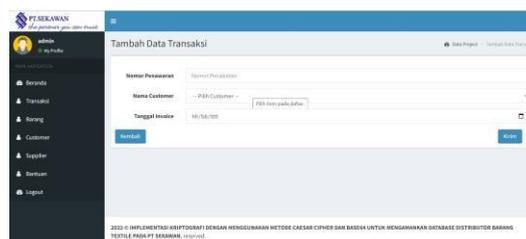
Berikut adalah Tampilan Layar Transaksi yaitu tampil data transaksi yang sudah di proses dekripsi dari table transaksi, lalu menampilkan data nomor penawaran, nama customer, dan tanggal invoice, diperlihatkan pada Gambar 3.8 dibawah ini:



Gambar 3. 8 Layar Tampilan Transaksi

3.3.4 Tampilan Layar Tambah Transaksi

Berikut adalah Tampilan Layar Tambah Transaksi yaitu form tambah data transaksi untuk memproses enkripsi dengan cara user memasukan data transaksi lalu sistem mengenkripsi data transaksi, diperlihatkan pada Gambar 3.9 dibawah ini:



Gambar 3. 9 Layar Tambah Transaksi



Gambar 3.13 Ubah Data *Customer*

3.3.9 Tampilan Layar Tampil *Customer*

Berikut adalah Tampilan Layar *Customer* yaitu tampil data barang yang sudah di proses dekripsi dari table *customer*, lalu menampilkan data kode customer, nama customer, email *customer* dan phone *customer*, dan alamat *customer*, di perlihatkan pada Gambar 3.14:

No.	Kode Customer	Nama	CP	Phone	Email	Cabang	Alamat	Maksud Deskripsi	Maksud Deskripsi
1	001	001	001	001	001	001	JL. TOGOL BELLENDONG 1 RT 011 R010A BELLENDONG CIRUGU, SUBANG	001	001
2	002	002	002	002	002	002	JL. TOGOL BELLENDONG 1 RT 011 R010A BELLENDONG CIRUGU, SUBANG	002	002
3	003	003	003	003	003	003	JL. TOGOL BELLENDONG 1 RT 011 R010A BELLENDONG CIRUGU, SUBANG	003	003
4	004	004	004	004	004	004	JL. TOGOL BELLENDONG 1 RT 011 R010A BELLENDONG CIRUGU, SUBANG	004	004
5	005	005	005	005	005	005	JL. TOGOL BELLENDONG 1 RT 011 R010A BELLENDONG CIRUGU, SUBANG	005	005

Gambar 3. 84 Tampil *Customer*

4. PENUTUP

4.1 Kesimpulan

Berdasarkan analisis yang telah dilakukan mulai dari pengumpulan data hingga pemecahan masalah, serta pengembangan aplikasi ini, maka dapat membuat kesimpulan dan saran yang perlu diperhatikan agar sistem ini dapat berfungsi dengan baik.

- Dari hasil implementasi yang sudah dilakukan dapat diketahui bahwa kriptografi dapat digunakan untuk melindungi data dan informasi yang disimpan ke dalam record *database*.
- Diimplementasikan menggunakan bahasa pemrograman *PHP* dengan menggunakan algoritma *CaesarCipher*, dan *Base64* untuk enkripsi dan dekripsi.
- Dalam *system* keamanan penyandian sederhana kita dapat menggunakan metode *Caesar Cipher* dan *base64* untuk melakukan enkripsi dan dekripsi.

4.2 Saran

Untuk lebih menyempurnakan aplikasi ini, saran untuk pengembangan lebih lanjut dari aplikasi ini diantara lain:

- Dibutuhkan suatu percobaan penerapan metode konversi teks pada gambar video.
- Sistem masih sangat sederhana, diharapkan dapat menambahkan fitur seperti laporan penjualan dan laporan pembelian.
- Untuk ke depannya aplikasi ini bisa disempurnakan, serta diperbaharui setiap item yang tersedia dalam sistem aplikasi sehingga dapat mengikuti perkembangan zaman.

DAFTAR PUSTAKA

- [1] M. Fadlan, Haryansyah and Rosmini, "Perpaduan Algoritma Kriptografi Atbash dan Autokey Cipher dalam Mengamankan Data," *Jurnal Media Informatika Budidarma*, vol. 5, no. 3, pp. 806-812, 2021.
- [2] A. Hermawan and I. Erik, "Implementasi Enkripsi Data Menggunakan Kombinasi AES dan RSA," *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 5, no. 2, pp. 326-330, 2021.
- [3] E. S. Marsian, I. Setiadi and A. Cahyo, "Implementasi Sistem Keamanan Aes 256-Bit Gcm Guna Mengamankan Data Pribadi," *JRKT (Jurnal Rekayasa Komputasi Terapan)*, vol. 1, no. 2, pp. 108-114, 2021.

- [4] Siswanto, A. Saputro, G. P. Utama and H. P. B, “Penerapan Algoritma Kriptografi Twofish Untuk Mengamankan Data File,” *Jurnal BIT*, vol. 18, no. 1, pp. 9-18, 2021.
- [5] Y. D. Putri, Rosihan and S. Lutfi, “Penerapan Kriptografi Caesar Cipher Pada Fitur Chatting Sistem Informasi Freelance,” *Jurnal Informatika dan Ilmu Komputer (JIKO)*, vol. 2, no. 2, pp. 87-94, 2019.
- [6] D. Nurani, “Perancangan Aplikasi Email Menggunakan Algoritma Ceaser Cipher dan Base64,” *Jurnal Informatika Sunan Kalijaga*, vol. 2, no. 3, pp. 175-180, 2018.
- [7] N. A. Saputri, and N. E. Sari, “Implementasi Pengamanan Data Dan Informasi Di Balai Desa Tanding Marga Dengan Metode Steganografi Lsb dan Algoritma Kriptografi Aes,” *Jurnal Informanika*, vol. 7, no. 1, pp. 63-71 2021.
- [8] N. E. Saragih, “Implementasi Algoritma ONE TIME PAD Pada Pesan,” *Jurnal Ilmiah MATRIK*, vol. 20, no. 1, pp 31-40, 2018.
- [9] Siswanto, M. Anif and W. Gata, “Penerapan Algoritma Kriptografi Tea dan Base64 Untuk Mengamankan Email,” *Jurnal ELTIKOM*, vol. 2, no. 1, pp. 34-41, 2018.
- [10] S. V. Wahdani, et al, “Pengamanan Data Pelanggan dan Penjualan Menggunakan Implementasi Kriptografi Metode RSA,” *Journal of Informatics Management and Information Technology*, vol. 5, no. 1, pp. 101-107, 2021.