KEAMANAN DATA HASIL E-VOTING PEMILIHAN KEPALA DESA DENGAN ALGORITMA VIGENERE CIPHER PERTUKARAN KUNCI THREE PAS PROTOCOL PADA KECAMATAN BARUS KABUPATEN TAPANULI TENGAH

E-VOTING DATA SECURITY OF VILLAGE HEAD ELECTION WITH VIGENERE CIPHER ALGORITHM THREE PASS PROTOCOL KEY EXCHANGE IN BARUS DISTRICT CENTRAL TAPANULI REGENCY

Aprizaldi Isnan Simamora[1)], Oris Krianto Sulaiman,ST,M.Kom[2)], Mhd. Zulfansyuri Siambaton,ST,M.Kom[3)]

[1),2),3)]Program Studi Teknik Informatika, [1),2),3)]Universitas Islam Sumatera Utara,

e-mail: [1)]aprizaldyisnan@gmail.com, [2)]Oris.ks@ft.uisu.ac.id, [3)]zulfansyuri@ft.uisu.ac.id

ABSTRAK

Prosedur pemungutan suara yang digunakan dalam istilah *e-voting* memungkinkan pemilih untuk memberikan suara yang aman, rahasia, dan terjamin. untuk memastikan keamanan dan kerahasiaan data tersebut dapat dilakukan dengan menggunakan algoritma kriptografi *vigenere cipher*. Algoritma *vigenere cipher* menggunakan sebuah kunci pada saat melakukan enkripsi dan dekripsi. Oleh karena itu, untuk menghindari adanya pendistribusian kunci maka pada penelitian ini algoritma *vigenere cipher* akan dibantu dengan skema *three pass protocol*. Penelitian ini bertujuan untuk mengetahui bagaimana membuat aplikasi *e-voting* pemilihan kepala desa dengan menerapkan algoritma *vigenere cipher* dan skema *three pass protocol*. Algoritma *vigenere cipher* dan skema *three pass protocol* yang diterapkan pada aplikasi *e-voting* kepala desa ini berhasil diimplementasikan dengan baik dengan melihat hasil *plaintext* sebelum dilakukan enkripsi dan setelah dilakukan enkripsi yang ditampilkan pada *user* sebelum memilih kandidat serta dengan adanya skema *three pass protocol* sehingga attacker tidak dapat dengan mudah melakukan dekripsi hasil enkripsi suara dikarenakan *ciphertext* memiliki 3 kunci yang berbeda dengan menggunakan algoritma *vigenere cipher*.

Kata Kunci: *E-voting, Vigenere Cipher, Three Pass Protocol*

ABSTRACT

The voting procedure used in the term e-voting allows voters to cast a safe, confidential and secure vote. to ensure the security and confidentiality of the data can be done by using the cryptographic algorithm vigenere cipher. The vigenere cipher algorithm uses a key when performing
encryption and decryption. Therefore, to avoid any distribution
key, in this study the vigenere cipher algorithm will be assisted by a three pass protocol scheme. This study aims to find out how to make an e-voting application for village head elections by applying the vigenere cipher algorithm and three pass protocol scheme. The vigenere cipher algorithm and the three pass protocol scheme applied to the village head's e-voting application were successfully implemented by looking at the plaintext results before encryption and after encryption which was displayed to the user before

selecting a candidate and with the three pass protocol scheme so that the attacker does not can easily decrypt the results of voice encryption because the ciphertext has 3 different keys using the vigenere cipher algorithm.

Keywords: *E-voting, Vigenere Cipher, Three Pass Protocol*

1. PENDAHULUAN

Perkembangan teknologi informasi saat ini sudah jadi hal penting untuk dimanfaatkan, sehingga diperlukan sarana dan prasarana yang dapat mencukupi kebutuhan akan informasi tersebut. Timbulnya berbagai informasi tersebut mendorong manusia untuk mencapai dan mengembangkan teknik-teknik baru agar pengolahan data dapat dilaksanakan dengan cepat, akurat, dan efisien. Salah satunya adalah melakukan pemilihan kepala desa dengan memanfaatkan teknologi. Pemilihan kepala desa di Kecamatan Barus, Kabupaten Tapanuli Tengah banyak dilakukan dengan cara coblos lembar kertas suara, kemudian memasukkan kertas suara tersebut kedalam kotak suara yang tersedia. Setelah tahapan pemungutan selesai akan dilanjutkan ke perhitungan suara. Proses pemilihan kepala desa tersebut sering terjadi kesalahan yang disebabkan oleh *human error*, yakni pemilih salah dalam pencoblosan lembar kertas suara, sehingga banyak kertas suara yang rusak dan dinyatakan tidak sah. Proses perhitungan suara masih dilakukan dengan cara manual, hal ini menyebabkan perhitungan menjadi lambat karena proses tersebut harus meghitung satu persatu lembar kertas suara. Adanya permasalahan tersebut membuat proses pemilihan kepala desa menjadi tidak efektif. Untuk itu, dibutuhkan sebuah sistem yang dapat mengatasi permasalahan tersebut.

Dengan adanya permasalahan di atas, penulis mencoba membangun sebuah sistem pemilihan kepala desa dengan menggunakan *e-voting* (*electronic voting*). Dimana *e-voting* merupakan penggunaan teknologi komputer dalam melaksanakan pemilihan dan penghitungan suara (Sany, 2021).

Prosedur pemungutan suara yang digunakan dalam istilah *e-voting* memungkinkan pemilih untuk memberikan suara yang aman, rahasia, dan terjamin melalui sistem elektronik (Abba et al., 2017).

Langkah-langkah untuk memastikan keamanan dan kerahasiaan data tersebut dapat dilakukan dengan menggunakan algoritma kriptografi. Algoritma kriptografi melakukan dua fungsi yaitu enkripsi dan dekripsi. Salah satu algoritma enkripsi yang dapat digunakan untuk menjaga keamanan dan kerahasiaan data adalah *vigenere cipher*.

Menurut (Pramudya et al., 2021) *vigenere cipher* merupakan hasil dari penyederhanaan sandi substitusi polialfabetik dan terdiri dari beberapa bagian sandi *caesar* dengan proses pergeseran nilai yang berbeda dengan menambahkan angka kata kunci dan angka pesan lalu dimoduluskan dengan 26 dan hasilnya yang berupa angka tersebut dirubah ke dalam huruf untuk mendapatkan huruf yang tersandi (Lukman Sholeh & Ali Muharom, 2016).

Algoritma *vigenere cipher* menggunakan sebuah kunci pada saat melakukan enkripsi dan dekripsi. Oleh karena itu, untuk menghindari adanya pendistribusian kunci serta sebagai model keamanan data voting dengan keamanan ganda, maka algoritma *vigenere cipher* ini akan dibantu dengan skema *three pass protocol*.

Three pass protocol memungkinkan satu pihak untuk mengirim pesan dengan aman ke pihak lain tanpa bertukar atau mendistribusikan kunci enkripsi. Disebut dengan *three pass protocol* karena terdapat tiga pertukaran untuk mengotentikasi pengirim dan penerima dari protokol pertama (Oktaviana & Utama Siahaan, 2016).

Maka berdasarkan latar belakang masalah yang sudah diuraikan, penulis melakukan penelitian dengan judul "KEAMANAN DATA HASIL *E-VOTING* PEMILIHAN KEPALA DESA DENGAN ALGORITMA *VIGENERE CIPHER* PERTUKARAN

KUNCI *THREE PASS PROTOCOL* PADA KECAMATAN BARUS KABUPATEN TAPANULI TENGAH".

2. METODE PENELITIAN

Tempat dan Waktu Penelitian

Penelitian ini dilaksanakan di Kantor Kepala Desa Kecamatan Barus Kabupaten Tapanuli Tengah. Penelitian ini dilakukan selama 3 bulan mulai dari bulan Maret 2022 sampai bulan Mei 2022.

Instrumen Penelitian

Untuk melakukan perancangan aplikasi *e-voting* pemilihan kepala desa pada Kecamatan Barus Kabupaten Tapanuli Tengah, peneliti membutuhkan kesediaan perangkat keras (*hardware*) dan lunak (*software*). Adapun instrumen penelitian yang digunakan dalam penelitian ini yaitu:

Perangkat Keras

Perangkat keras yang digunakan untuk mengembangkan dan mengumpulkan data pada penelitian ini adalah:

Laptop dengan Intel Celeron N3050
RAM 2 GB
Hardisk 500 GB
Dan Intel HD Graphics.

Perangkat Lunak

Adapun perangkat lunak yang digunakan dalam penelitian ini diantaranya adalah:

Sistem operasi Windows 7
Microsoft Visual Studio Code
XAMPP
Bahasa pemrograman PHP dan Javascript

Teknik Pengumpulan Data

Di dalam penelitian ini peneliti menggunakan beberapa metode dalam pengumpulan data, yaitu menggunakan dokumentasi serta studi literatur.

Dokumentasi

Dokumentasi digunakan untuk mengumpulkan data–data sekunder yang dapat berbentuk tulisan, gambar, atau data–data yang bersangkutan dengan penelitian.

Studi Literatur

Studi literatur dilakukan untuk mendapatkan teori serta konsep yang mendukung penelitian dan berkaitan dengan masalah yang diangkat dalam penelitian.

3.HASIL DAN PEMBAHASAN

Source Code Tahap Enkripsi

```
function encrypt(message, key) {
    let result = ''

    for (let i = 0, j = 0; i < message.length; i++) {
        const c = message.charAt(i)
        if (isLetter(c)) {
            if (isUpperCase(c)) {
                result += String.fromCharCode((c.charCodeAt(0) + key.toUpperCase().charCodeAt(j) - 2 * 65) % 26 + 65)
            } else {
                result += String.fromCharCode((c.charCodeAt(0) + key.toLowerCase().charCodeAt(j) - 2 * 97) % 26 + 97)
            }
        } else {
            result += c
        }
        j = ++j % key.length
    }
    return result
}
```

Gambar 1 Source Code Tahap Enkripsi

Gambar 1 merupakan fungsi untuk melakukan enkripsi algoritma *vigenere cipher* dengan menggunakan bahasa pemrograman Javascript.

Source Code Tahap Dekripsi

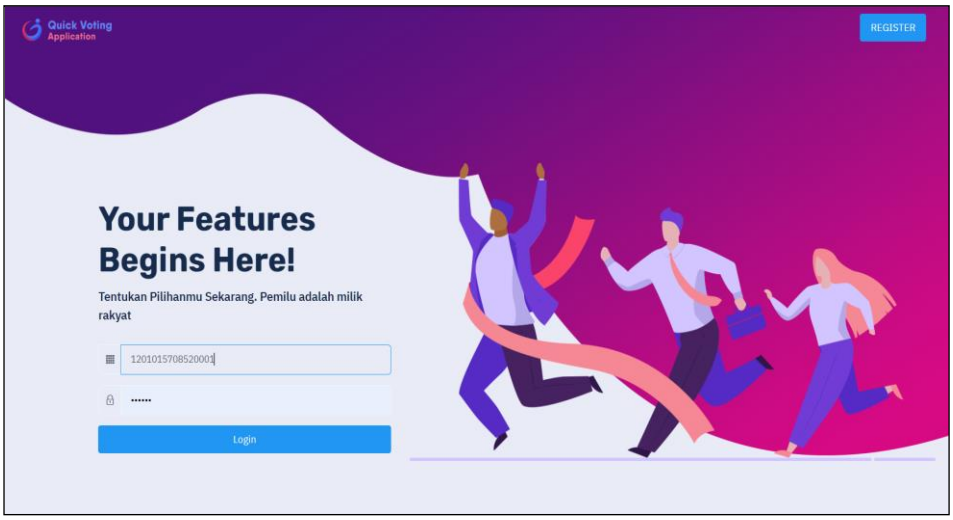
```
function decrypt(message, key) {
    let result = ''

    for (let i = 0, j = 0; i < message.length; i++) {
        const c = message.charAt(i)
        if (isLetter(c)) {
            if (isUpperCase(c)) {
                result += String.fromCharCode(90 - (25 - (c.charCodeAt(0) - key.toUpperCase().charCodeAt(j))) % 26)
            } else {
                result += String.fromCharCode(122 - (25 - (c.charCodeAt(0) - key.toLowerCase().charCodeAt(j))) % 26)
            }
        } else {
            result += c
        }
        j = ++j % key.length
    }
    return result
}
```

Gambar 2 Source Code Tahap Dekripsi

Gambar 2 merupakan fungsi untuk melakukan dekripsi algoritma *vigenere cipher* dengan menggunakan bahasa pemrograman Javascript.

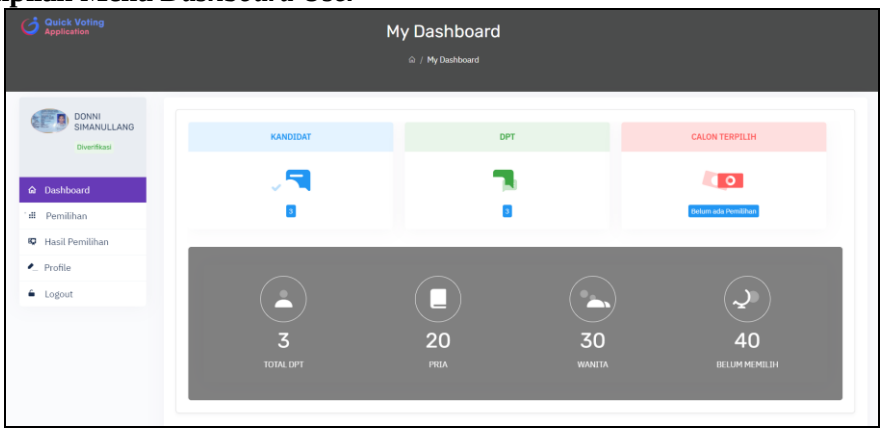
Tampilan Halaman *Login User*



Gambar 3 Tampilan Halaman Login User

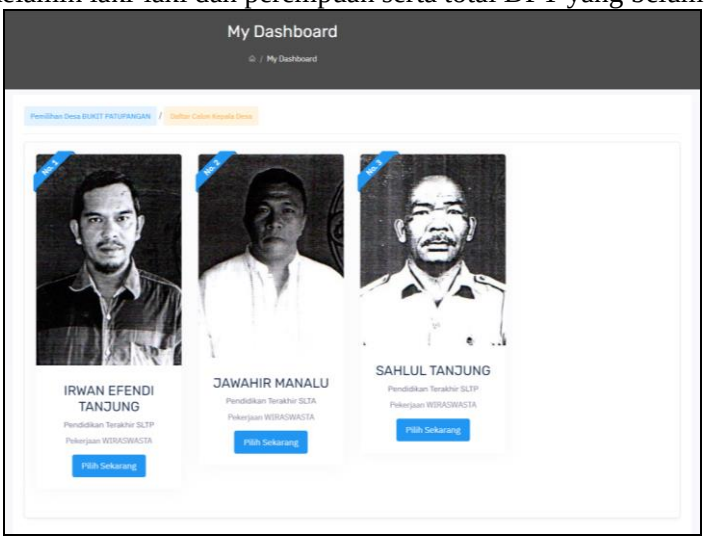
Halaman yang pertama kali tampil saat *user* mengakses aplikasi pemilihan kepala desa adalah halaman *login*.

Tampilan Menu *Dashboard User*



Gambar 4 Tampilan Dashboard User

Gambar di atas merupakan halaman utama dari aplikasi pemilihan kepala desa yang dapat dilihat setelah melakukan *login*. Informasi yang ditampilkan pada halaman ini berupa total kandidat, total DPT, total calon terpilih, dan informasi lainnya seperti total DPT yang berjenis kelamin laki-laki dan perempuan serta total DPT yang belum memilih.



Gambar 5 Tampilan Menu Pemilihan Calon Kepala Desa User

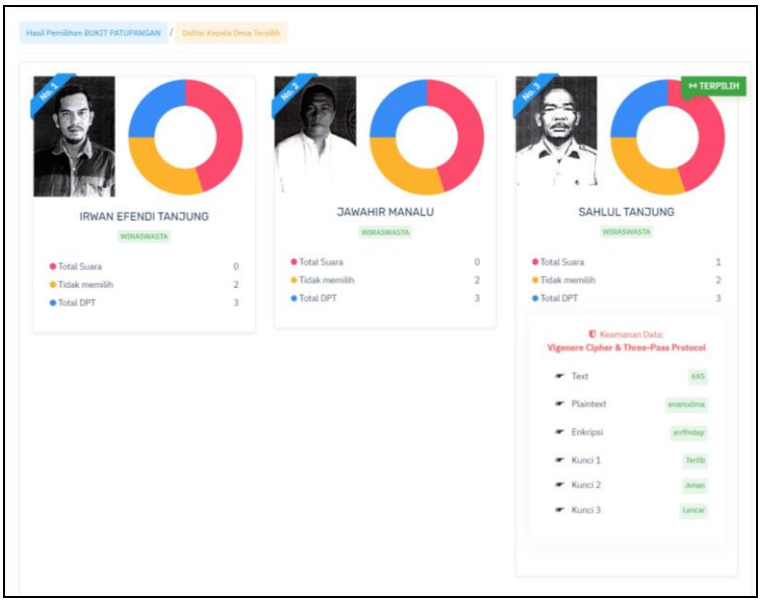
Pada Gambar diatas dapat dilihat bahwa Tindakan yang dapat dilakukan oleh *user* adalah memilih kandidat kepala desa yang diinginkan.

Tampilan Konfirmasi Pemilihan

Gambar 6 Tampilan Konfirmasi Pemilihan

Gambar 6 di atas merupakan tampilan konfirmasi saat *user* ingin memilih seorang kandidat. Pada tampilan konfimasi ini akan ditampilkan data nomor urut calon yang ingin dipilih, token sebelum dilakukan enkripsi, penggunaan kunci enkripsi dan token sesudah dilakukan enkripsi. Selain itu, terdapat pesan peringatan untuk memastikan bahwa *user* yakin untuk memilih seorang kandidat berdasarkan data yang dipilih dan ditampilkan.

Tampilan Menu Hasil Pemilihan



Gambar 7 *Tampilan Menu Hasil Pemilihan*

Gambar di atas merupakan menu untuk melihat hasil pemilihan. Pada halaman ini, akan tampil daftar kandidat kepala desa untuk pemilihan kepala desa pada suatu desa yang ditampilkan dalam bentuk kartu-kartu diikuti dengan informasi detail suara yang didapatkan serta informasi kandidat yang terpilih jika pemungutan suara telah selesai dilakukan. Pada kartu kandidat yang terpilih, akan ditampilkan detail kemanan data menggunakan algoritma *vigenere cipher* dan skema *three pass protocol*.

4. KESIMPULAN

Pembuatan aplikasi pemilihan kepala desa berhasil dilakukan dengan menggunakan bahasa pemrograman Javascript dan PHP, DBMS MySQL serta algoritma *vigenere cipher* dan skema *three pass protocol* untuk pengamanan datanya.

Dalam menerapkan algoritma *vigenere cipher* dan skema *three pass protocol* untuk pengamanan data pemilihan kepala desa, terlebih dahulu menentukan bentuk *plaintext* yang akan dienkripsi. Dalam hal ini plaintext-nya akan berbentuk "IdKandidatxIdDPT". Lalu menentukan kunci yang akan digunakan. Pada penelitian ini, kunci yang digunakan ada 3 yaitu: tertib, aman dan lancar. Dimana, kunci pertama merupakan kunci *default*, kunci kedua merupakan kunci pengirim (*user*) dan kunci ketiga merupakan kunci penerima (admin). Kunci *default* dibutuhkan untuk pengamanan ganda sebelum dilakukan enkripsi dengan skema *three pass protocol*. Setelah menentukan kunci yang akan digunakan pada algoritma *vigenere cipher*, dilanjutkan dengan menerapkan skema *three pass protocol*. Sehingga akan terjadi 3 kali enkripsi dan 3 kali dekripsi.

DAFTAR PUSTAKA

Abba, A. L., Awad, M., Al-Qudah, Z., & Jallad, A. H. (2017). Security Analysis of Current Voting Systems. *2017 International Conference on Electrical and Computing Technologies and Applications, ICECTA 2017*, *2018-Janua*, 1–6. https://doi.org/10.1109/ICECTA.2017.8252006

Fauzi Siregar, H., Handika Siregar, Y., & Melani. (2018). Perancangan Aplikasi Komik Hadist Berbasis Multimedia. *Jurnal Teknologi Informasi*, *2*(2), 113–121.

Ibnu Sa'ad, M. (2020). *Otodidak Web Programming: Membuat Website Edutainment*. PT Elex Media Komputindo.

Khasanah, Nguyen, P. T., Gunawan, G., & Rahim, R. (2020). Three-pass Protocol Scheme on Vigenere Cipher to Avoid Key Distribution. *Journal of Critical Reviews*, *7*(1), 68–71. https://doi.org/10.22159/jcr.07.01.13

Lukman Sholeh, Moh., & Ali Muharom, L. (2016). SMART PRESENSI MENGGUNAKAN QRCode DENGAN ENKRIPSI VIGENERE CIPHER. *J. Math. and Its Appl.*, *13*(2), 31–44.

Maimunah, M., Supriyanti, D., & Hendrian, H. (2017). Aplikasi Sistem Order Online Berbasis Mobile Android Pada Outlet Pizza Hut Delivery. *Semnasteknomedia Online*, *5*(1), 4-5–1. http://ojs.amikom.ac.id/index.php/semnasteknomedia/article/view/1737/1465

Mulyani, S. (2016). *Metode Analisis dan Perancangan Sistem* (2nd ed.). Abdi Sistematika.

Musla, A., Tommy, & Elhanafi, A. M. (2021). Kombinasi Kriptografi Algoritma Polyalphabetic Dan Kompresi Huffman Untuk Pengamanan Data. *SNASTIKOM: Seminar Nasional Teknologi Informasi & Komunikasi*, 303–310.

Oktaviana, B., & Utama Siahaan, A. P. (2016). Three-Pass Protocol Implementation in Caesar Cipher Classic Cryptography. *IOSR Journal of Computer Engineering*, *18*(04), 26–29.

Pramudya, E. R., Handoko, L. B., & Muslih. (2021). KRIPTOGRAFI VIGENERE UNTUK MENGAMANKAN PESAN TEKS BERBASIS OCR (OPTICAL

CHARACTER RECOGNITION). *Proceeding SENDI_U*, 460–467.

Prananda, R., Anra, H., & Pratiwi, H. S. (2017). Rancang Bangun Aplikasi E-Voting Berbasis Android (Studi Kasus: Pemilihan Ketua Organisasi di Lingkungan Fakultas Teknik Universitas Tanjungpura). *Jurnal Sistem Dan Teknologi Informasi (JUSTIN)*, *5*(1), 17–21.

Sany, E. (2021). Seminar Nasional Informatika (SENATIKA) Prosiding SENATIKA 2021 Aplikasi eVoting Pada Pemilihan Presiden Badan Eksekutif Mahasiswa (BEM) Universitas Nurdin Hamzah. *Seminar Nasional Informatika (SENATIKA)*, 398–408.

Sulaiman, O. K., Nasution, K., & Siambaton, M. Z. (2020). Three Pass Protocol untuk Keamanan Kunci Berbasis Base64 pada XOR Cipher. *Jurnal Sains Komputer & Informatika (J-SAKTI)*, *4*(September), 721–727.

Sumiati, M., Abdillah, R., & Cahyo, A. (2021). Pemodelan UML untuk Sistem Informasi Persewaan Alat Pesta. *FASILKOM*, *11*(2), 79–86.