JITET (Jurnal Informatika dan Teknik Elektro Terapan)
Vol. 13 No. 3, pISSN: 2303-0577 eISSN: 2830-7062 http://dx.doi.org/10.23960/jitet.v13i3.6550

OPTIMASI ALGORITMA VIGENERE CIPHER DAN SHA-256 UNTUK KEAMANAN DATA KELURAHAN LASIANA

Yuni Ernawati Lutgardis Bifel[1], Menhya Snae[2]
Teknik Informatika, STIKOM Uyelindo Kupang

Keywords:
Data Security, SHA-256, Vigenere Cipher

Corespondent Email:
yunibifel4@gmail.com , menhyasnae@gmail.com

Abstrak. *Keamanan data merupakan aspek penting dalam sistem informasi, terutama dalam melindungi data sensitif seperti data penduduk. Di Kelurahan Lasiana, sistem keamanan data masih belum optimal, sehingga berpotensi meningkatkan risiko pencurian data, peretasan, dan kejahatan siber lainnya. Tantangan ini membutuhkan solusi yang efektif untuk melindungi informasi sensitif dari pihak yang tidak berwenang. Penelitian ini bertujuan untuk merancang sistem keamanan data yang menggabungkan Algoritma Vigenere Cipher dan SHA-256. Algoritma Vigenere Cipher digunakan untuk mengenkripsi data agar sulit dipahami oleh pihak tidak berwenang, sedangkan SHA-256 menghasilkan nilai hash yang unik untuk memastikan integritas data. Tujuan penelitian ini adalah menciptakan sistem keamanan data yang mampu meminimalkan risiko kejahatan siber dan meningkatkan kepercayaan dalam pengelolaan data penduduk. Solusi yang ditawarkan berupa perancangan dan implementasi sistem keamanan berbasis kedua algoritma tersebut. Sistem diuji untuk memastikan keandalannya dalam mengenkripsi data dan melindungi informasi sensitif. Penelitian ini diharapkan memberikan kontribusi signifikan dalam pengembangan teknologi keamanan data di lingkungan pemerintahan, khususnya untuk melindungi data penduduk secara lebih aman, efisien, dan transparan.*

Abstract. *Data security is an important aspect in information systems, especially in protecting sensitive data such as population data. In Lasiana Village, the data security system is still not optimal, thus potentially increasing the risk of data theft, hacking and other cyber crimes. This challenge requires effective solutions to protect sensitive information from unauthorized parties. This research aims to design a data security system that combines the Vigenere Cipher Algorithm and SHA-256. The Vigenere Cipher Algorithm is used to encrypt data to make it difficult for unauthorized parties to understand, while SHA-256 produces a unique hash value to ensure data integrity. The aim of this research is to create a data security system that is able to minimize the risk of cyber crime and increase trust in managing population data. The solution offered is in the form of designing and implementing a security system based on these two algorithms. The system is tested to ensure its reliability in encrypting data and protecting sensitive information. This research is expected to make a significant contribution to the development of data security technology in the government environment, especially to protect citizen data more safely, efficiently and transparently.*

1. PENDAHULUAN

Keamanan data adalah upaya untuk melindungi data dari berbagai ancaman, seperti akses tidak sah, pencurian, perubahan, atau kerusakan. Keamanan suatu data menjadi sangat penting saat sudah berkaitan dengan data

yang sangat rahasia. Karena jika sampai dapat diretas atau diketahui oleh orang lain, data yang ada dapat disalahgunakan [1]. Tujuan utama dari keamanan data adalah untuk memastikan bahwa informasi tetap rahasia, utuh, dan tersedia hanya bagi pihak yang berwenang. Keamanan data melibatkan penggunaan berbagai teknik, seperti enkripsi, autentikasi, kontrol akses, dan backup, untuk menjaga data dari risiko keamanan. Oleh karena itu pentingnya keamanan data dalam sistem informasi, terutama di instansi pemerintahan yang menyimpan data sensitif seperti data penduduk. Dalam menjaga kerahasiaan informasi saat melakukan pertukaran data, kerahasiaan dan keamanann adalah sesuatu hal yang sangat penting dalam komunikasi data, baik untuk tujuan privasi ataupun individu, maupun untuk keamanan bersama. Salah satu cara agar keamanan dan kerahasiaan pesan atau informasi dapat terjaga yaitu dengan menggunakan teknik kriptografi [2]. Hampir semua kehidupan saat ini dilingkupi oleh kriptografi sebagai alat untuk menjamin keamanan, kerahasiaan informasi yang menggunakan persamaan matematis untuk melakukan proses enkripsi dan dekripsi. Teknik ini untuk mengkonversi data ke bentuk kode-kode tertentu agar informasi tidak dapat terbaca oleh siapapun kecuali pihak yang berhak [3]. Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah [4]. Saat ini Kriptografi bukan hanya dipakai untuk menulis atau pun menyelesaikan kode, tetapi kriptografi sudah berkembang ke berbagai macam fungsi seperti enkripsi/dekripsi untuk pengamanan data, otentikasi identitas dan pesan, tanda tangan dan sertifikat digital, protokol pertukaran kunci, uang digital, dan lain sebagainya [5].

2. TINJAUAN PUSTAKA

2.1. Keamanan Data

Keamanan biasanya digambarkan sebagai kebebasan dari bahaya atau sebagai kondisi keselamatan. Keamanan komputer, secara rinci adalah perlindungan data di dalam suatu sistem melawan terhadap otorisasi tidak sah, modifikasi, atau perusakan dan perlindungan sistem komputer terhadap penggunaan tidak sah atau modifikasi [6]. Dalam rangka menghindari pencurian data yang disebabkan oleh pihak yang tidak memiliki hak maka penerapan keamanan data adalah hal yang sangat penting untuk melindungi informasi pribadi dari serangan siber dan kejahatan yang di salah gunakan oleh pihak yang tidak berwenang.

Oleh karena itu untuk mengatasi masalah tersebut dan mengurangi risiko kejahatan siber seperti hacking, cracking, dan pencurian data yaitu dengan menggunakan Metode Kriptografi Vigenere Cipher yang melibatkan penggunaan kunci enkripsi untuk mengubah data menjadi format yang tidak dapat dibaca oleh pihak yang tidak berwenang sedangkan SHA-256 digunakan untuk menghasilkan nilai hash yang membuat data semakin sulit dipecahkan.

2.2. Vigenere Cipher

Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi Caesar berdasarkan huruf-huruf pada kata kunci [7]. Penyandian pesan dalam plaintext untuk menghasilkan ciphertext disebut enkripsi, sedangkan untuk mengembalikan pesan yang dihasilkan dari ciphertext ke kata atau kalimat asli disebut deskripsi.

2.3. Enkripsi Dan Deskripsi

Enkripsi bertujuan untuk menyembunyikan pesan dan informasi dari orang yang tidak berwenang. Deskripsi ini untuk tujuan memulihkan kata sandi terenkripsi atau informasi dalam bentuk aslinya menggunakan kunci yang sama dalam proses enkripsi [8].

2.4. SHA-256 (*Secure Has Algoritma*)

SHA-256 adalah salah satu algoritma hash yang relatif masih baru. Algoritma ini dirancang oleh *The National Institute of Standards and Tecnology* (NIST) pada tahun 2002. SHA-256 menghasilkan message digest dengan panjang 256 bit. SHA-256 aman karena

didesain sedemikian rupa sehingga tidak memungkinkan mendapat pesan yang berhubungan dengan *message digest*, atau untuk menemukan dua pesan yang berbeda yang menghasilkan message digest yang sama [9]. Fungsi hash SHA-256 merupakan versi SHA dengan ukuran digest 256 pada versi SHA-2. SHA didasarkan pada MD4 yang dibuat oleh Ronald L, Rivest dari MIT. SHA-256 menggunakan enam logika yang merupakan kombinasi dasar seperti AND, OR, XOR, pergeseran bit kekanan (shift right), dan rotasi bit kekanan (rotate right). Algoritma ini mengubah sebuah message schedule yang terdiri dari 64 element 32-bit word, delapan buah variabel 32-bit, dan variabel penyimpan nilai hash 8 buah word 32-bit [10].

2.5. Website

Website merupakan suatu kumpulan dari halaman-halaman situs yang terangkum dalam sebuah domain atau subdomain, yang tempatnya berada di dalam *World Wide Web* (WWW) di dalam internet. Sebuah halaman pada web biasanya berupa suatu dokumen yang ditulis dalam format HTML(*Hyper Text Markup Language*), yang selalu bisa diakses melalui HTTP, yang merupakan sebuah protokol yang menyampaikan suatu informasi dari server website untuk ditampilkan kepada para pengguna melaui web browser dan website dapat diartikan sebagai kumpulan halaman yang dapat menampilkan informasi data teks, data gambar diam atau gerak, data animasi, suara, video dan atau gabungan dari semuanya, baik itu bersifat dinamis yang dapat membentuk satu rangkaian bangunan yang saling terkait dimana pada masing-masing dihubungkan dengan jaringan-jaringan halaman (*hyperlink*) [11].

2.6. PHP (*Hypertext Preprocessor*)

PHP adalah singkatan dari *Hypertext Prepocessor*, yaitu bahasa pemrograman yang digunakan secara luas untuk penanganan, pembuatan, dan pengembangan sebuah situs web dan biasanya digunakan bersama dengan HTML. Sampai saat ini PHP merupakan bahasa wajib programmer web dan masih menjadi standar bahasa pemrograman server side untuk pembuatan website. PHP disebut bahasa pemrograman server side karena PHP diproses pada komputer server[12].

2.7. MySQL

MySQL adalah perangkat lunak RDMS (*Relational Database Management System*) yang dirancang untuk mengelola database dengan kecepatan tinggi, mampu menangani data dalam jumlah besar, dan mendukung akses oleh banyak pengguna secara bersamaan. MySQL, salah satu database server yang paling terkenal, menggunakan bahasa SQL untuk mengelola database-nya. Lisensinya mencakup FOSS License Exception serta opsi versi komersial. Dikenal dengan julukan "*The World's most popular open source database*", MySQL tersedia untuk berbagai platform, termasuk Windows dan Linux. Untuk mempermudah administrasi MySQL, penggunaan perangkat lunak seperti phpMyAdmin sangat disarankan[13].

2.8. Visual Studio Code

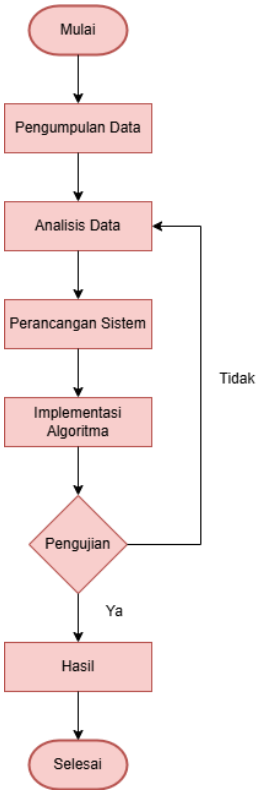
Visual studio code aplikasi berbasis *open source* yang mendukung banyak bahasa dan ekstensi. Kelebihan Visual Studio Code adalah memiliki banyak fitur seperti dapat melacak kesalahan pengkodean dengan cepat, dan memiliki antarmuka yang *user-friendly*[14].

2.9. CryTool

Crytool adalah perangkat lunak yang dirancang untuk implementasi enkripsi dan keamanan kriptografi. Perangkat lunak ini menyediakan antarmuka yang mempermudah penggunaan metode enkripsi seperti *Caesar Cipher*, serta memungkinkan manajemen key dan operasi enkripsi yang aman[15].

3. METODE PENELITIAN

Metode penelitian menjelaskan mengenai prosedur penelitian yang akan dilakukan.



Gambar 3.1 Prosedur penelitian

Berikut adalah penjelasan dari tahan-tahap yang dilakukan :

1. Pengumpulan Data : melalui Studi Literatur dan melakukan Observasi
   Mengumpulkan informasi terkait algoritma vigenere cipher dan SHA-256 dari jurnal-jurnal dan artikel penelitian terdahulu. Studi literatur ini bertujuan untuk memahami dasar-dasar teori yang digunakan dalam penelitian.
2. Analisis Data : Tahap ini melibatkan analisis data yang telah dikumpulkan untuk mengidentifikasi pola, kebutuhan sistem, dan solusi yang diperlukan. Analisis data juga mencakup evaluasi dan pemetaan proses yang ada serta penentuan kebutuhan sistem yang harus dipenuhi.
3. Perancangan Sistem : Berdasarkan analisis data, penulis merancang sistem yang akan dibangun. Tahap perancangan mencakup pembuatan diagram *use case*, diagram alur atau *Sequence diagram*, dan rancangan antarmuka (*interface design*) yang menggambarkan bagaimana sistem akan berfungsi dan berinteraksi dengan pengguna.
4. Implementasi : Pada tahap ini perancangan yang telah dibuat di implementasikan ke dalam program sehingga sesuai dengan perancangan dengan menambahkan Algoritma *Vigenere Chiper* yang berfungsi untuk mengenkripsi data menggunakan kunci yang bersifat dinamis serta Algoritma SHA-256 digunakan untuk menghasilkan hash data yang unik dan sulit untuk direkayasa ulang.
5. Pengujian : Pengujian dilakukan untuk mengevaluasi performa dan keamanan sistem. Proses ini mencakup pengujian fungsionalitas, kecepatan proses, serta keamanan data yang telah dienkripsi dan di-hash.
6. Hasil : Hasil pengujian digunakan untuk menilai sejauh mana sistem memenuhi tujuan penelitian dan memberikan data yang akurat dan aman.

4. HASIL DAN PEMBAHASAN

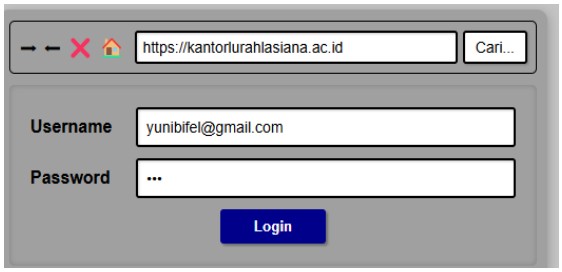
Pada penelitian ini menghasilkan sebuah sistem informasi pengelolaan data penduduk berbasis *website* yang melibatkan kedua algoritma kriptografi, yaitu algoritma *Vigenere Cipher* dan SHA-256, yang diimplementasikan di dalam program. Sistem ini dibangun menggunakan PHP, MySQL, dan *Visual Studio Code* sebagai lingkungan pengembangan. Sistem ini dirancang untuk menyimpan data penduduk dalam bentuk terenkripsi didalam database, sehingga informasi sensitif seperti Nama, NIK, dan Jenis Kelamin tidak dapat dibaca langsung oleh pihak yang tidak berwenang. Algoritma *Vigenere Cipher* digunakan untuk mengenkripsi data sebelum disimpan di database, sementara SHA-256 digunakan untuk menghasilkan nilai hash guna menjaga integritas data sehingga lebih sulit lagi untuk dipecahkan.

```php
<?php
// Fungsi Enkripsi Vigenere Cipher
function vigenere_encrypt($plaintext, $key) {
    $ciphertext = "";
    $key = strtoupper($key);
    $plaintext = strtoupper($plaintext);
    $key_length = strlen($key);

    for ($i = 0, $j = 0; $i < strlen($plaintext); $i++) {
        if (ctype_alpha($plaintext[$i])) { // Hanya mengenkripsi huruf
            $p = ord($plaintext[$i]) - ord('A');
            $k = ord($key[$j % $key_length]) - ord('A');
            $c = ($p + $k) % 26;
            $ciphertext .= chr($c + ord('A'));
            $j++;
        } else {
            $ciphertext .= $plaintext[$i]; // Biarkan karakter selain huruf tetap
        }
    }
    return $ciphertext;
}

// Fungsi Dekripsi Vigenere Cipher
function vigenere_decrypt($ciphertext, $key) {
    $plaintext = "";
    $key = strtoupper($key);
    $ciphertext = strtoupper($ciphertext);
    $key_length = strlen($key);

    for ($i = 0, $j = 0; $i < strlen($ciphertext); $i++) {
        if (ctype_alpha($ciphertext[$i])) { // Hanya mendekripsi huruf
            $c = ord($ciphertext[$i]) - ord('A');
            $k = ord($key[$j % $key_length]) - ord('A');
            $p = ($c - $k + 26) % 26;
            $plaintext .= chr($p + ord('A'));
            $j++;
        } else {
            $plaintext .= $ciphertext[$i]; // Biarkan karakter selain huruf tetap
        }
    }
    return $plaintext;
}

// Fungsi Hashing SHA-256
function sha256_hash($text) {
    return hash('sha256', $text);
}
```

Gambar 4.1 Code program PHP

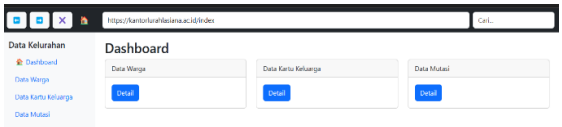
4.1. Pengujian Sistem

Pada halaman login ini, admin dapat mengakses sistem dengan memasukkan username dan password yang valid lalu menekan tombol "Login". Setelah berhasil login, admin akan diarahkan ke menu utama atau dashboard untuk mengelola sistem. Halaman ini dirancang dengan tampilan sederhana dan mudah digunakan, memastikan proses autentikasi berjalan dengan aman dan efisien.



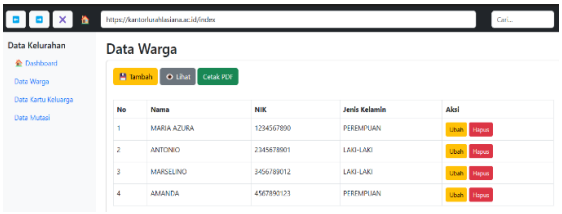
Gambar 4.2 Halaman login

Pada Saat tombol "Detail" pada data warga diklik, sistem akan mengarahkan admin ke halaman data warga, yang menampilkan daftar warga yang terdaftar dalam sistem, termasuk informasi di dalamnya. Hal ini berlaku juga untuk data kartu keluarga dan data mutasi.



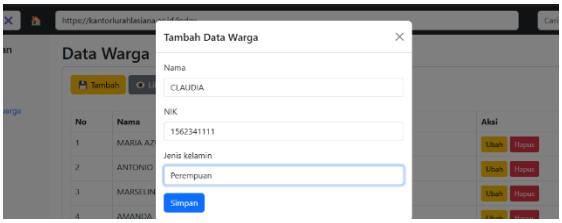
Gambar 4.3 Halaman *dashboard*

Halaman data warga ini menampilkan daftar warga yang terdaftar dalam sistem data kelurahan, lengkap dengan informasi seperti Nama, NIK, dan Jenis Kelamin. Admin dapat mengelola data dengan beberapa tombol aksi, seperti Tambah untuk menambahkan warga baru, Ubah untuk mengedit data, dan Hapus untuk menghapus data yang tidak diperlukan. Selain itu, terdapat fitur Lihat untuk menampilkan detail lebih lanjut serta Cetak PDF untuk mencetak data dalam format dokumen. Halaman ini mempermudah pengelolaan data warga secara efektif dan terorganisir.



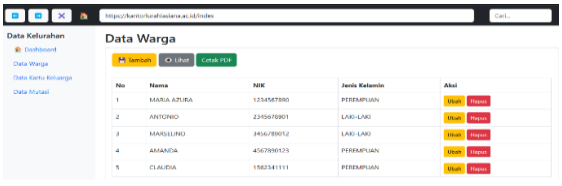
Gambar 4.4 Halaman data warga

Saat kita mengklik tombol "Tambah", sistem akan menampilkan forum tambah data. Di dalam forum ini, kita bisa memasukkan informasi berupa data warga, seperti Nama, NIK, dan Jenis Kelamin. Setelah semua data diisi dengan benar, kita dapat menekan tombol "Simpan".



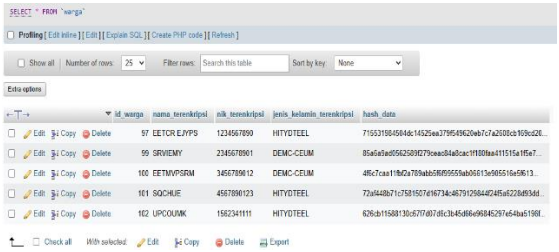
Gambar 4.5 *Forum* tambah data

Jika proses berhasil, data yang dimasukkan akan tersimpan dengan baik di dalam sistem dan muncul dalam daftar warga.



Gambar 4.6 Hasil tambah data

Saat pengguna memasukkan data ke dalam sistem, informasi seperti nama, NIK, dan jenis kelamin terlihat dalam bentuk yang dapat dibaca. Namun, setelah data disimpan ke dalam database, sistem secara otomatis mengenkripsinya sehingga tidak dapat dibaca secara langsung. Enkripsi ini bertujuan untuk melindungi data agar tidak mudah diakses oleh pihak yang tidak berwenang. Misalnya, nama yang awalnya jelas terbaca akan berubah menjadi teks terenkripsi, begitu juga dengan jenis kelamin sedangkan untuk NIK karena dia merupakan inputan angka maka output yang dihasilkan tetap tidak berubah, karena dalam kode PHP yang digunakan proses enkripsi hanya diterapkan pada karakter huruf dengan menggunakan fungsi `ctype_alpha()`. Selain itu, terdapat kolom hash_data yang kemungkinan digunakan untuk keamanan tambahan, seperti memastikan integritas data.

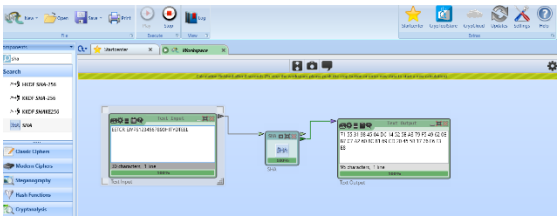


Gambar 4.7 Hasil data terenkripsi

Nilai hash yang dihasilkan dalam database merupakan representasi unik dari data terenkripsi yang bertujuan untuk menjaga integritas serta keamanan informasi. Dalam proses ini, data awal terlebih dahulu dienkripsi menggunakan algoritma *Vigenere Cipher* yang merupakan metode enkripsi. Setelah data terenkripsi, hasil enkripsi tersebut kemudian diproses lebih lanjut menggunakan algoritma SHA-256 yang mengubahnya menjadi nilai hash dalam format heksadesimal. Hash yang dihasilkan ini bersifat unik dan tidak dapat dikembalikan ke bentuk semula, sehingga sangat efektif untuk mendeteksi perubahan atau manipulasi data. Untuk menguji apakah data tetap utuh dan tidak dapat dimanipulasi maka nilai hash ini akan diuji menggunakan aplikasi *CryTool 2.1.*

4.2 Pengujian Menggunakan Aplikasi CryTool

Dalam uji coba ini, sistem akan menghasilkan kembali hash dari data asli yang telah dienkripsi dan dibandingkan dengan hash yang tersimpan di database. Jika hasilnya identik atau sama, maka ini membuktikan bahwa data tetap aman dan tidak mengalami perubahan. Sebaliknya, jika terdapat perbedaan, maka ada kemungkinan data telah dimanipulasi atau diubah, yang menunjukkan bahwa integritas data telah terganggu atau program eror.



Gambar 4.8 Hasil ujicoba

Uji coba yang dilakukan menggunakan aplikasi *Crytool* menunjukan proses hashing teks menggunakan algoritma SHA-256. Teks input yang dimasukkan berasal dari database yaitu **"ETCTREJYPS12345678 90HITY DTEEL"** yang merupakan gabungan dari Nama, NIK, dan Jenis kelamin, yang kemudian diproses melalui fungsi hash SHA-256. Proses ini menghasilkan output dalam bentuk nilai heksadesimal, yaitu **"71 55 31 98 45 04 DC 14 52 5E A3 79 F5 49 62 0E B7 C7 A2 60 BC B1 69 CD 20 45 5B 17 76 E6 F3 E8"**. Hasil ini menunjukkan bahwa data berupa teks enkripsi tersebut merupakan data asli yang telah melalui proses hashing menggunakan algoritma SHA-256. Dengan demikian, penggunaan algoritma ini terbukti berhasil diterapkan untuk menjaga kerahasiaan dan keamanan data penduduk di Kelurahan Lasiana, memastikan bahwa informasi sensitif tetap terlindungi dari akses yang tidak sah.

5. KESIMPULAN

Berdasarkan hasil penelitian dan implementasi yang telah dilakukan, dapat disimpulkan bahwa sistem informasi

pengelolaan data penduduk Kelurahan Lasiana berbasis website berhasil menerapkan algoritma *Vigenere Cipher* untuk enkripsi data serta SHA-256 untuk menjaga integritasnya. Sistem ini mampu mengamankan informasi sensitif seperti nama, NIK, dan jenis kelamin sebelum disimpan ke dalam database, sehingga data tidak dapat diakses secara langsung oleh pihak yang tidak berwenang. Pengujian nilai hash menggunakan aplikasi *CrypTool* menunjukkan bahwa integritas data tetap terjaga dengan baik. Namun, karena algoritma *Vigenere Cipher* klasik hanya mengenkripsi huruf (A–Z) dan tidak mencakup angka, maka data numerik seperti NIK tidak mengalami perubahan selama proses enkripsi.

Oleh karena itu, perlu dilakukan modifikasi algoritma agar dapat mengenkripsi angka dengan baik atau mempertimbangkan penggunaan algoritma kriptografi modern. Secara keseluruhan, sistem ini efektif dalam meningkatkan keamanan informasi penduduk dan membantu pengelolaan data secara efisien, meskipun masih terdapat beberapa keterbatasan seperti belum tersedianya fitur pemulihan data otomatis dan belum didukungnya sistem multi-user dengan hak akses berbeda.

DAFTAR PUSTAKA

[1] Rahim, I., Anwar, N., Widodo, A. M., Juman, K. K., & Setiawan, I. (2023). Komparasi fungsi hash MD5 dan SHA256 dalam keamanan gambar dan teks. *Ikra-Ith Informatika: Jurnal Komputer dan Informatika, 7*(2).

[2] Azura, S., Tahir, M., Lestari, A. D., Mardiana, A. S., Turrofifah, A., Susanti, K. N., & Rohman, M. S. (2023). Penerapan Kemanan Data Text menggunakan Metode Kriptografi Vigener Chiper Berbasis Web. *Digital Transformation Technology, 3*(1), 20-28.

[3] Silalahi, L., Sindar, A., & Nusantara, S. P. (2020). Penerapan Kriptografi Keamanan Data Administrasi Kependudukan Desa Pagar Jati Menggunakan SHA-1. *Jurnal Nasional Komputasi dan Teknologi Informasi, 3*(2), 182-186.

[4] Putra, N. B., Andika, B. C., Purba, A. D., & Ridwan, M. (2023). Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan. *JOCITIS-Journal Science Infomatica and Robotics, 1*(1), 42-50

[5] Nanda, N. A., Sari, M., & Gunawan, I. (2023). Kriptografi dan Penerapannya Dalam Sistem Keamanan Data. *Jurnal Media Informatika, 4*(2), 90-93.

[6] Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar cipher atau Vigenere cipher pada pengenkripsian pesan teks. *Journal on Education, 5*(3), 8563-8573.

[7] Alam, H., Habibi, A. K., & Widya, H. (2022). Penggunaan Algoritma Vigenere Cipher Dan One Time Pad Untuk Keamanan Pesan Teks. *In Prosiding Seminar Nasional Teknik UISU (SEMNASTEK)* (Vol. 5, No. 1, pp. 160-166).

[8] Murni, I., Lubis, B. R., & Ikhwan, A. (2023). Pengamanan Pesan Rahasia dengan Algoritma Vigenere Cipher Menggunakan PHP. *Journal on Education, 5*(2), 3466-3476.

[9] Endelina, E. (2021). Implementasi Digital Signature Pada File Audio Menerapkan Metode SHA-256. *Journal of Informatics Management and Information Technology, 1*(2), 60-67.

[10] Sulastri, S., & Putri, R. D. M. (2018). Implementasi enkripsi data Secure Hash Algorithm (SHA-256) dan Message Digest Algorithm (MD5) pada proses pengamanan kata sandi sistem penjadwalan karyawan. *Jurnal Teknik Elektro, 10*(2), 70-74.

[11] Aditya, M., & Putra, S. H. (2022). Perancangan Aplikasi Repository Skripsi Universitas Amir Hamzah Berbasis Web. *Remik: Riset dan E-Jurnal Manajemen Informatika Komputer, 6*(3), 589-598.

[12] Oetomo, I. H. W., & Ir Pontjo Bambang Mahargiono, M. M. (2020). *E-Commerce Aplikasi PHP dan MySQL pada Bidang Manajemen: Program Studi S-1*

Manajemen Tahun Ajaran 2019/2020. Penerbit Andi.

[13] Bazaz, T. M. (2024). SISTEM PENUNJANG KEPUTUSAN PENENTUAN SISWA BERPRESTASI PADA SEKOLAH MENENGAH PERTAMA SATU ATAP TAMBELANG MENGGUNAKAN METODE SIMPLE ADDITIVE WEIGHTING. *Jurnal Informatika SIMANTIK, 9*(2), 29-36.

[14] Darmawan, D., Al Azhima, S. A. T., & Hakim, N. F. A. (2022). Sistem Informasi Rekam Medis Berbasis Aplikasi Desktop Untuk Daerah Pedesaan. *Epsilon: Journal Of Electrical Engineering And Information Technology, 20*(2), 89-99.

[15] Ramadhan, S. S., & Rahman, R. (2024). IMPLEMENTASI ENKRIPSI DAN KEAMANAN KRIPTOGRAPI. *Digital Business and Entrepreneurship Journal, 2*(2), 110-117.