Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

Kombinasi Algoritma Kriptografi Vigenere Cipher dan SHA256 untuk Keamanan Basis Data

Rian Oktafiani*, Erik Iman Heri Ujianto, Rianto

Pascasarjana, Magister Teknologi Informasi, Universitas Teknologi Yogyakarta, Sleman, Indonesia
Email: 1*rian.oktafiani@student.uty.ac.id, 2erik.iman@uty.ac.id, 3rianto@staff.uty.ac.id
Email Penulis Korespondensi: rian.oktafiani@student.uty.ac.id
Submitted: **25/01/2023**; Accepted: **07/03/2023**; Published: **31/03/2023**

Abstrak–Suatu organisasi harus memperhitungkan dan mengelola keamanan penyimpanan data dalam basis data atau database, dan prosedur khusus diperlukan untuk melindungi data dari berbagai risiko keamanan. Permasalahan dalam penelitian ini yaitu, data penduduk yang terdapat pada sistem informasi pelayanan administrasi desa Girisuko belum dienkripsi atau diamankan. Hal ini dapat menimbulkan risiko data yang disimpan di dalam database dapat disadap dan disalahgunakan. Pada penelitian ini, teknik kriptografi yang digunakan yaitu kombinasi algoritma Vigenere Cipher dan SHA 256 untuk mengamankan atau mengenkripsi database, khususnya data penduduk pada sistem informasi pelayanan administrasi desa Girisuko. Teks dalam database dienkripsi menggunakan Vigenere Cipher, dan SHA-256 digunakan untuk menghasilkan hash value atau nilai acak yang berbeda dari teks di dalam database. Pesan akan terenkripsi menggunakan Vigenere Cipher dan kemudian di-hash dengan SHA-256 secara bersamaan. Akibatnya, akan sulit bagi penyerang untuk mendekripsi teks yang disimpan dalam database karena harus memecahkan enkripsi Vigenere Cipher, dan juga harus memecahkan hash value yang dihasilkan menggunakan SHA-256. Kombinasi ini bertujuan untuk meningkatkan keamanan dan menjaga kerahasiaan pesan dari penyerang. Penerapan Vigenere Cipher dan SHA pada aplikasi sistem informasi pelayanan administrasi desa dengan realtime database bekerja dengan baik, dibuktikan dengan dengan running-time yang cepat yaitu 0.39 detik proses enkripsi data menggunakan Vigenere Cipher dengan sebesar 894.968 keys/second dan analyzed keylenght 7 karakter kemudian teks pada database penduduk berhasil diamankan. Dengan melakukan penelitian ini, diharapkan dapat memberikan kontribusi untuk meningkatkan keamanan sistem basis data.

Kata Kunci: Keamanan; Basis Data; Kriptografi; Vigenere Cipher; Fungsi Hash

Abstract–An organization must consider and manage the security of data storage in databases or databases, and special procedures are needed to protect data from various security risks. The problem in this study is that the population data contained in the Girisuko village administrative service information system has not been encrypted or secured. This can pose a risk that the data stored in the database can be intercepted and misused. In this study, the cryptographic technique used was a combination of the Vigenere Cipher and SHA 256 algorithms to secure or encrypt databases, especially population data in the Girisuko village administrative service information system. The text in the database is encrypted using the Vigenere Cipher, and SHA-256 is used to generate a hash value or a random value that is different from the text in the database. Messages will be encrypted using the Vigenere Cipher and then hashed with SHA-256 simultaneously. As a result, it will be difficult for an attacker to decrypt the text stored in the database because they have to break the Vigenere Cipher encryption, and also have to solve the hash value generated using SHA-256. This combination aims to increase security and maintain the confidentiality of messages from attackers. The application of the Vigenere Cipher and SHA to the village administration service information system application with a real-time database works well, as evidenced by the fast running-time of 0.39 seconds the data encryption process uses the Vigenere Cipher with 894,968 keys/second and an analyzed key length of 7 characters then text on population database successfully secured. By conducting this research, it is hoped that it can contribute to improving database system security.

Keywords: Security; Database; Cryptography; Vigenere Cipher; Hash Function

1. PENDAHULUAN

Teknologi informasi telah menjadi bagian penting dari berbagai aspek kehidupan, baik secara langsung maupun tidak langsung. Karena banyaknya manfaat yang ditawarkannya, teknologi informasi sangat erat kaitannya dengan berbagai aspek kehidupan manusia [1]. Perkembangan teknologi yang signifikan dan bebas pada saat ini sangat berkaitan dengan privasi dan keamanan data. Data-data yang tersimpan juga semakin besar, dan data tersebut disimpan dalam database. Namun, tanpa keamanan data yang memadai, jika data hanya disimpan dalam basis data, sangat rentan untuk dicuri atau diubah oleh orang yang tidak berhak atau berwenang.

Perusahaan atau organisasi didirikan untuk mendapatkan suatu keuntungan. Namun, beberapa organisasi tidak memperhatikan keamanan data yang mereka miliki. Instansi pemerintahan menyimpan banyak data penting, salah satunya yaitu data penduduk. Kelurahan Girisuko yang terletak di Kecamatan Panggang, Kabupaten Gunungkidul, Daerah Istimewa Yogyakarta memiliki Sistem Informasi Pelayanan Administrasi Desa. Sistem ini digunakan untuk memberikan pelayanan administrasi berupa surat menyurat dan pelayanan pengaduan masyarakat. Sistem ini menyimpan banyak data penting dan bersifat rahasia.

Dalam menjaga kerahasiaan informasi, terutama informasi sensitif yang isinya hanya dapat diketahui oleh individu yang berwenang, maka keamanan data sangat penting. Apalagi jika pengiriman data tersebut dilakukan melalui jaringan publik yang dapat diakses oleh banyak orang, karena jika data tersebut tidak diamankan terlebih dahulu, akan relatif mudah untuk disadap dan isinya dapat diketahui oleh pihak lain atau pihak yang tidak bertanggung jawab [2]. Basis data merupakan susunan catatan operasional lengkap dari suatu organisasi atau

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

bisnis, yang diatur menggunakan metode tertentu di komputer dan disimpan secara terintegrasi sehingga dapat memberikan informasi yang dibutuhkan pengguna dengan sebaik-baiknya [3].

Basis data di dalam sebuah sistem informasi sangat penting, karena tidak ada sistem informasi yang dibangun tanpa adanya basis data. Keamanan basis data berkaitan dengan perlindungan terhadap basis data dari ancaman terhadapan perubahan, penghapusan dan pencurian data, baik dengan menggunakan elemen kontrol peralatan komputasi maupun non-komputasi [4] Oleh karena itu, agar tidak ada pihak yang tidak berwenang yang dapat mengubah atau mencuri data yang ada, dibutuhkan metode untuk melindungi data dalam database sistem.

Banyak teknik yang dapat digunakan untuk mengamankan atau penyandian data diantaranya adalah menggunakan teknik kriptografi. Kriptografi merupakan ilmu dan seni yang digunakan untuk menjaga kerahasiaan atau privasi pesan dengan cara kerja mengubah kode menjadi bentuk yang tidak dapat dipahami. Terdapat dua proses dalam ilmu kriptografi, yaitu melakukan proses enkripsi dan dekripsi.

Proses enkripsi memberi sandi plainteks(pesan yang telah dienkripsi atau di berikan kode) ke cipherteks (teks sandi). Pesan yaitu data atau informasi yang dapat dibaca dan dipahami dari maknanya [5]. Kriptografi dapat dipahami sebagai bagian dari matematika yang mempelajari aspek informasi dan keamanan, dilindungi, validasi, integritas maupun otentikasi data [6]. Penelitian oleh Maulana, D.K., et.al (2023) menggunakan algoritma Vigenere cipher untuk mengenkripsi password di dalam database. Dengan mengubah data menjadi kata sandi yang tidak dapat ditebak oleh orang yang tidak berwenang, aplikasi kriptografi yang dibuat dalam penelitian ini dapat dimanfaatkan untuk menyandikan informasi atau data penting [7].

Penelitian lain oleh Zulfikar dan Mulyati (2022) yang membahas mengenai penerapan kriptografi dengan menggunakan algoritma Caesar Cipher dan Vigenere Cipher. Aplikasi yang telah diimplementasikan dapat berguna dan dipakai sistem keamanannya oleh PT Multi Mitra Usaha Bersama. Aplikasi ini diimplementasikan menggunakan bahasa pemrograman PHP. Enkripsi dan dekripsi teks menggunakan algoritma Caesar Cipher dan Vigenere Cipher. Algoritma kriptografi diimplementasikan untuk menu transaksi, data barang, supplier, dan customer. Penelitian ini menggunakan kunci berbeda-beda pada saat enkripsi dan dekripsi [8].

Penelitian oleh Handoko, L.B., dan Umam, C. (2022) menyatakan fungsi hash SHA-256 digunakan untuk generate kunci agar menjadi standar kunci dari AES-256 bekerja dengan baik. Penerapan Vigenere Cipher dan AES256 pada aplikasi chatting dengan realtime database firebase bekerja dengan baik, dibuktikan dengan dengan running-time yang cepat dan teks pesan yang berhasil diamankan dengan kriptografi tersebut[9]. Vigenere Cipher dibuat dengan proses penyandian data dari plaintext menjadi ciphertext dengan menggunakan tabel diagram dengan huruf alfabet terurut secara diagonal atau umum.

Huruf-huruf plaintext pertama-tama disusun satu per satu di bagian atas, diikuti dengan kunci di sebelah kiri. Selanjutnya, cari titik temu huruf untuk mendapatkan ciphertext yang diperlukan, dan seterusnya hingga plaintext akhir. Jika kunci tidak cukup, mulailah dari awal dengan huruf pertama lagi[10]. Kesulitan kriptanalisis menggunakan metode analisis frekuensi merupakan salah satu kelebihan Vigenère cipher karena dua huruf yang sama pada teks kode tidak selalu dapat diterjemahkan menjadi dua huruf yang sama pada teks aslinya. Sementara jika pembuat kunci Vigenère Cipher lupa kunci yang dibuat itu merupakan kelemahan terbesarnya [11]

Berdasarkan penelitian-penelitian di atas dapat disimpulkan bahwa penelitian sebelumnya memiliki beberapa perbedaan yaitu dari pola yang digunakan untuk merancang kriptografi, serta proses kriptografi yang dilakukan. Pada penelitian ini mencoba menggabungkan kombinasi algoritma Vigenere Cipher dan Secure Hash Algorithm (SHA) 256 dalam mengamankan atau melakukan enkripsi basis data, khususnya pada data penduduk pada sistem informasi pelayanan administrasi desa Girisuko.

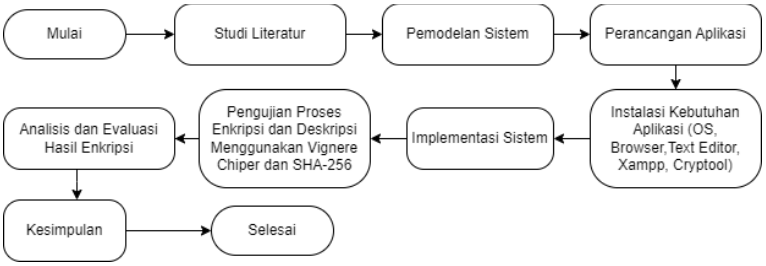
Teks dalam database dienkripsi menggunakan Vigenere Cipher, dan SHA-256 digunakan untuk menghasilkan hash value atau nilai acak yang berbeda dari teks di dalam database. Pesan akan terenkripsi menggunakan Vigenere Cipher dan kemudian di-hash dengan SHA-256 secara bersamaan. Akibatnya, akan sulit bagi penyerang untuk mendekripsi teks yang disimpan dalam database karena harus memecahkan enkripsi Vigenere Cipher, dan juga harus memecahkan hash value yang dihasilkan menggunakan SHA-256. Kombinasi ini bertujuan untuk meningkatkan keamanan sistem aplikasi dan basis data dan menjaga kerahasiaan pesan dari penyerang dari berbagai tindak kejahatan. Dengan dilakukannya penelitian ini diharapkan dapat berkontribusi dalam meningkatkan keamanan sistem basis data.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Peneliti melakukan teknik penelitian, yaitu tahapan yang melibatkan pengumpulan informasi atau data dan melakukan analisis terhadapnya. Tahapan dalam penelitian ini terdiri dari studi literatur, pemodelan sistem, perancangan aplikasi, instalasi kebutuhan aplikasi seperti instalasi (sistem operasi, browser, text editor, xampp, dan CrypTool 2.1), implementasi sistem, proses pengujian proses enkripsi dan dekripsi menggunakan algoritma Vigenere Cipher dan SHA-256, hasil pengujian di analisis dan evaluasi sehingga menghasilkan kesimpulan. Berikut skema tahapan penelitian yang digambarkan pada Gambar 1.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583



Gambar 1. Tahapan Penelitian

Tahapan pada penelitian ini terdiri dari beberapa tahapan. Pada tahapan studi literatur, peneliti mempelajari jurnal, artikel web, buku dan sumber internet lainnya yang berkaitan dengan algoritma kriptografi Vigenere Cipher dan SHA256. Pada tahapan perancangan sistem atau aplikasi diperlukan adanya analisis kebutuhan pada sistem. Setelah mengetahui kebutuhan sistem dan perancangan sistem dilakukan tahapan instalasi kebutuhan aplikasi yaitu dilakukannya instalasi perangkat lunak yang akan digunakan untuk membangun sistem. perangkat lunak yang digunakan yaitu browser, text editor (Visual Studio Code), Xampp, dan database yang digunakan menggunakan MySQL, kemudian Cryptool yaitu perangkat lunak untuk kriptografi dan melakukan fungsi hash. Kemudian dilakukan implementasi sistem administrasi pelayanan administrasi desa Girisuko menggunakan kombinasi kriptografi Vigenere Cipher dan SHA256 untuk keamanan database. Sistem yang diimplementasi kemudian dilakukan pengujian menggunakan Cryptool untuk menguji proses enkripsi dan dekripsi algoritma Program gratis (Open Source) yang disebut CrypTool digunakan untuk menjelaskan atau menjelaskan prinsip-prinsip kriptografi dan kriptanalisis[12]. Vigenere Cipher dan pengujian nilai hash yang dihchipasilkan menggunakan SHA256. Hasil pengujian kemudian dianalisis dan dievaluasi sehingga menghasilkan kesimpulan penelitian.

2.2 Vigenere Cipher

Giovan Battista Bellaso, seorang kriptografer Italia, menciptakan Vigenere Cipher pada tahun 1553. Namun, Blaisede Vigenère, seorang kriptografer Prancis dari abad ke-16, dikaitkan dengan Vigenere Cipher karena menciptakan sandi yang serupa pada tahun 1586. Sandi Vigenère adalah bentuk sandi substitusi yang digunakan untuk enkripsi data. Ini menggunakan semacam substitusi cipher monoalphabetic untuk membuat struktur plaintext asli tampak agak kabur dalam ciphertext. Substitusi mana yang akan diterapkan untuk menyandikan setiap simbol plaintext ditentukan oleh kunci kode. Cipher polyalphabetic berikutnya telah digunakan untuk waktu yang sangat lama. Perbedaan utama adalah bagaimana kelompok yang berbeda dari aturan substitusi monoalphabetic dipilih menggunakan kunci [13]. Vigenere Cipher menggunakan tabel substitusi alfabet 26x26 yang disusun secara horizontal dan vertikal sebagai bagian dari sandi polialfabet [14]. Ciphertext yang dihasilkan di awal akan mengenkripsi data dengan menggeser posisi bagian-bagian karakter melalui transposisi, maka algoritma Vigenere lebih menantang untuk dipecahkan [15]. Vigenere Cipher menggunakan kunci dengan panjang tertentu, kunci bisa kurang dari atau sama dengan panjang teks aslinya. Kunci ini dibuat oleh pembuat kunci. Kunci akan diulang hingga panjang kunci sama dengan panjang plaintext (teks asli). Algoritma enkripsi Vigenere Cipher sebagai berikut:

$$Ci = (Pi + Ki) \bmod 95 \quad (1)$$

Algoritma dekripsi vigenere cipher:

$$Pi = (Ci - Ki) \bmod 95 \quad (2)$$

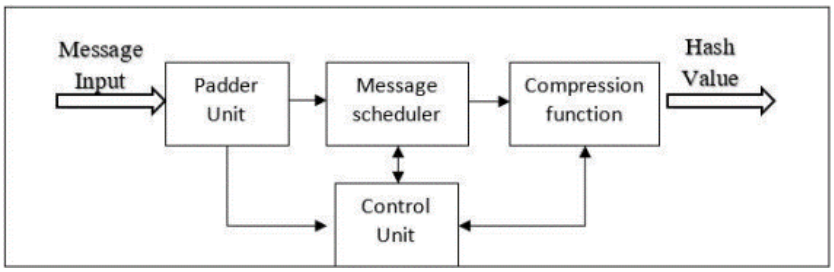
Dimana:
Ci = nilai decimal karakter ciphertext ke-i
Pi = nilai decimal karakter plaintext ke-i
Ki = nilai decimal karakter kunci ke-i

2.3 SHA256

Secure Hash Algorithm (SHA) yang dikembangkan oleh National Institute of Standards and Technology (NIST) juga dirancang dengan prinsip yang sama dengan MD4 dan diterbitkan sebagai Federal Information Processing Standard (FIPS 180) pada tahun 1993. Fungsi hash adalah algoritma Kriptografi yang memampatkan pesan (kompresi) dari berbagai ukuran pesan menjadi intisari pesan tetap. Beberapa fungsi hash, antara lain MD (Message Digest) 5, SHA-1, SHA-2, Keccak (SHA-3), SHA256, RIPEMD, dan seterusnya. SHA256 merupakan SHA generasi ke-2 (kedua). Fungsi hash bersifat satu arah, artinya pesan yang dikompres menjadi hash (ciphertext) maka pesan tersebut tidak dapat dikembalikan ke pesan aslinya. Fungsi hash menjadi bagian penting dalam kriptografi, dengan fungsi hash sebuah pesan keamanan dapat diuji integritasnya, karena dua pesan yang berbeda (meskipun hanya satu karakter yang berbeda) akan menghasilkan hash yang berbeda secara signifikan [16]. Fungsi kompresi SHA-256 membutuhkan 2^{256} upaya untuk memecahkan nilai hash karena 64 putarannya, dua jenis fungsi

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

non-linear, rotasi siklik, dan konstanta yang bergantung pada putaran [17]. Gambar 2 di bawah ini akan menjelaskan mengenai arsitektur SHA256.



Gambar 2. Arsitektur SHA256 [18]

Pada Gambar 2 yaitu arsitektur SHA256, yaitu message input yaitu pesan dari file pesan atau data yang disediakan sebagai input ditentukan menggunakan SHA. File atau pesan dilihat sebagai kumpulan bit. Jumlah bit dalam pesan menentukan berapa panjangnya (pesan kosong memiliki panjang 0). Pada tahapan Massage Padding Dimungkinkan untuk menampilkan pesan dalam format heksadesimal agar lebih mudah dibaca jika jumlah bit adalah kelipatan 8. Membuat seluruh panjang konten pesan menjadi kelipatan 512 bit adalah tujuan dari padding pesan. Saat menghitung intisari pesan, SHA melewati blok 512 bit secara berurutan. Proses parsing menambahkan biner "1" atau "0", hingga 64-bit, dan satu "1" ke padding pesan untuk membuat pesan dengan panjang 512 * n. Proses massage expansion yaitu panjang pesan asli sebelum padding pesan diwakili oleh bilangan bulat 64 bit dan diberi label W0 hingga W63. Proses pemrosesan memiliki 64 operasi setiap rondenya. Tahapan message scheduler yaitu setiap pemrosesan akan dijadwalkan kemudian akan dihitung nilai hash untuk setiap blok pesan. Pada tahapan message compression merupakan sebuah fungsi yang berdasarkan informasi dari penjadwal pesan di setiap putaran kemudian mengeksekusi operasi hashing sebenarnya dari pesan tersebut [19]. Kata yang telah dilabeli W0 hingga W63 diproses menggunakan SHA256 dengan membuat 8 variabel dan diberikan nilai awal L0 hingga L7. Tabel 1 akan menjelaskan mengenai nilai awal tersebut.

Tabel 1. Nilai Awal SHA256

L0	a	6A09E667	L4	e	510E527F
L1	b	BB67AE85	L5	f	9B05688C
L2	c	3C6EF372	L6	g	IF83D9AB
L3	d	A54FF53A	L7	h	5BE0CD19

Setelah itu dilakukan perhitungan dengan 64 kali putaran untuk setiap blok. Nilai awal untuk delapan variabel berkisar dari L0 hingga L7, dengan asumsi bahwa mereka memiliki nilai a, b, c, d, e, f, g, dan h, dan nilainya akan berubah selama siklus. Keluaran sebesar 256 message digest diperoleh setelah pemrosesan.

2.5 Data Penelitian

Data penelitian berupa data penduduk yang ada di dalam sistem informasi pelayanan administrasi desa. Data yang dienkripsi yaitu data penduduk yang terdiri dari data NIK, nomor KK, nama, tempat tanggal lahir dan alamat. Berikut data penduduk pada Tabel 2.

Tabel 2. Data Penduduk Girisuko

NIK	No KK	Nama	Tempat Lahir	Tanggal Lahir	Alamat
9977xxxxx4367	76764xxxxx76850	Yawas	Yogyakarta	199x-08-xx	Pacar
1505xxxxx0001	1111xxxxx4444	Rian Oktafiani	Muaro Jambi, Jambi	199x-10-xx	Gebang RT.01
1505xxxxx0001	1111xxxxx4444	Wasgi	Gunung Kidul, DI Yogyakarta	196x-01-xx	Gebang RT.01
1505xxxxx0001	1111xxxxx4444	Suwartini	Gunung Kidul, DI Yogyakarta	196x-09-xx	Gebang RT.01
……	……..	……	……	…….	……
34030xxxx0001	3404xxxxx5843	Giyono	Gunungkidul	196x-01-xx	Gebang

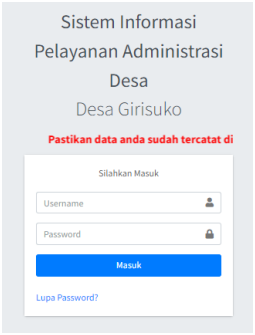
Data penduduk Girisuko pada Tabel 2 akan digunakan untuk penelitian ini. Data penduduk memiliki data sensitif yang bersifat privasi dan rahasia seperti data NIK, nomor KK, serta tempat tanggal lahir. Oleh karena itu, dalam penelitian ini, data penduduk akan dienkripsi menggunakan algoritma Vigenere cipher dan dilakukan hash value menggunakan SHA256.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

3. HASIL DAN PEMBAHASAN

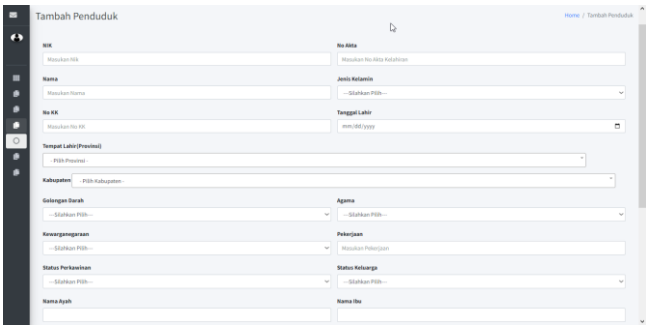
3.1 Hasil Perancangan Sistem

Penelitian ini menggunakan basis data yang dibuat menggunakan MySql. Isi basis data terdiri dari tabel penduduk. Antarmuka sistem informasi pelayanan administrasi desa ini dibangun menggunakan bahasa pemrograman PHP. Penelitian ini menggunakan kombinasi algoritma Vigenere Cipher dan SHA256 untuk mengenkripsi data di dalam database penduduk. Pertama, data akan dienkripsi menggunakan Vigenere Cipher, kemudian file hasil enkripsi Vigenere Cipher digunakan untuk proses kriptografi menggunakan SHA256. Data yang telah dienkripsi menggunakan Vigenere Cipher dan SHA256 akan sulit dipecahkan. Implementasi sistem disajikan dalam bentuk website sistem informasi pelayanan administrasi desa Girisuko. Gambar 3 dan Gambar 4 merupakan implementasi dari halaman login dan halaman form data penduduk.



Gambar 3. Halaman Login

Sistem informasi pelayanan administrasi desa Girisuko, hanya dapat diakses oleh pihak yang berwenang yaitu bagian petugas pelayanan administrasi, sekretaris desa dan kepala desa. Pengguna sistem harus melakukan login dengan menginputkan username dan password untuk masuk kedalam sistem, seperti pada Gambar 3.



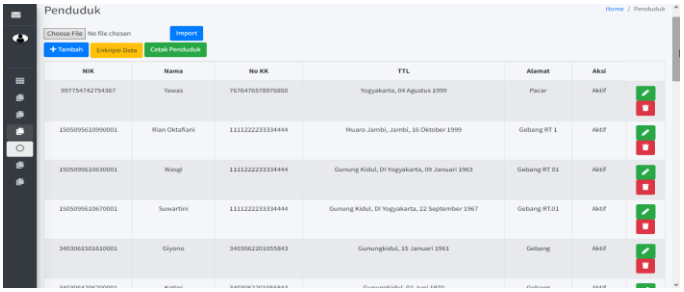
Gambar 4. Halaman Tambah Penduduk

Gambar 4 merupakan halaman tambah penduduk, halaman ini digunakan untuk menginputkan data penduduk. Algoritma Vigenere Cipher dan fungsi hash SHA-256 akan diterapkan pada halaman ini. Ketika petugas menginputkan data penduduk maka sistem akan otomatis mengenkripsi data penduduk yang diinputkan.

3.1.1 Implementasi Metode

a. Proses Enkripsi Data Penduduk

Dalam melakukan proses enkripsi data penduduk, admin terlebih dahulu memilih menu tambah data penduduk. Admin dapat menekan tombol tambah atau import file data penduduk berformat excel dengan memilih file excel dan menekan tombol import. Setelah admin menginputkan data penduduk kemudian menekan tombol enkripsi, maka data penduduk akan otomatis terenkripsi dan ditambahkan ke dalam database.



Gambar 5. Halaman Data Penduduk

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

Algoritma proses enkripsi ini menerangkan bagaimana proses algoritma Vigenere Cipher melakukan proses enkripsi sehingga berhasil mendapatkan ciphertext. Pada proses ini akan menerangkan plaintext menjadi ciphertext yang nantinya akan dilakukan proses menggunakan algoritma Vigenere Cipher. Gambar 6, merupakan kode program untuk enkripsi data pada database penduduk.

1. Masukkan plaintext
2. Masukkan kunci
3. P = Plaintext; C = Ciphertext; K = Kunci; len = Panjang Plaintext
4. i = 0
5. num;
6. for (i < len(P)) do
7. num = mod(num(C[i]) – num(K[i % strlen(K)]), 95)
8. C .= chr(num + ord('A'))
9. i++
10. end for
11. Return (C)
12. Tampilkan hasil
13.Selesai

```php
<?php
    $eks = array('.txt');
    $ekst = strrchr($_FILES['teks']['name'],'.');
    $kunci = $_POST['key']; $idx =0; $idx1 = 0; $j =0;

    if(!in_array($ekst,$eks)) {
    echo "<script>alert('datapenduduk.xls');location.replace('enkripsi.php');</script>";
    //echo $ekst;
    }

    if ($_FILES['teks']['error'] == UPLOAD_ERR_OK && is_uploaded_file($_FILES['teks']['tmp_name'])) { //checks
    $isi = file_get_contents($_FILES['teks']['tmp_name']);
    }
    for($k=0;$k<=strlen($tab);$k++) {
        if($kunci[$j]==$tab[$k] || $kunci[$j]==$tab1[$k]) {
            $idx1 = $k;
        }   }
        $hasil = ($idx + $idx1)%;
    if($hasil<0) {
        $hasil1 = ($hasil+95)%95;
        array_push($ciparr,$tab[$hasil1]);
    } else {
        array_push($ciparr,$tab[$hasil]);
    }
        if($j==(strlen($kunci)-1)) {
        $j = 0;
    } else {
        $j++;
    }
}
$cipher1 = implode('',$ciparr);
?>
```

Gambar 6. Kode Program Enkripsi Vignere Cipher

Pada Gambar 6 di atas, merupakan kode program enkripsi menggunakan Vigenere Cipher, file yang diupload yaitu file datapenduduk.xls akan dienkripsi secara otomatis menggunakan kode program tersebut. Keluaran program, yaitu data yang telah dienkripsi dapat dilihat pada database data penduduk. Setelah muncul notifikasi input data penduduk berhasil terenkripsi oleh aplikasi ini, maka seluruh data akan masuk kedalam database dengan bentuk atau huruf acak algoritma Vigenere Cipher dan SHA-256. Seperti Tabel 3 berikut ini:

Tabel 3. Data Penduduk Terenkripsi

NIK	No KK	Nama	Tempat Lahir	Tanggal Lahir	Alamat
739493786596006	5093866916393240	Qeyrw	Qsipedkvrs	88 Cxyldyq 9316	Heerv
9922485058317491	9538612671751834	Jmce Sddedaepz	Eycis Ckqza, Ncdfb	90 Qbxhlip 9316	Yidrrz BX.49
9922485058057491	9538612671751834	Oeuxm	Yyplrz Umbmp, FZ Chqcycetke	83 Lrrnkvg 9380	Yidrrz BX.49
9922485058097491	9538612671751834	Kyyrvmsrg	Yyplrz Umbmp, FZ Chqcycetke	06 Uvtmoqzwv 3606	Yidrrz BX.49
……	……..	……	……	……	……
1820451949037491	1820452649472233	Ymafrh	Yyplrzumbmp	99 Lrrnkvg 9388	Yidrrz

Pada Tabel 3, data penduduk telah dienkripsi menggunakan algoritma vigenere cipher. Database tersebut akan disimpan menjadi sebuah file, kemudian file tersebut akan dienkripsi menggunakan fungsi hash SHA256 secara otomatis. Pada Gambar 7 merupakan kode program untuk menjalankan fungsi hash SHA256 pada file database data penduduk.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583


```php
<?php
/* Create a file to calculate hash of */
file_put_contents('enkripsipenduduk.xml', 'datapenduduk');

echo hash_file('sha256', 'enkripsipenduduk.xml');
?>
```

Gambar 7. Kode Program Fungsi Hash SHA256

Setelah kode program pada Gambar 7 dijalankan pada sistem, maka otomatis file database penduduk akan dienkripsi menggunakan Vigenere Cipher dan SHA256. Data di dalam database yang sebelumnya telah dienkripsi menggunakan Vigenere Cipher kemudian file hasil enkripsi dikombinasikan atau dienkripsi ulang menggunakan fungsi hash SHA256. Gambar 7 menjelaskan, menggambil file enkripsipenduduk.xls kemudian dilakukan file tersebut dienkripsi menggunakan SHA256, kemudian file akan ditampilkan menjadi kode SHA256 seperti pada Gambar 8.

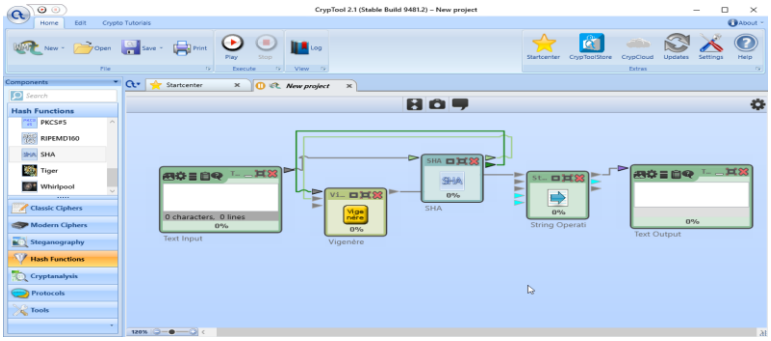
e9615f9c05e0a4b6cb53382d994249fc0ad8f2f6c9c1a6d43dd93b4622074216

Gambar 8. Hasil Enkripsi File Menggunakan Kombinasi Vigenere Cipher dan SHA256

Gambar 8, merupakan kode acak hasil kombinasi algoritma Vigenere Cipher dan SHA256. Kode acak ini akan sulit dipecahkan, karena untuk memecahkan kode ini harus mendekripsi algoritma SHA256 terlebih dahulu. Namun setelah dekripsi SHA256, didalamnya terdapat file yang telah terenkripsi menggunakan Vigenere Cipher. Pada penelitian ini, setelah implementasi pada sistem akan dilakukan pengujian mengenai kombinasi algoritma Vigenere Cipher dan SHA256.

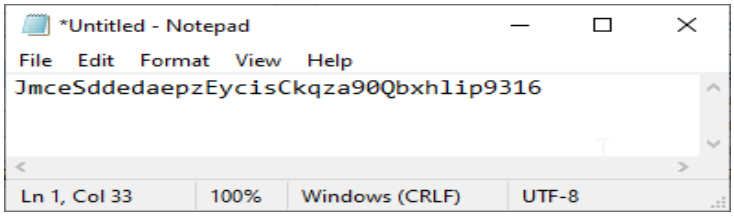
3.2 Pengujian

Proses pengujian menggunakan aplikasi CrypTool 2.1. Langkah awal yaitu dengan menambahkan text input untuk memasukkan teks yang telah terenkripsi. Algoritma Vigenere Cipher dan SHA-256 akan diimplementasikan terhadap teks tersebut. Kemudian ditambahkan operasi string. Ketika dijalankan maka akan tampil hasil pada text output. Berikut pada Gambar 9, merupakan proses pengujian menggunakan tool CrypTool 2.1 mengenai implementasi algoritma Vigenere Cipher dan SHA-256 dan hasil yang didapat.



Gambar 9. Rancangan Simulasi dekripsi dengan Kombinasi SHA-256 dan Vigenere Cipher pada Aplikasi CrypTool

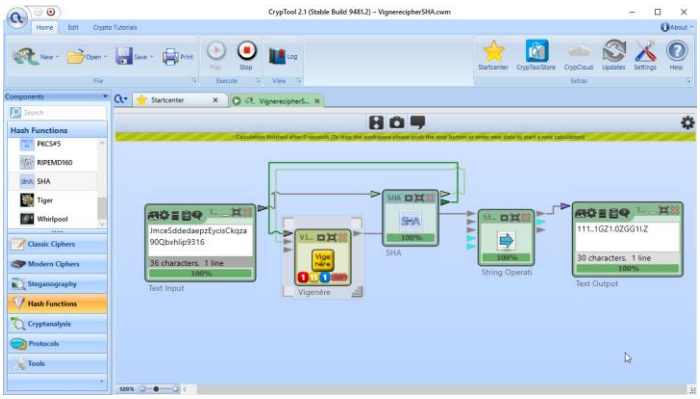
Gambar 9 merupakan rancangan simulasi dekripsi menggunakan aplikasi CrypTool. Rancangan simulasi terdiri teks input yang digunakan untuk menginputkan data teks. Kemudian inputan data akan dienkripsi menggunakan Vigenere Cipher dan SHA256. Vigenere Cipher akan dihubungkan dengan SHA 256 dan sebaliknya. Kemudian hasil enkripsi menggunakan fungsi hash SHA256 akan dihubungkan dengan String Operation yang berfungsi untuk memodifikasi nilai string. Kemudian yang terakhir yaitu setelah operasi string, hasil enkripsi akan dihubungkan dengan Text Output yang berfungsi untuk menampilkan teks hasil enkripsi. Gambar 10 merupakan contoh teks hasil enkripsi menggunakan Vigenere Cipher, kemudian teks yang telah terenkripsi akan diinputkan dalam teks input dan diproses.



Gambar 10. Contoh kode hasil enkripsi

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

Setelah kode pada Gambar 10 tersebut dimasukkan, maka dapat menjalankan simulasi dengan menekan tombol “Play” yang tersedia. Pada Gambar 11 di bawah dapat dilihat hasil dari proses dekripsi atau decode.

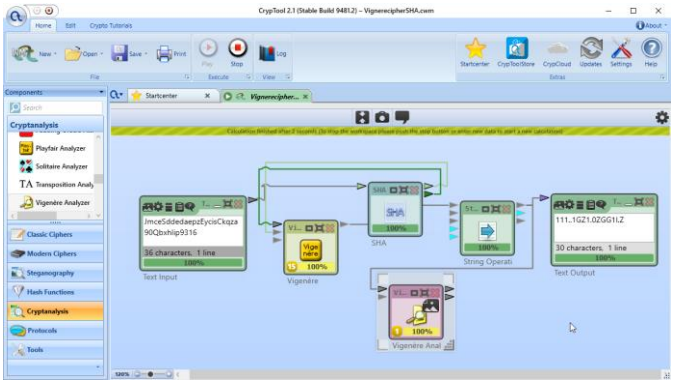


Gambar 11. Hasil Simulasi Dekripsi dengan Kombinasi Vigenere Cipher dan SHA-256 pada CrypTool

Gambar 11 merupakan hasil simulasi dekripsi menggunakan algoritma Vigenere Cipher dan fungsi hash SHA-256, hasil tersebut menunjukkan bahwa teks tidak berhasil di dekripsi seperti teks aslinya.

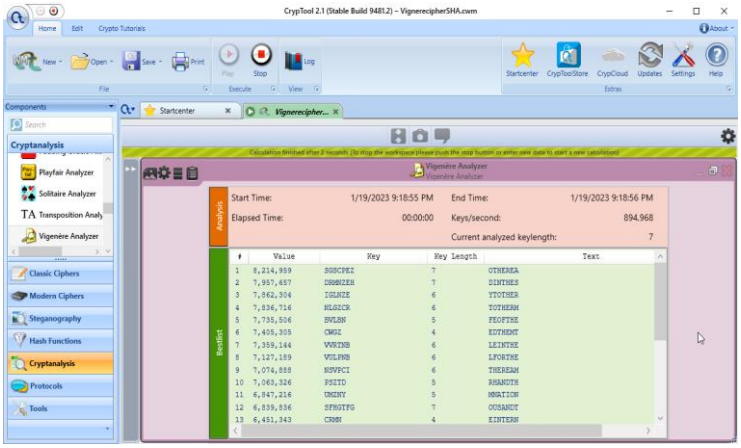
3.3 Analisis Hasil dan Evaluasi

Dalam melakukan analisis kriptografi yang diterapkan, pada penelitian ini menggunakan Cryptanalysis pada CrypTool 2.1. Analisis yang dilakukan yaitu dengan menambahkan Vigenere Analysis. Berikut pada Gambar 12 merupakan rancangan simulasi cryptanalysis menggunakan vigenere analysis.



Gambar 12. Hasil Simulasi Penerapan Vigenere Analysis pada CrypTool

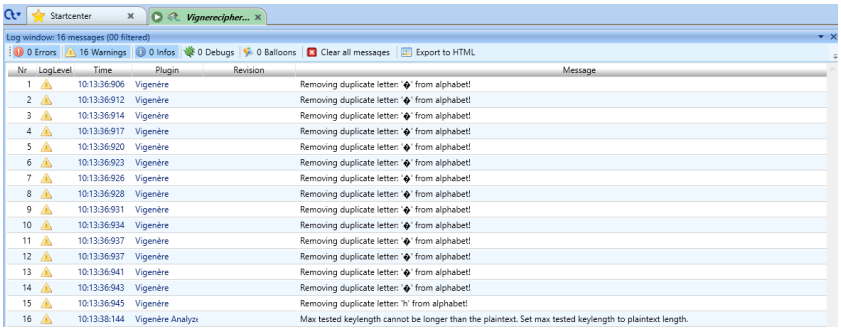
Pada Gambar 12, merupakan rancangan simulasi untuk penerapan Vigenere Analysis pada Cryptool. Vigenere Analysis berfungsi untuk menganalisis waktu yang dibutuhkan untuk enkripsi teks menggunakan algoritma kriptografi Vigenere Cipher. Pada rancangan simulasi, hasil enkripsi menggunakan vigenere cipher dan SHA 256, dan pada string operation dihubungkan dengan Vigenere Analysis agar mendapatkan hasil analisis kecepatan enkripsi dan jumlah kunci perdetik saat enkripsi menggunakan Vigenere Cipher seperti pada Gambar 13 di bawah ini.



Gambar 13. Vigenere Analysis pada CrypTool

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 4, Nomor 3, Maret 2023
e-ISSN 2685-998X
DOI 10.30865/json.v4i3.5583

Hasil vigenere analysis dan log pada CrypTool pada Gambar 13 di atas menunjukkan bahwa waktu dekripsi menggunakan algoritma Vigenere Cipher dan SHA-256 memerlukan waktu 0.39 detik dengan analyzed keylenght sebesar 7 karakter, kemudian proses enkripsi menggunakan Vigenere Cipher dan SHA-256 pada aplikasi CrypTool 2.1 sebesar 894.968 key/second. Agar lebih jelas mengenai waktu enkripsi dilakukan pengecekan pada Log Cryptool seperti pada Gambar 14.



Gambar 14. Log pada CrypTool

Log Cryptool pada Gambar 14, menunjukkan bahwa waktu enkripsi dimulai pada 10:13:36:906 dan berakhir pada 10:13:38:144, yang berarti waktu untuk melakukan enkripsi menggunakan Vigenere Cipher dan SHA256 yaitu 0,39 detik. Hasil enkripsi SHA256 setelah dilakukan pengujian juga tidak berhasil didekripsi dengan mudah menggunakan tool Cryptool, hal ini menunjukkan bahwa penerapan kriptografi dengan menggunakan algoritma vigenere cipher dan SHA-256 berhasil untuk mengenkripsi teks pada database.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat disimpulkan bahwa, penelitian ini berhasil merancang keamanan basis data dengan antarmuka data penduduk pada sistem informasi pelayanan administrasi desa Girisuko. Teks dalam database dienkripsi menggunakan Vigenere Cipher, dan SHA-256 digunakan untuk menghasilkan hash value atau nilai acak yang berbeda dari teks di dalam database. Pesan akan terenkripsi menggunakan Vigenere Cipher dan kemudian di-hash dengan SHA-256 secara bersamaan. Penelitian ini berhasil menerapkan kombinasi teknik enkripsi Vigenere Cipher dan SHA-256. Dari hasil pengujian dengan menggunakan CrypTool 2.1 dapat diketahui bahwa Kombinasi SHA-256 dan Vigenere Cipher tidak berhasil didekripsi atau di-decode seperti teks asli. Fungsi hash pada algoritma SHA-256 yang digunakan untuk generate kunci agar menjadi standar kunci dari Vigenere Cipher berkerja dengan baik. Penerapan Vigenere Cipher dan SHA pada aplikasi sistem informasi pelayanan administrasi desa dengan realtime database bekerja dengan baik, dibuktikan dengan dengan running-time yang cepat yaitu 0.39 detik proses enkripsi data menggunakan vigenere cipher dengan hasil sebesar 894.968 keys/second dan analyzed keylenght sebanyak 7 karakter, kemudian teks pada database data penduduk berhasil diamankan dengan kriptografi Vigenere Cipher dan SHA-256. Dari hasil pengujian yang didapat, diharapkan pengembang dapat mengembangkan atau memperbaiki kombinasi teknik kriptografi lainnya, baik yang klasik maupun modern guna meningkatkan dan mengembangkan keamanan sistem basis data.

REFERENCES

[1] M. Sari, H. D. Purnomo, and I. Sembiring, “Review : Algoritma Kriptografi Sistem Keamanan SMS di Android,” Journal of Information Technology, vol. 2, no. 1, pp. 11–15, Mar. 2022, doi: 10.46229/jifotech.v2i1.292.
[2] F. Husaini, A. Pardede, and I. Gultom, “Penerapan Enkripsi Menggunakan Metode Elgamal guna Meningkatkan Keamanan Data Text dan Gambar,” JUKI: Jurnal Komputer dan Informatika, vol. 4, no. 1, pp. 55–61, May 2022, doi: https://doi.org/10.53842/juki.v4i1.104.
[3] S. R. Ningsih et al., Perancangan Basis Data, 1st ed. Yayasan Kita Menulis, 2022.
[4] A. M. Dirgayusari, N. Ahmad, B. T. Mahardika, Musyrifah, and H. Gemasih, Basis Data, 1st ed., vol. 1. Tangerang: Media Sains Indonesia, 2022.
[5] H. Bancin, M. A. Panjaitan, S. Putri, and A. B. Nasution, “Implementasi Kriptografi dengan Metode Caesar Chiper untuk Mengamankan Data File di Javanetbeans,” Jurnal Pendidikan Sains dan Teknologi, vol. 2, no. 1, pp. 17–21, Jan. 2023, doi: https://doi.org/10.47233/jpst.v2i1.438.
[6] K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, “Penerapan Kriptografi Caesar Cipher Pada Fitur Aplikasi Chatting Whatsapp,” JPPIE: Jurnal Hasil Penelitian dan Pengkajian Ilmiah Eksakta, vol. 2, no. 1, pp. 6–11, Jan. 2023, doi: https://doi.org/10.47233/jppie.v2i1.660.
[7] D. K. Maulana, S. M. Tanjung, R. S. Ritonga, and A. Ikhwan, “Penerapan Kriptografi Vigenere Cipher Pada Kekuatan Kata Sandi,” Jurnal Sains dan Teknologi (JSIT), vol. 3, no. 1, pp. 47–52, Jan. 2023, doi: https://doi.org/10.47233/jsit.v3i1.483.
[8] M. R. Zulfikar and S. Mulyati, “Penerapan Kriptografi Caesar Cipher Dan Vigenere Cipher Untuk Mengamankan Database Barang Belting Pada PT. Multi Mitra Usaha Bersama. Senafti : Seminar Nasional Mahasiswa Fakultas Teknologi

Informasi," in Prosiding Seminar Nasional Mahasiswa Fakultas Teknologi Informasi (SENAFTI), Sep. 2022, pp. 402–410. Accessed: Jan. 22, 2023. [Online]. Available: https://senafti.budiluhur.ac.id/index.php/senafti/article/view/471

[9] L. B. Handoko and C. Umam, "Kombinasi Vigenere-Aes 256 dan Fungsi Hash Dalam Kriptografi Aplikasi Chatting," Prosiding Sains Nasional dan Teknologi, vol. 12, no. 1, p. 390, Nov. 2022, doi: 10.36499/psnst.v12i1.7068.

[10] D. Astuti and C. Sundari, "Sistem Keamanan Data Obat dengan Implementasi Algoritma Vigenere Cipher pada Puskesman Mertoyudan I Magelang," in Prosiding Seminar Nasional STIE AAS, Dec. 2022, pp. 145–156. Accessed: Feb. 28, 2023. [Online]. Available: https://prosiding.stie-aas.ac.id/index.php/prosenas/article/view/202

[11] I. Saputra and S. D. Nasution, "Perbandingan Performa Algoritma Md5 Dan SHA-256 Dalam Membangkitkan Identitas File," Jurnal Sains Komputer dan Informatika (J-SAKTI), vol. 5, no. 2, pp. 240–254, Mar. 2022, doi: http://dx.doi.org/10.30645/j-sakti.v6i1.435.

[12] N. Rismawati and M. F. Mulya, "Analisis dan Perancangan Simulasi Enkripsi dan Dekripsi pada Algoritma Steganografi untuk Penyisipan Pesan Text pada Image menggunakan Metode Least Significant Bit (LSB) Berbasis Cryptool2," Faktor Exacta, vol. 12, no. 2, p. 132, Jul. 2019, doi: 10.30998/faktorexacta.v12i2.3527.

[13] M. A. Ruswandi and W. Windarto, "Enkripsi Database Sistem Informasi Helpdesk Dengan Algoritme Kriptografi Aes-128 Dan Vigenere Chiper," SKANIKA, vol. 5, no. 2, pp. 240–254, Jul. 2022, doi: 10.36080/skanika.v5i2.2957.

[14] A. Y. Suseno, N. Sulistiyowati, and P. -, "Analisis Peningkatan hybrid Cryptosystem Untuk Enkripsi dan Dekripsi Menggunakan Vigenere Cipher dan RSA Pada Text," STRING (Satuan Tulisan Riset dan Inovasi Teknologi), vol. 6, no. 2, p. 142, Dec. 2021, doi: 10.30998/string.v6i2.10309.

[15] Megawati, Muhammad Fitra Hamidy, Sasqia Ismi Aulia, Yuhendri Putra, and Mhd Arief Hasan, "Enkripsi dan Deskripsi File Menggunakan Kombinasi Vigenere dan Shift Cipher di Python," SATIN - Sains dan Teknologi Informasi, vol. 7, no. 1, pp. 102–111, Jun. 2021, doi: 10.33372/stn.v7i1.686.

[16] I. Surya Permana, T. Hidayat, and R. Mahardiko, "Raw Data Security By Using Elgamal And Sha 256 Public Key Algorithm," TEKNOKOM, vol. 4, no. 1, pp. 1–6, Apr. 2021, doi: 10.31943/teknokom.v4i1.53.

[17] I. Rahim, N. Anwar, A. M. Widodo, K. Karsono Juman, and I. Setiawan, "Komparasi Fungsi Hash Md5 Dan Sha256 Dalam Keamanan Gambar Dan Teks," ikraith-informatika, vol. 7, no. 2, Nov. 2022, doi: 10.37817/ikraith-informatika.v7i2.2249.

[18] Z. Panjaitan, E. F. Ginting, and Y. Yusnidah, "Modifikasi SHA-256 dengan Algoritma Hill Cipher untuk Pengamanan Fungsi Hash dari Upaya Decode Hash," Jurnal SAINTIKOM (Jurnal Sains Manajemen Informatika dan Komputer), vol. 19, no. 1, p. 53, Feb. 2020, doi: 10.53513/jis.v19i1.225.

[19] H. Herman, R. Wijaya, K. Farandi, S. Mihaja, and Wilson, "Implementasi Algoritma Aes-128 Dan Sha-256 Dalam Perancangan Aplikasi Pengamanan File Dokumen," Jurnal Times, vol. 10, no. 2, pp. 80–87, Jan. 2021, Accessed: Feb. 28, 2023. [Online]. Available: https://ejournal.stmik-time.ac.id/index.php/jurnalTIMES/article/view/666