

Implementasi Keamanan Data Dana Desa Dengan Metode Railfence Cipher Dan Beaufort Cipher (Studi Kasus Kantor Desa Atualuo)

Design of Building Material Sales Application (Case Study: Holimas Home) Based on Android

Tenida Gulo^{a,1}, Muhammad Taufiq Rustam^{b,2}

^a Program Studi Informatika, Fakultas Teknik Dan ilmu komputer , Mahasiswa Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia

^b Dosen Universitas Potensi Utama, Jl.K.L Yos Sudarso KM 6.5 Tj.Mulia, Medan, 20241, Indonesia
E-mail: tenidagulo@gmail.com¹, taufiqasfa2013@gmail.com²

ABSTRAK

Masalah yang terjadi adalah data dana desa tidak memiliki keamanan pada isi recordnya, sehingga dapat diketahui oleh pihak yang tidak diizinkan. Data pribadi pada data dana desa dapat disalahgunakan oleh pihak yang tidak diizinkan diantaranya potensi penipuan, pencemaran nama baik dan pemanfaatan data. Oleh karena itu diperlukan sebuah cara agar isi data dana desa tidak dapat diketahui pihak yang tidak diizinkan. Peneliti menggunakan komputer untuk membuat sebuah aplikasi yang dapat mengamankan isi data dana desa, ilmu komputer yang dapat digunakan adalah kriptografi. Namun untuk dapat mengamankan data dana desa menggunakan teknik kriptografi dibutuhkan metode yang tepat sehingga keamanan data menjadi lebih baik. Penelitian ini menggunakan metode Beaufort Cipher untuk mengatasi masalah keamanan data dana desa. Beaufort cipher adalah salah satu varian dari vigenere cipher dimana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada vigenere cipher. Akan tetapi peneliti menambahkan metode yang lain sehingga mendapatkan kekuatan keamanan data yang lebih baik. Oleh karena itu peneliti menggunakan metode Beaufort cipher untuk menambahkan kekuatan kerahasiaan data dana desa. Beaufort cipher merupakan salah satu algoritma dalam teknik keamanan. Dengan adanya metode Railfence Cipher dan Beaufort Cipher maka data dana desa mendapatkan keamanan pada isi datanya.

Kata Kunci : Keamanan Data, Railfence Cipher, Beaufort Cipher

ABSTRACT

The problem that occurs is that village fund data does not have security in the contents of the records, so it can be known by unauthorized parties. Personal data in village fund data can be misused by unauthorized parties, including potential fraud, defamation and use of data. Therefore, a way is needed so that the contents of village fund data cannot be known by unauthorized parties. Researchers use computers to create an application that can secure the contents of village fund data. The computer science that can be used is cryptography. However, to be able to secure village fund data using cryptographic techniques, appropriate methods are needed so that data security is better. This research uses the Beaufort Cipher method to overcome the problem of village fund data security. The Beaufort cipher is a variant of the Vigenere cipher where the method for encrypting and decrypting is almost the same as encrypting and decrypting the Vigenere cipher. However, researchers added other methods to get better data security. Therefore, researchers use the Beaufort cipher method to increase the confidentiality of village fund data. Beaufort cipher is an algorithm in security techniques. With the Railfence Cipher and Beaufort Cipher methods, village fund data has security in its data contents.

Keywords: Data Security, Railfence Cipher, Beaufort Cipher

Info Artikel :

Disubmit: 5 Oktober 2023

Direview: 9 November 2023

Diterima : 1 Desember 2023

Copyright © 2024 - Journal UPU. All rights reserved.

1. PENDAHULUAN

Desa Atualuo merupakan salah satu desa yang ada di kecamatan Ma'u, kabupaten Nias, provinsi

Sumatra Utara, Indonesia. Desa Atualuo memiliki beberapa pegawai yang mengelola desa dari segi pendanaan dan aktifitas desa.

Setiap kebutuhan desa dicatat dan disimpan ke dalam aplikasi MS. Excel. Dana Desa merupakan jumlah anggaran dana yang dialokasikan pada desa dari pemerintahan. Pengelola dana desa di desa atualuo adalah bendahara pengelola KASI dan KAUR yang melaksanakan kegiatan di lapangan sesuai dengan Rencana Anggaran Biaya (RAB).

Masalah yang terjadi adalah data dana desa tidak memiliki keamanan pada isi *recordnya*, sehingga dapat diketahui oleh pihak yang tidak diizinkan. Data pribadi pada data dana desa dapat disalahgunakan oleh pihak yang tidak diizinkan diantaranya potensi penipuan, pencemaran nama baik dan pemanfaatan data. Oleh karena itu diperlukan sebuah cara agar isi data dana desa tidak dapat diketahui pihak yang tidak diizinkan. Peneliti menggunakan komputer untuk membuat sebuah aplikasi yang dapat mengamankan isi data dana desa, ilmu komputer yang dapat digunakan adalah kriptografi. Namun untuk dapat mengamankan data dana desa menggunakan teknik kriptografi dibutuhkan metode yang tepat sehingga keamanan data menjadi lebih baik.

Penelitian ini menggunakan metode *Beaufort Cipher* untuk mengatasi masalah keamanan data dana desa. *Beaufort cipher* adalah salah satu varian dari *vigenere cipher* dimana cara melakukan enkripsi dan dekripsi hampir sama dengan melakukan enkripsi dan dekripsi pada *vigenere cipher*. Akan tetapi peneliti menambahkan metode yang lain sehingga mendapatkan kekuatan keamanan data yang lebih baik. Oleh karena itu peneliti menggunakan metode *Beaufort cipher* untuk menambahkan kekuatan kerahasiaan data dana desa. *Beaufort cipher* merupakan salah satu algoritma dalam teknik keamanan. Dengan adanya metode *Railfence Cipher* dan *Beaufort Cipher* maka data dana desa mendapatkan keamanan pada isi datanya.

2. METODE

Algoritma *Railfence* adalah salah satu bentuk cipher transposisi yang sederhana yang diinspirasi dari model *Polybius square*. *Polybius square* adalah menyusun huruf sebagai matriks 5x5 dan mengkodekan huruf A sebagai 1-1, huruf B sebagai 1-2 dan seterusnya. Setiap karakter pada *Polybius square* diganti dengan indeks cell matriks tanpa menggunakan kunci khusus dan hanya merubah posisi sehingga teks tidak terbaca. *Railfence* atau biasa disebut alur pagar adalah bentuk penyandian transposisi dengan cara menuliskan huruf-huruf teks asli secara turun naik dalam sebuah pagar imajiner. Teks sandinya dibaca secara baris per baris. *Beaufort cipher* merupakan salah satu algoritma dalam teknik keamanan kriptografi klasik. Kunci (K) pada *beaufort cipher* adalah urutan karakter-karakter $K = k_1 \dots k_d$ dimana k_1 didapat dari banyaknya pergeseran dari alfabet ke-i sama seperti *vigenere cipher*. Artinya bahwa jumlah kunci yang dibangkitkan harus sama dengan jumlah karakter *plaintext* yang diamankan.

Algoritma Enkrip *beaufort cipher*:

$$C_i = 256 - (P_i + K_i) \bmod 256$$

Dimana:

C : Ciphertext hasil proses enkrip

P : Plaintext untuk proses enkrip

K : Key untuk proses enkrip

mod : Sisa bagi

256 : Total ASCII pada keyboard

Algoritma Dekrip *beaufort cipher*:

$$P_i = 256 - (C_i + K_i) \bmod 256$$

Dimana:

P : Plaintext hasil proses dekrip

C : Ciphertext untuk proses dekrip

K : Key untuk proses dekrip

mod : Sisa bagi

256 : Total ASCII pada keyboard. [6].

Gambar 1. Data Dana Desa Aktualuo Rincian
(Sumber: Desa Aktualuo, 2023)

Tujuan: Mendukung Pelaksanaan Peraturan Bupati Nias Nomor 12 Tahun 2022
 dalam hal ini sebagai berikut:

1. bahwa, berdasarkan Peraturan Bupati Nias Nomor 12 Tahun 2022
 tentang Pedoman Penyusunan Anggaran Pendapatan dan Belanja Desa di
 Kabupaten Nias, Kepala Desa Atualuo bersama Badan Permusyawaratan
 Desa Atualuo dan seluruh peserta musyawarah telah menyetujui Peraturan
 Desa Atualuo tentang Anggaran Pendapatan dan Belanja Desa (APBDesa)
 Atualuo Tahun Anggaran 2023.
2. bahwa, berdasarkan APBDesa Atualuo Tahun Anggaran 2023 untuk
 masing-masing pos anggaran pendapatan dan belanja desa, secara rinci
 disusun dan dipaparkan dalam lampiran Peraturan Desa Atualuo tentang
 Anggaran Pendapatan dan Belanja Desa Atualuo Tahun Anggaran 2023
 yang merupakan bagian tidak terpisahkan dari dokumen peraturan desa.
3. bahwa, penjabaran dimaknai pada poin 2 di atas sebagai berikut:

1. PendapatanDesa	Rp.	1.256.640.833,-
a. Pendapatan Asli Desa	Rp.	
b. Pendapatan Transfer	Rp.	1.256.640.833,-
c. Lain-lain Pendapatan Desa yang sah	Rp.	
2. BelanjaDesa	Rp.	1.387.508.880,-
a. Bidang Penyelenggaraan Pemerintahan	Rp.	477.806.200,-
b. Bidang Pengembangan Desa	Rp.	
c. Bidang Pengembangan	Rp.	103.432.000,-
d. Bidang Pembinaan Masyarakat	Rp.	69.167.000,-
e. Bidang Pemberdayaan Masyarakat	Rp.	249.504.200,-
f. Bidang Penanggulangan Bencana	Rp.	487.496.480,-
Surplus/Defisit	Rp.	(130.868.047)
3. Pembiayaan	Rp.	
a. Penerimaan Pembiayaan	Rp.	131.815.295,-
b. Pengeluaran Pembiayaan	Rp.	
Sisa Lebih/(Kurang) Perhitungan Anggaran	Rp.	950.288,-

Gambar 2. Data Dana Desa Atualuo Total
 (Sumber: Desa Atualuo, 2023)

Rail Fence Cipher merupakan salah satu variasi implementasi *cipher* transposisi. Pada *Rail Fence Cipher*, plaintexts dituliskan secara vertikal ke bawah sepanjang *n-rails*, dan menulis lagi ke kolom baruketika telah mencapai karakter ke-*n*. Cipherteks yangdihasilkan adalah urutan karakter yang dibaca secarahorizontal.

Studi Kasus:

Berikut ini contoh enkripsi dari penerapan metode *rail fence cipher*:

Plaintext : Rp.1256640833

Key : 3

R	1	6	0	3
P	2	6	8	
.	5	4	3	

Hasil enkripsi *Railfence Cipher*

Ciphertext: R1603p268 .543

Berikut ini contoh Dekripsi dari penerapan metode *rail fence cipher*:

Hitung Jumlah Karakter *Ciphertext*, selanjutnya Bagikan dengan Nilai Kunci Dekripsi, Maka hasilnya sebagai Kunci Dekripsi.

Ciphertext:

R1603p268 .543= 15

Key Lama : 3

Key Dekripsi: 15/3 = 5

R	p	.
---	---	---

1	2	5
6	6	4
0	8	3
3		

Plaintext:Rp.1256640833

Metode Beaufort cipher

Beaufort cipher merupakan salah satu algoritma dalam teknik keamanan kriptografi klasik. Kunci (K) pada *beaufort cipher* adalah urutan karakter-karakter $K = k_1 \dots k_d$ dimana k_1 didapat dari banyaknya pergeseran dari alfabet ke-i sama seperti *viginere cipher*. Berikut ini adalah langkah-langkah dan contoh enkripsi dan dekripsi dari metode *beaufort cipher*:

1. Enkrip

Algoritma Enkrip *beaufort cipher*:

$$C_i = 256 - (P_i + K_i) \bmod 256$$

Dimana:

C : *Ciphertext* hasil proses enkrip

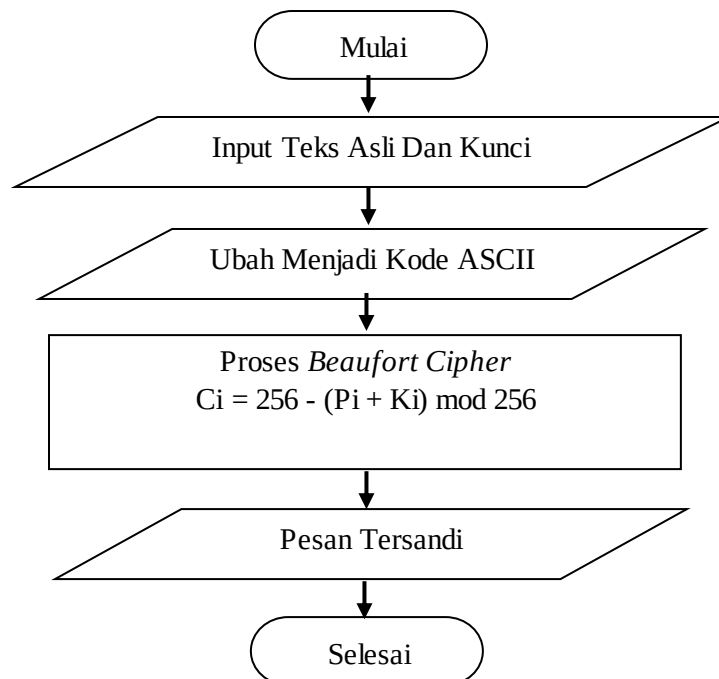
P : *Plaintext* untuk proses enkrip

K : *Key* untuk proses enkrip

mod : Sisa bagi

256 : Total ASCII pada *keyboard*

Flowchart enkripsi metode *beaufort cipher*:



Gambar 3. Flowchart Enkripsi *Beaufort Cipher*

Contoh Proses Enkrip:

Plaintext : Rp.1256640833

Key : 12

Solusi:

P	R	p	.	1	2	5	6	6	4	0	8	3	3	
---	---	---	---	---	---	---	---	---	---	---	---	---	---	--

256	256	256	256	256	256	256	256	256	256	256	256	256	256	-
Asc	82	112	46	49	50	53	54	54	52	48	56	51	51	+
K	49	50	49	50	49	50	49	50	49	50	49	50	49	=
C	125	94	161	157	157	153	153	152	155	158	151	155	156	

Ciphertext: }^iœœ^{TMTM}ž—>œ

2. Dekrip

Algoritma Dekrip *beaufort cipher*:

$$P_i = 256 - (C_i - K_i) \bmod 256$$

Dimana:

P : Plaintext hasil proses dekrip

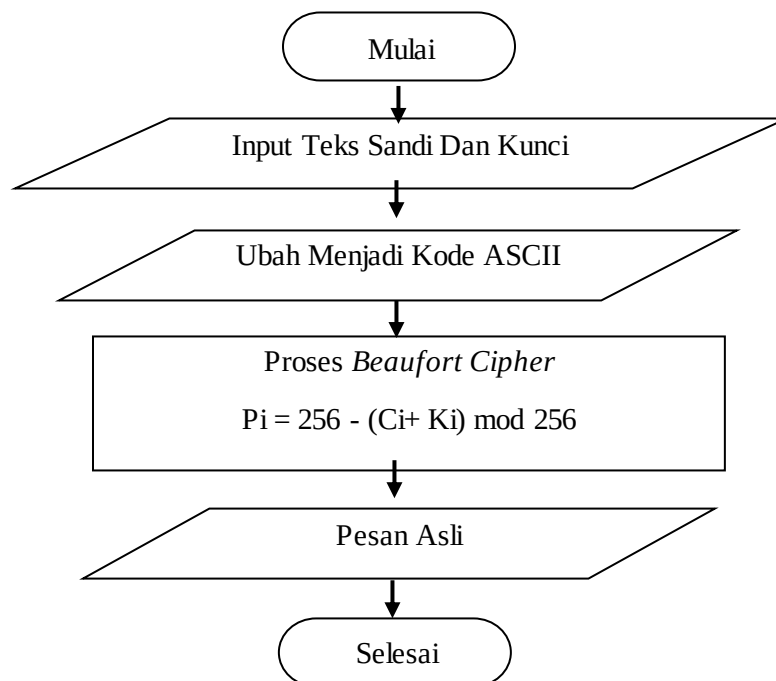
C : Ciphertext untuk proses dekrip

K : Key untuk proses dekrip

mod : Sisa bagi

256 : Total ASCII pada keyboard

Flowchart dekripsi metode *beaufort cipher*:



Gambar 4. Flowchart Dekripsi *Beaufort Cipher*

Berikut adalah contoh dekrip:

Contoh Proses Dekrip:

Ciphertext: }^iœœ^{TMTM}ž—>œ

Key : 12

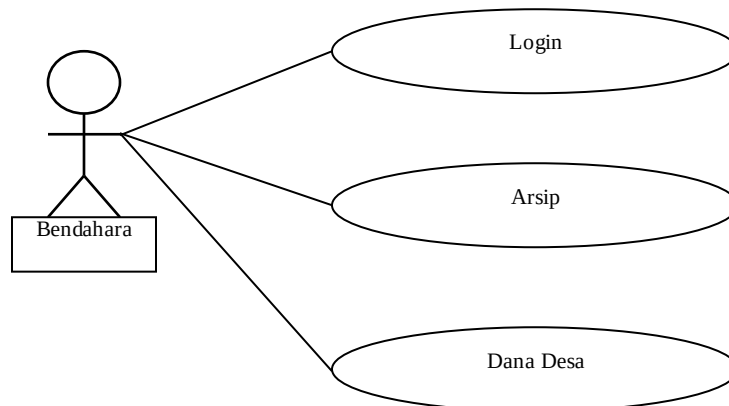
Solusi:

C	}	^	i	œ	œ	TM	TM	~	>	ž	—	>	œ	
256	256	256	256	256	256	256	256	256	256	256	256	256	256	-

Asc	125	94	161	157	157	153	153	152	155	158	151	155	156	+
K	49	50	49	50	49	50	49	50	49	50	49	50	49	=
P	82	112	46	49	50	53	54	54	52	48	56	51	51	

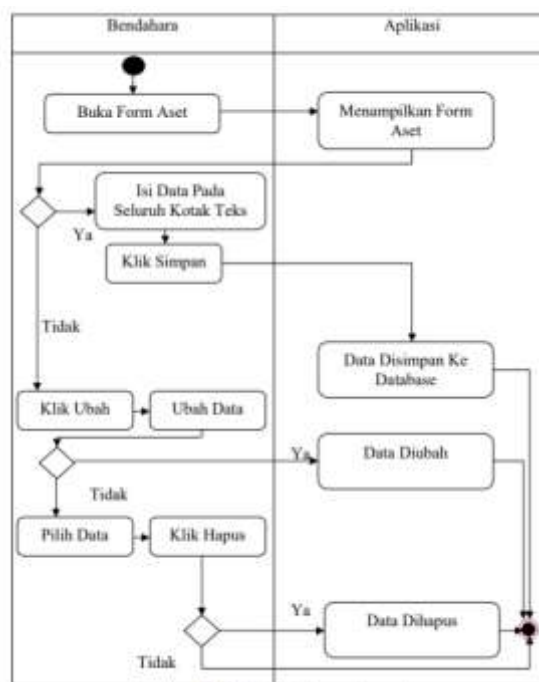
Plaintext: Rp.1256640833

Use case diagram keamanan basis datamenggunakan metode *railfence cipher* dan *beaufort cipher* dapat dilihat pada gambar 3.



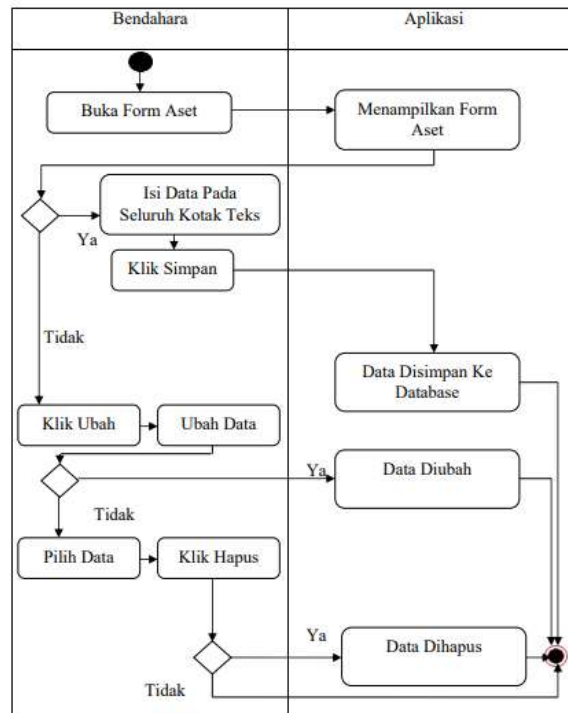
Gambar 5. Use Case Diagram

Gambar 6 merupakan *Activity Diagram Form Aset* dari Aplikasi Implementasi Keamanan Data Dana Desa Dengan Metode *Railfence Cipher* dan *Beaufort Cipher* (Studi Kasus Kantor Desa Atualuo).



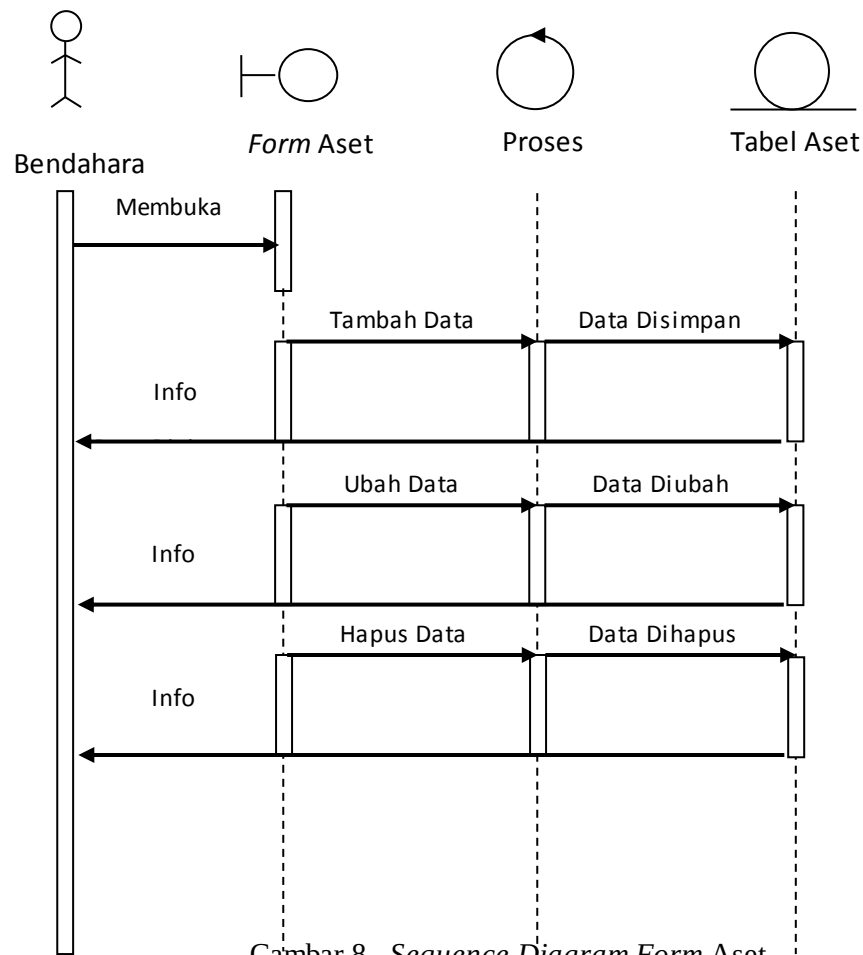
Gambar 6. Activity Diagram Form Aset

Gambar 7 merupakan *Activity Diagram Form Dana Desa* dari Aplikasi Implementasi Keamanan Data Dana Desa Dengan Metode *Railfence Cipher* dan *Beaufort Cipher* (Studi Kasus Kantor Desa Atualuo).



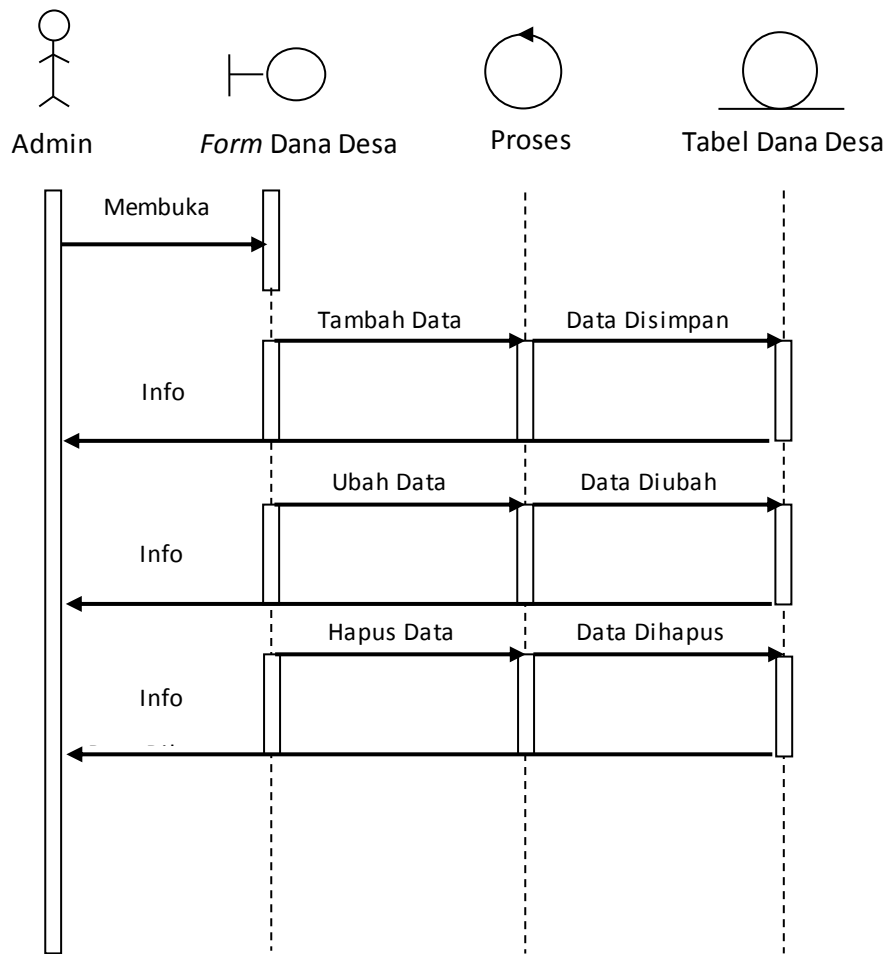
Gambar 7. Activity Diagram Form Dana Desa

Gambar 8 merupakan *Sequence Diagram Form Aset Aplikasi Implementasi Keamanan Data Dana Desa Dengan Metode Railfence Cipher dan Beaufort Cipher* (Studi Kasus Kantor Desa Atualuo).



Gambar 8. *Sequence Diagram Form Aset*

Gambar 9 merupakan *Sequence Diagram Form Dana Desa* Aplikasi Implementasi Keamanan Data Dana Desa Dengan Metode *Railfence Cipher* dan *Beaufort Cipher* (Studi Kasus Kantor Desa Atualuo).

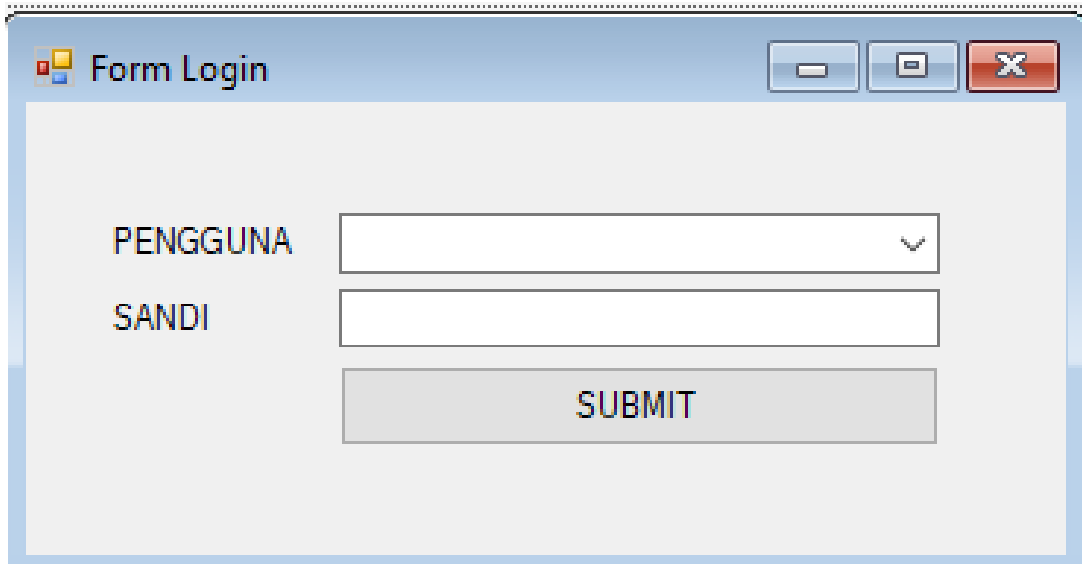


Gambar 9. Sequence Diagram Form Dana Desa

B. Hasil

1. Tampilan Form Login

Tampilan Form Login berfungsi menampilkan form login. Adapun Tampilan Form Login dapat dilihat pada Gambar 4. sebagai berikut:



Gambar 4. Tampilan *Form Login*

2. Tampilan *Form Menu*

Tampilan *Form Menu* berfungsi menampilkan *form Menu*. Adapun Tampilan *Form Menu* dapat dilihat pada Gambar 5. sebagai berikut:



Gambar 5. Tampilan *Form Menu*

3. Tampilan *Form Arsip*

Tampilan *Form Arsip* berfungsi menampilkan *form Arsip*. Adapun Tampilan *Form Arsip* dapat dilihat pada Gambar 6. sebagai berikut:

Gambar 6. Tampilan *Form* Arsip

4. Tampilan *Form* Dana Desa

Tampilan *Form* Dana Desa berfungsi menampilkan *form* Arsip. Adapun Tampilan *Form* Dana Desa dapat dilihat pada Gambar 7. sebagai berikut:

Gambar 7. Tampilan *Form* Dana Desa

4. KESIMPULAN

Berdasarkan pembahasan dari bab-bab sebelumnya yang telah dilakukan maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Dengan menerapkan kriptografi Metode *Railfence Cipher* dan *Beaufort Cipher* maka data dana desa mendapatkan keamanan.

2. Dengan menggunakan data dana desa dan kunci yang ditentukan, kemudian data teks dari data dana desadan kunci diubah menjadi ASCII maka dapat menerapkan metode *Railfence Cipher* dan *Beaufort Cipher* untuk keamanan data dana desa.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Universitas Potensi Utama yang telah banyak memberikan masukan dan saran dalam penyelesaian Skripsi ini.

REFERENSI

- [1] D. Purnamasari, "Implementasi Algoritma Kriptografi Caesar Cipher dan Rail Fence Cipher untuk Keamanan Data Teks Menggunakan Python," *E-Journal.Ivet.Ac.Id*, vol. 4, pp. 1–7, 2021, [Online]. Available: <http://e-journal.ivet.ac.id/index.php/jiptika/article/view/1697>
- [2] D. Febriani, D. F. Purba, and R. Puspasari, "Penerapan Algoritma Rail Fence Untuk Penghasil Pesan Rahasia Berbasis Android," *E-Journal.Potensi-Utama.Ac.Id*, pp. 745–756, 2020, [Online]. Available: <http://e-journal.potensi-utama.ac.id/ojs/index.php/FTIK/article/view/921>
- [3] M. H. Jannah and H. Aspriyono, "1527-Article Text-4658-1-10-20211126 (1)," vol. 6, no. 2, 2021.
- [4] D. Setiyadi, R. . Arifin, and Henderi, "Fungsi Date dalam Data Manipulation Language Menggunakan Bahasa Query dengan SQL Server," *Informatics Educ. Prof.*, vol. 4, no. 2, pp. 163–172, 2020.
- [5] T. Zebua, "Penerapan Multiply With Carry Generator pada Proses Pembangkitan Kunci Algoritma Beaufort Cipher," vol. 4, no. 2, pp. 607–613, 2023, doi: 10.47065/josh.v4i2.2928.
- [6] A. Abiyuda and L. Nababan, "Jurnal InSeDS (Information System and Data Science) Rancang Bangun Aplikasi Chatting Dengan Wireless LAN Menggunakan Metode Beaufort Cipher," vol. 1, no. 2, 2023.
- [7] A. S. Salabi, "Efektivitas Dalam Implementasi Kurikulum Sekolah," *Educ. Achievement J. Sci. Res.*, vol. 1, no. 1, p. 13, 2020.
- [8] E. Rusilawati, C. Angkasa, A. A. Purwati, and M. L. Hamzah, "Online Consumer Review , Keamanan dan Persepsi Risiko Terhadap Keputusan Pembelian Online Disitus Jual Beli Shopee," *Manag. Stud. Entrep. J.*, vol. 3, no. 2, pp. 606–617, 2022.
- [9] M. Olva, R. Dwiputri Permatasari, S. Majid, P. Syair, and A. Suganda, "Pemanfaatan Dasbor pada Pemantauan Data Transaksi Penjualan," *J. Eng. Technol. Appl. Sci.*, vol. 3, no. 1, pp. 1–15, 2021, doi: 10.36079/lamintang.jetas-0301.188.
- [10] P. D. K. Pardede, D. J. Tafonao, and E. E. Buulolo, "Optimalisasi Penggunaan Dana Desa Dalam Pembangunan Desa Lolosoni Kecamatan Gomo Kabupaten Nias Selatan 2019/2020," *J. Gov. Opin.*, vol. 6, no. 2, pp. 78–89, 2021.
- [11] S. J. Dinata, "Implementasi Algoritma Penyandian Transposisi Rail Fence Pada Data Rekam Medis," *Ejurnal.Stmik-Budidarma.Ac.Id*, vol. 7, no. 3, pp. 305–309, 2020, [Online]. Available: <https://www.ejurnal.stmik-budidarma.ac.id/index.php/inti/article/view/2406>
- [12] E. Helmud, "Optimasi Basis Data Oracle Menggunakan Complex View Studi Kasus : Pt. Berkat Optimis Sejahtera (Pt.Bos) Pangkalpinang," *J. Inform.*, vol. 7, no. 1, pp. 80–86, 2021.
- [13] E. R. Dewi, J. Hutabarat, and J. H. G. W., "Rancang Bangun Sistem Informasi Persediaan Bahan Baku Menggunakan Microsoft Visual Studio," *J. Valtech*, vol. 4, no. 2, pp. 26–33, 2021, [Online]. Available: <https://ejournal.itn.ac.id/index.php/valtech/article/view/3820>

- [14] Y. N. S. Monikha Oktra Bella, “Siswa Baru Berbasis Android Pada Sma Muhammadiyah Jarai,” *J. Siskomti*, vol. 4, no. 2, pp. 8–15, 2020.