ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

Penerapan Kriptografi untuk Pengamanan Data Nilai Siswa dengan Algoritma Super Enkripsi

Jefry G G Saragih

Fakultas Ilmu Komputer dan Teknologi Informasi, Prodi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: jefrysaragih7@gmail.com

Abstrak−Penelitian ini membahas penerapan kriptografi dengan metode super enkripsi sebagai solusi pengamanan data nilai siswa di SMA Negeri 5 Medan yang masih menggunakan sistem manual sehingga rentan terhadap manipulasi dan kebocoran informasi. Super enkripsi dipilih karena menggabungkan dua teknik cipher untuk memperkuat keamanan, dengan algoritma Vigenere Cipher sebagai salah satu metode yang digunakan dalam enkripsi dan dekripsi data. Tahapan penelitian meliputi studi literatur, analisis kebutuhan sistem, perancangan arsitektur dan algoritma, implementasi aplikasi, pengujian, serta dokumentasi hasil. Proses enkripsi berhasil mengubah plaintext nilai siswa menjadi ciphertext yang sulit dimengerti pihak luar, sementara proses dekripsi mengembalikan ciphertext ke bentuk asli secara akurat menggunakan kunci yang sama. Hasil pengujian menunjukkan bahwa metode ini mampu menjamin kerahasiaan dan integritas data akademik, serta meningkatkan keamanan sistem informasi berbasis multi-user. Dengan demikian, penelitian ini menegaskan bahwa penerapan super enkripsi pada sistem pengolahan nilai siswa tidak hanya menjaga privasi dan keaslian informasi, tetapi juga menjadi solusi strategis dalam menghadapi ancaman keamanan siber di dunia pendidikan.

Kata Kunci: Kriptografi; Vigenere; Trasposisi Kolom; Enkripsi; Pengamanan Pesan; Super Enkripsi

Abstract−This study discusses the application of cryptography using the super-encryption method as a solution for securing student grade data at SMA Negeri 5 Medan, which still relies on manual systems and is therefore vulnerable to manipulation and data leakage. Super-encryption was chosen because it combines two cipher techniques to strengthen security, with the Vigenere Cipher algorithm employed as one of the methods for both encryption and decryption processes. The research stages include literature review, system requirements analysis, architecture and algorithm design, application implementation, testing, and result documentation. The encryption process successfully transformed the plaintext of student grades into ciphertext that is difficult for unauthorized parties to interpret, while the decryption process accurately restored the ciphertext to its original form using the same key. The testing results indicate that this method ensures the confidentiality and integrity of academic data while enhancing the security of multi-user information systems. Thus, this research emphasizes that implementing super-encryption in student grade management systems not only protects privacy and data authenticity but also serves as a strategic solution to address cybersecurity threats in the field of education.

Keywords: Cryptography; Vigenere; Column Trasposition; Encryption; Message Security; Super Encryption

1. PENDAHULUAN

Kriptografi merupakan salah satu disiplin ilmu yang berfokus pada teknik pengamanan data melalui proses enkripsi dan dekripsi yang menjadikan data sulit dipahami oleh pihak tidak berwenang [1]. Algoritma kriptografi terbagi menjadi dua kategori besar, yaitu algoritma simetris dan algoritma asimetris[2][3]. Pada algoritma simetris, enkripsi dan dekripsi menggunakan kunci yang sama sehingga proses dapat berjalan lebih cepat dibandingkan dengan algoritma asimetris[4]. Salah satu keunggulan dari algoritma simetris adalah efisiensi dalam pemrosesan data, khususnya pada data berukuran besar seperti database akademik[5][6]. Kriptografi simetris terdiri dari dua jenis pendekatan, yaitu block cipher dan stream cipher. Block cipher bekerja dengan memproses data dalam blok-blok tetap, sementara stream cipher bekerja dengan mengenkripsi data dalam bentuk aliran bit atau karakter [7]. Dalam konteks pendidikan, penerapan kriptografi pada sistem pengolahan data nilai siswa dapat memberikan proteksi terhadap manipulasi data akademik [8]. Keamanan data nilai siswa menjadi prioritas penting karena menyangkut privasi dan integritas informasi akademik. Oleh karena itu, penggunaan algoritma super enkripsi yang mengombinasikan beberapa teknik simetris dapat memperkuat keamanan data akademik dari potensi peretasan[9].

Kajian mengenai algoritma kriptografi simetris menekankan pada pentingnya pemilihan metode enkripsi yang tidak hanya aman tetapi juga efisien dalam implementasi pada sistem informasi sekolah[10]. Simetris encryption seperti AES, Blowfish, dan Twofish sering digunakan dalam konteks data akademik karena tingkat keamanannya yang tinggi[11]. Namun, setiap algoritma memiliki kelebihan dan kelemahan yang perlu diperhatikan, misalnya AES unggul pada kecepatan enkripsi, sedangkan Blowfish lebih fleksibel pada ukuran kunci[12]. Super enkripsi, yang merupakan kombinasi beberapa algoritma, muncul sebagai pendekatan baru untuk meningkatkan kekuatan keamanan tanpa mengorbankan kinerja[13]. Dengan meningkatnya ancaman serangan siber terhadap data pendidikan, pemilihan algoritma yang tepat menjadi semakin krusial[14]. Hal ini juga sejalan dengan kebutuhan lembaga pendidikan untuk meningkatkan perlindungan terhadap kerahasiaan data nilai siswa[15]. Kajian teori ini menunjukkan bahwa penerapan super enkripsi dalam pengolahan nilai siswa dapat memberikan solusi strategis dalam menghadapi risiko kebocoran data akademik. Dengan demikian, teori kriptografi simetris yang dikombinasikan dalam bentuk super enkripsi dapat dijadikan dasar dalam penelitian ini untuk menjaga keamanan data siswa secara lebih optimal[16].

Permasalahan utama yang dihadapi dalam pengolahan data nilai siswa adalah rendahnya tingkat keamanan informasi akademik yang masih banyak disimpan secara manual maupun dalam sistem sederhana[8]. Kondisi ini

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

menyebabkan data nilai siswa rentan terhadap manipulasi baik dari pihak internal maupun eksternal. Sistem manual yang masih diterapkan membuat proses distribusi nilai kurang efisien dan tidak transparan [17]. Ketika data nilai disimpan tanpa enkripsi, risiko pencurian atau kebocoran data menjadi semakin tinggi. Dalam dunia pendidikan, kerahasiaan data nilai memiliki dampak yang besar karena terkait dengan kredibilitas lembaga dan kepercayaan masyarakat[1]. Permasalahan lain adalah lemahnya pemahaman tenaga pendidik terkait pentingnya penerapan sistem keamanan data digital[14]. Selain itu, ancaman peretasan yang semakin canggih menuntut sistem keamanan yang lebih adaptif dan kuat[13]. Penerapan algoritma klasik yang sederhana sudah tidak memadai dalam melindungi data akademik[11]. Hal ini menegaskan perlunya pengembangan sistem berbasis kriptografi dengan pendekatan super enkripsi untuk meminimalkan risiko manipulasi data. Oleh karena itu, penelitian ini muncul dari kebutuhan nyata untuk memperkuat sistem pengolahan data nilai siswa melalui solusi kriptografi yang lebih inovatif[10].

Selain lemahnya perlindungan data akademik, permasalahan lain terletak pada keterbatasan sistem informasi sekolah dalam mendukung multi-user dengan kontrol akses yang aman. Banyak sistem yang masih belum mampu memisahkan hak akses guru, siswa, dan admin secara efektif sehingga menimbulkan risiko kebocoran data[18]. Minimnya penerapan kriptografi juga menyebabkan data mudah dibaca ketika terjadi peretasan terhadap server sekolah. Sistem manual yang digunakan sebelumnya juga tidak dapat mendeteksi upaya manipulasi nilai sehingga integritas data sering diragukan. Hal ini semakin memperbesar kemungkinan adanya perubahan data tanpa sepengetahuan pihak yang berwenang. Kekurangan lain dari sistem tradisional adalah tidak adanya pencatatan log aktivitas yang memungkinkan jejak digital mudah hilang [15] . Oleh karena itu, solusi berbasis kriptografi yang mengadopsi metode super enkripsi dapat membantu memberikan keamanan ganda terhadap setiap proses transaksi data nilai. Dengan adanya sistem tersebut, setiap pihak hanya dapat mengakses data sesuai otoritasnya sehingga risiko penyalahgunaan dapat ditekan secara signifikan[13]. Kondisi inilah yang mendorong dilakukannya penelitian dalam bidang kriptografi pendidikan untuk memberikan solusi praktis yang aman dan efisien[8].

Penelitian terdahulu oleh [6] menjelaskan bahwa baik kriptografi simetris maupun asimetris memiliki peran krusial dalam keamanan informasi, di mana kriptografi simetris unggul dalam hal kecepatan dan efisiensi pemrosesan data, sementara kriptografi asimetris lebih unggul dalam hal keamanan untuk komunikasi jarak jauh dan tanda tangan digital. Oleh karena itu, pemilihan algoritma yang paling tepat untuk suatu sistem informasi sangat bergantung pada pertimbangan kebutuhan spesifik seperti tingkat keamanan yang diinginkan, efisiensi, dan kemudahan implementasi, dimana sering kali kombinasi keduanya digunakan untuk saling melengkapi keunggulan masing-masing.

Penelitian lain oleh [19] dimana menjelaskan bahwa kemajuan teknologi informasi memang mempermudah akses dan pertukaran informasi, namun hal ini juga membuat informasi menjadi rentan terhadap ancaman keamanan seperti intersepsi dan manipulasi oleh pihak yang tidak bertanggung jawab. Oleh karena itu, kriptografi hadir sebagai solusi penting untuk menjaga kerahasiaan data. Penelitian yang membandingkan kinerja algoritma kriptografi populer seperti DES, AES, IDEA, dan Blowfish menunjukkan bahwa masing-masing algoritma memiliki perbedaan signifikan dalam hal kecepatan proses enkripsi dan dekripsi serta ukuran file hasil enkripsi, sehingga pemilihan algoritma yang tepat harus disesuaikan dengan kebutuhan spesifik akan kecepatan dan efisiensi ruang penyimpanan.

Penelitian yang lebih aplikatif dilakukan oleh [8] dengan menerapkan algoritma AES-256 pada sistem pengolahan data. Penelitian tersebut menunjukkan efektivitas AES-256 dalam melindungi data dari ancaman peretasan, namun masih terbatas pada penggunaan satu algoritma tunggal. Dalam konteks sekolah, penggunaan satu algoritma saja mungkin belum cukup menghadapi serangan yang lebih kompleks. GAP penelitian ini terletak pada kurangnya pendekatan multi-layer yang menggabungkan kekuatan beberapa algoritma. Oleh karena itu, penelitian dengan super enkripsi yang memadukan algoritma simetris berbeda menjadi sangat relevan. Dengan cara ini, sistem pengolahan data nilai dapat terlindungi secara lebih komprehensif. GAP ini sekaligus memperlihatkan bahwa penelitian sebelumnya masih belum sepenuhnya menjawab tantangan keamanan data akademik. Penelitian ini hadir sebagai jawaban atas kebutuhan tersebut. Dengan super enkripsi, sistem pengolahan data nilai siswa dapat lebih aman dan adaptif.

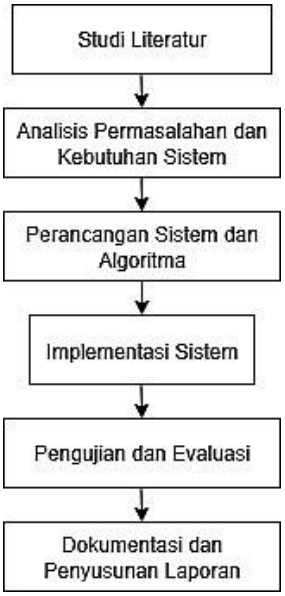
Tujuan utama penelitian ini adalah merancang dan mengimplementasikan sistem pengamanan data nilai siswa berbasis algoritma super enkripsi yang memadukan beberapa algoritma kriptografi simetris. Dengan penerapan super enkripsi, diharapkan data nilai siswa yang tersimpan dalam database sekolah dapat terlindungi dari ancaman manipulasi maupun kebocoran informasi. Selain itu, penelitian ini juga bertujuan untuk memastikan bahwa sistem tetap efisien dan dapat digunakan dalam lingkungan multi-user tanpa mengurangi kinerja aplikasi akademik. Penelitian ini diharapkan dapat memberikan kontribusi nyata terhadap peningkatan keamanan sistem informasi sekolah sekaligus memperkuat integritas data akademik siswa.

2. METODOLOGI PENELITIAN

2.1 Tahapan Penelitian

Tahapan Penelitian untuk Pengamanan Data Nilai Siswa Dengan Algoritma Super Enkripsi yang akan dilakukan dalam penelitian ini dapat dilihat pada Gambar 1 sebagai berikut.

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78



Gambar 1. Tahapan Penelitian

Berdasarkan Gambar 1, berikut penjelasan setiap tahapan yang telah digambarkan agar lebih mudah di pahami tahapan yang dilakukan.

2.1.1 Studi Literatur

Tahap awal penelitian ini adalah melakukan studi literatur untuk memahami konsep dasar kriptografi, algoritma simetris, serta penerapan super enkripsi dalam konteks keamanan data. Studi literatur dilakukan dengan meninjau jurnal internasional, prosiding konferensi, dan penelitian terdahulu yang membahas pengamanan data akademik. Peneliti mengidentifikasi kelebihan dan kelemahan berbagai algoritma simetris seperti AES, Blowfish, dan Twofish. Hasil studi literatur ini menjadi dasar pemilihan algoritma yang akan dikombinasikan dalam penelitian. Selain itu, peneliti juga mengkaji standar keamanan informasi yang relevan dengan sistem pendidikan. Kajian ini bertujuan untuk memastikan penelitian memiliki landasan teoritis yang kuat. Dari literatur juga diperoleh gambaran penelitian terdahulu serta celah riset yang belum terjawab. Tahapan ini juga mencakup analisis kebutuhan sistem akademik, khususnya pengolahan data nilai siswa. Dengan demikian, studi literatur menjadi fondasi penting dalam menentukan arah penelitian.

2.1.2 Analisis Permasalahan dan Kebutuhan Sistem

Setelah studi literatur, tahap berikutnya adalah analisis permasalahan yang dihadapi sekolah dalam mengelola data nilai siswa. Peneliti melakukan observasi langsung terhadap sistem pengolahan nilai di sekolah yang masih manual. Data diperoleh melalui wawancara dengan guru dan staf administrasi untuk mengidentifikasi kelemahan sistem. Hasil analisis menunjukkan adanya kerentanan terhadap manipulasi dan kebocoran data. Dari sini peneliti merumuskan kebutuhan sistem baru yang lebih aman dengan menerapkan kriptografi. Analisis juga mencakup kebutuhan fungsional, seperti otorisasi multi-user, serta kebutuhan non-fungsional, seperti efisiensi waktu enkripsi. Dengan analisis ini, peneliti dapat memetakan risiko dan merancang solusi berbasis super enkripsi. Tahap ini menghasilkan spesifikasi kebutuhan sistem yang menjadi dasar perancangan. Hasil akhir dari tahap ini adalah dokumen kebutuhan sistem yang terstruktur.

2.1.3 Perancangan Sistem dan Algoritma

Pada tahap perancangan, peneliti mulai menyusun arsitektur sistem pengolahan data nilai berbasis kriptografi. Desain mencakup diagram alur proses enkripsi dan dekripsi data. Peneliti merancang skema super enkripsi dengan mengombinasikan dua algoritma simetris yang dipilih dari hasil studi literatur. Perancangan juga mencakup desain database yang aman dengan field khusus untuk data terenkripsi. Selain itu, peneliti menyusun user interface sederhana untuk mendukung interaksi guru dan admin. Tahapan ini bertujuan agar sistem dapat digunakan secara praktis namun tetap menjaga keamanan. Pada tahap ini pula, disusun protokol pengelolaan kunci agar distribusi kunci aman. Perancangan dilakukan menggunakan metode UML untuk menggambarkan alur sistem. Hasil tahap ini adalah blueprint sistem yang siap diimplementasikan.

2.1.4 Implementasi Sistem

Tahap implementasi dilakukan dengan membangun aplikasi pengolahan nilai siswa berbasis kriptografi. Peneliti mengimplementasikan algoritma super enkripsi ke dalam kode program menggunakan bahasa pemrograman yang sesuai, misalnya Python atau Java. Database dibangun menggunakan sistem manajemen database seperti MySQL

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

dengan dukungan field terenkripsi. Proses implementasi mencakup pengembangan modul enkripsi, dekripsi, login multi-user, dan manajemen nilai siswa. Aplikasi diuji secara lokal untuk memastikan bahwa fungsi enkripsi berjalan sesuai desain. Selain itu, peneliti juga memastikan efisiensi sistem dengan mengukur waktu proses enkripsi dan dekripsi. Implementasi dilakukan secara iteratif agar kesalahan dapat diperbaiki dengan cepat. Tahapan ini menghasilkan aplikasi prototipe yang dapat digunakan sekolah untuk mengelola data nilai siswa. Prototipe ini sekaligus menjadi objek uji coba pada tahap berikutnya.

2.1.5 Pengujian dan Evaluasi

Tahap pengujian dilakukan untuk memastikan aplikasi berjalan sesuai dengan tujuan penelitian. Pengujian mencakup uji fungsionalitas untuk mengecek apakah enkripsi dan dekripsi berhasil dilakukan dengan benar. Peneliti juga melakukan uji performa untuk menilai kecepatan proses enkripsi pada data berukuran besar. Selain itu, dilakukan uji keamanan untuk menilai apakah data terenkripsi dapat diproteksi dari serangan sederhana. Evaluasi dilakukan dengan membandingkan hasil sistem baru dengan metode penyimpanan manual sebelumnya. Guru dan admin sekolah juga dilibatkan untuk memberikan umpan balik terhadap kemudahan penggunaan sistem. Hasil pengujian ini dianalisis untuk mengetahui kelebihan dan kelemahan sistem. Jika ditemukan masalah, peneliti melakukan perbaikan pada kode program. Tahapan ini penting untuk memastikan bahwa aplikasi benar-benar layak digunakan.

2.1.6 Dokumentasi dan Penyusunan Laporan

Tahap akhir adalah dokumentasi seluruh hasil penelitian dalam bentuk laporan. Dokumentasi mencakup penjelasan teori, metodologi, hasil implementasi, dan evaluasi sistem. Laporan disusun sesuai format penulisan ilmiah agar dapat dipublikasikan. Selain itu, peneliti menambahkan analisis perbandingan dengan penelitian terdahulu untuk menegaskan kontribusi penelitian ini. Dokumentasi juga mencakup manual penggunaan sistem bagi sekolah yang akan menerapkannya. Dengan adanya dokumentasi, penelitian ini dapat dijadikan rujukan bagi penelitian lanjutan. Penyusunan laporan juga memuat keterbatasan penelitian yang dapat menjadi bahan evaluasi. Tahap ini menegaskan capaian penelitian sekaligus kontribusinya pada bidang keamanan data akademik. Hasil akhir berupa laporan penelitian yang komprehensif dan siap dipresentasikan.

2.2 **Kriptografi**

Kriptografi secara teoritis merupakan ilmu dan seni untuk menjaga keamanan informasi melalui teknik transformasi data sehingga pesan asli (plaintext) diubah menjadi bentuk terenkripsi (ciphertext) yang tidak dapat dibaca tanpa kunci tertentu. Tujuan utama kriptografi adalah menjamin kerahasiaan (confidentiality), integritas (integrity), otentikasi (authentication), serta mencegah penyangkalan (non-repudiation) dalam pertukaran data digital [20][21]. Teori dasar kriptografi terbagi menjadi dua pendekatan utama, yaitu kriptografi simetris yang menggunakan satu kunci untuk enkripsi dan dekripsi, serta kriptografi asimetris yang menggunakan pasangan kunci publik dan privat [22]. Kriptografi simetris memiliki keunggulan dalam kecepatan pemrosesan data, namun memiliki kelemahan pada distribusi kunci yang rawan bocor[23][24]. Sebaliknya, kriptografi asimetris lebih aman dalam distribusi kunci, tetapi membutuhkan waktu pemrosesan yang lebih lama, sehingga tidak efisien untuk data berukuran besar[25]. Perkembangan teori kriptografi modern juga telah melibatkan penggunaan metode hibrida, yakni menggabungkan kriptografi simetris dan asimetris untuk menyeimbangkan antara keamanan dan kecepatan. Lebih jauh, konsep dasar kriptografi tidak hanya terbatas pada enkripsi teks, tetapi juga dapat diterapkan pada file digital, database, serta komunikasi jaringan untuk melindungi data dari penyadapan dan manipulasi[26]. Secara matematis, kriptografi menggunakan operasi kompleks seperti permutasi, substitusi, serta fungsi hash untuk memperkuat keamanan pesan[27]. Teori kriptografi juga terus berkembang seiring munculnya ancaman baru seperti serangan brute force, side-channel attack, dan quantum attack yang menuntut algoritma lebih adaptif dan kuat. Oleh karena itu, pemahaman teoritis kriptografi menjadi fondasi penting dalam pengembangan aplikasi keamanan data modern, termasuk dalam pengelolaan data akademik yang sangat sensitif[28].

2.3 Metode Super Enkripsi

Super Enkripsi merupakan salah satu kriptografi berbasis karakter yang menggabungkan dua buah cipher. Hal tersebut bertujuan untuk mendapatkan cipher yang lebih kuat sehingga tidak mudah untuk dipecahkan, dan juga untuk mengatasi penggunaan cipher tunggal yang secara komparatif lemah. Pada penelitian ini digunakan *Vigenere cipher* dan Playfair cipher dengan proses enkripsi dan deskripsi dilakukan degan cara satu kali proses untuk masing-masing cipher[29][30].

2.4 Algortima Vigenere Cipher

Vigenere cipher adalah algoritma substitusi jamak (*polyalphabetical substitution cipher*) dimana suatu huruf plainteks tidak selalu disubstitusi menjadi huruf yang sama, namun disubstitusi berdasarkan kunci yang digunakan[31][32].

Kekuatan algoritma *Vigenere chipper* ini adalah dapat mencegah frekuensi huruf-huruf didalam chiperteks yang memiliki pola tertentu yang sama, seperti yang terjadi pada chiper abjad-tunggal. Secara matematis, misalkan

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

kunci K dengan panjang m adalah rangkaian huruf-huruf K = k1 … km dimana ki didapat dari banyak penggeseran pada alfabet ke-i, plainteks adalah rangkaian p1, p2, …, pm, dan cipherteks adalah rangkaian c1, c2, …, cm. Misalkan m menentukan beberapa nilai integer positive. Diberikan P= C= K= (Z26). Untuk sebuah kunci K= (k1, k2, …, km), kita definisikan[33][34]:

$$eK(c1, \dots, cm) = (p1 + k1, \dots, pm + km)\ mod\ 26 \quad (1)$$

$$dK(p1, \dots, pm) = (c1 - k1, \dots, cm - km)\ mod\ 26 \quad (2)$$

Dimana semua operasi adalah berbasis pada Z26. Pengembangan dari metode Vigenere Cipher untuk penyandian citra dilakukan menggunakan formula Vigenere Cipher dengan menggunakan nilai basis modulo 256 sesuai dengan intensitas warna pada citra[35]. Rumus enkripsi untuk menghitung nilai cipher image tiap piksel adalah sebagai berikut:

$$E_{ki}(a) = (a + ki) mod\ 256 \quad (3)$$

Dengan a merupakan Intensitas ke-i, j citra asli, dan ki merupakan kunci ke-i. Sedangkan rumus untuk mendapatkan kembali plainteks yang berupa citra tiap piksel yang telah terenkripsi adalah :

$$D_{ki}(a) = (a - ki) mod\ 256 \quad (4)$$

Dengan a merupakan Intensitas citra piksel ke-i, j yang terenkripsi dan kimerupakan kunci ke-i. *Vigenere cipher* ini masih dapat dipecahkan dengan metode exhaustive search apabila panjang kunci diketahui karena kunci berikutnya merupakan pengulangan dari kunci apabila panjang kunci tidak sama dengan panjang plainteksnya. Untuk mengatasi kelemahan ini, digunakan metode keystream generator untuk mengacak urutan kunci berikutnya agar kriptanalis kesulitan mendapatkan kuncinya. Rumus yang digunakan untuk membangkitkan kunci ke-i menggunakan keystream adalah[36]:

$$k_i = (k_{i-1} + k_{i-m}) mod\ 256 \quad (5)$$

3. HASIL DAN PEMBAHASAN

Dengan perkembangan teknologi yang semakin pesat, pemanfaatan internet dalam dunia pendidikan telah menjadi suatu keharusan yang tidak dapat dihindarkan. Internet memungkinkan siswa maupun guru mengakses informasi kapan saja dan di mana saja, termasuk dalam proses pengolahan data nilai siswa yang menjadi bagian vital dari kegiatan belajar mengajar (KBM). Nilai siswa tidak hanya berfungsi sebagai indikator prestasi akademik, tetapi juga sebagai bahan evaluasi bagi guru dan sekolah dalam meningkatkan kualitas pembelajaran. Oleh karena itu, sistem pengolahan nilai yang cepat, akurat, dan aman sangat dibutuhkan agar dapat mendukung kinerja administrasi akademik secara efektif. Pada penelitian ini, sistem pengolahan data nilai siswa di SMA Negeri 5 Medan masih dilakukan secara manual sehingga rentan terhadap kesalahan, keterlambatan, bahkan manipulasi data. Dengan memanfaatkan metode kriptografi super enkripsi, penelitian ini bertujuan untuk menghadirkan solusi berupa pengamanan nilai siswa sehingga hanya pihak berwenang yang dapat mengakses data.

Aplikasi pengolahan data nilai siswa yang dibangun menggunakan pendekatan multi-user diharapkan mampu mencegah akses tidak sah dari pihak lain. Hal ini penting karena dalam praktiknya, tidak semua guru memiliki kewenangan untuk mengakses nilai siswa selain kelas yang mereka ajar. Dengan adanya sistem yang dilengkapi super enkripsi, data yang tersimpan di database akan melalui proses enkripsi terlebih dahulu sebelum dapat diakses. Super enkripsi menggabungkan dua teknik dasar kriptografi, yaitu substitusi dan transposisi, sehingga tingkat keamanan data menjadi lebih kuat. Proses enkripsi dilakukan pada plaintext nilai siswa untuk menghasilkan ciphertext yang sulit dimengerti oleh pihak yang tidak memiliki kunci dekripsi. Dengan cara ini, potensi manipulasi nilai dapat ditekan seminimal mungkin, serta menjamin kerahasiaan informasi akademik siswa.

3.1 Penerapan Algoritma *Vigenere Cipher*

Pada tahap implementasi, algoritma Vigenere Cipher dipilih karena termasuk stream cipher simetris yang relatif sederhana namun cukup kuat dalam melindungi data teks. Plaintext yang digunakan dalam contoh adalah kata "NILAI SISWA" dengan kunci "JEFRY SARAGIH". Proses enkripsi dilakukan dengan formula dasar Ci = (Pi + Ki) mod 26, di mana Pi adalah nilai plaintext dan Ki adalah nilai kunci.

Sebelum dilakukan proses perhitungan, setiap huruf pada plaintext maupun kunci terlebih dahulu dikonversi ke bentuk angka. Konversi ini sangat penting karena operasi matematis dalam kriptografi tidak dilakukan langsung pada huruf, melainkan pada representasi numeriknya. Oleh karena itu, dibuat tabel substitusi huruf ke angka sebagaimana ditampilkan pada Tabel 1.

Tabel 1. Substitusi Huruf ke Angka

Huruf	Angka
A	
B	2

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

Huruf	Angka
C	3
D	4
E	5
F	6
G	7
H	8
I	9
J	10
K	11
L	12
M	13
N	14
O	15
P	16
Q	17
R	18
S	19
T	20
U	21
V	22
W	23
X	24
Y	25
Z	26

Tabel 1 di atas menunjukkan representasi huruf alfabet ke dalam bentuk angka, yang menjadi dasar perhitungan enkripsi dan dekripsi. Konversi ini penting karena semua operasi enkripsi dilakukan menggunakan bentuk numerik. Proses substitusi ini memungkinkan transformasi data menjadi lebih sistematis sehingga dapat diproses dengan formula matematis kriptografi.

Setelah proses konversi dilakukan, langkah berikutnya adalah melakukan enkripsi menggunakan formula yang telah ditentukan. Tabel 2 berikut menggambarkan detail proses enkripsi mulai dari plaintext, kunci, hasil perhitungan numerik, hingga ciphertext yang terbentuk.

Tabel 2. Proses Enkripsi Vigenere Cipher

Plaintext	14	9	12	1	9	19	9	19	23	1	14	9
Kunci	10	5	6	18	25	19	1	18	1	7	9	8
Hasil	**24**	**14**	**18**	**19**	**8**	**12**	**10**	**11**	**24**	**8**	**23**	**17**
Chipertext	W	N	R	S	H	L	J	K	X	H	W	Q

Berdasarkan Tabel 2, hasil enkripsi menunjukkan bahwa plaintext “NILAI SISWA” berhasil diubah menjadi ciphertext “WNRSHLJKXHWQ”. Perubahan huruf ini menunjukkan kekuatan Vigenere Cipher dalam menyamarkan data asli sehingga tidak dapat dikenali oleh pihak luar. Dengan panjang kunci yang sama atau lebih besar daripada plaintext, algoritma ini semakin sulit dipecahkan menggunakan metode brute force sederhana. Setelah dilakukan proses enkripsi, maka dilakukan pengembalian data asli menggunakan teknik dekripsi.

Proses dekripsi merupakan kebalikan dari enkripsi, di mana ciphertext dikembalikan menjadi plaintext dengan menggunakan kunci yang sama. Formula yang digunakan adalah Pi = (Ci – Ki) mod 26. Sebelum proses dilakukan, ciphertext juga dikonversi ke bentuk angka sehingga dapat diproses dengan metode yang sama. Tabel 3 berikut menunjukkan detail proses dekripsi mulai dari ciphertext, nilai kunci, hasil perhitungan, hingga plaintext yang diperoleh.

Tabel 3. Proses Dekripsi Vigenere Cipher

Chipertext	24	14	18	19	8	12	10	11	24	8	23	17
Kunci	10	5	6	18	25	19	1	18	1	7	9	8
Hasil	14	9	12	1	9	19	9	19	23	1	14	9
Plaintext	N	I	L	A	I	S	I	S	W	A	N	I

Proses dekripsi pada Tabel 3 berhasil mengembalikan ciphertext “WNRSHLJKXHWQ” menjadi plaintext “NILAI SISWA”. Hal ini membuktikan bahwa metode super enkripsi dengan Vigenere Cipher dapat menjaga integritas data. Ciphertext yang tampak acak dapat dikembalikan sepenuhnya menjadi teks asli dengan syarat kunci enkripsi diketahui. Dengan demikian, data nilai siswa yang dienkripsi pada sistem akan aman dari akses pihak yang tidak memiliki kunci.

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

3.2 Pembahasan

Hasil penelitian ini menunjukkan bahwa penerapan algoritma super enkripsi pada pengolahan data nilai siswa mampu menjamin keamanan dan kerahasiaan informasi. Enkripsi yang dilakukan menggunakan Vigenere Cipher berhasil mengubah plaintext menjadi ciphertext yang tidak bermakna bagi pihak luar. Proses dekripsi juga dapat dilakukan dengan akurat, sehingga menjamin integritas data tetap terjaga. Keunggulan metode ini adalah kesederhanaannya, namun memiliki kelemahan pada manajemen kunci jika digunakan dalam skala besar. Oleh karena itu, untuk implementasi jangka panjang, perlu dipertimbangkan penggabungan dengan algoritma lain seperti AES atau RSA agar lebih kuat menghadapi serangan kriptanalisis modern.

4. KESIMPULAN

Berdasarkan hasil penelitian yang dilakukan, dapat disimpulkan bahwa penerapan kriptografi dengan metode super enkripsi pada sistem pengolahan data nilai siswa di SMA Negeri 5 Medan mampu memberikan solusi efektif dalam menjaga keamanan, kerahasiaan, dan integritas data akademik. Proses enkripsi menggunakan algoritma Vigenere Cipher berhasil mengubah plaintext menjadi ciphertext yang sulit dipahami tanpa kunci, sedangkan proses dekripsi dapat mengembalikan ciphertext tersebut menjadi data asli secara akurat, sehingga menjamin keaslian informasi yang tersimpan dalam basis data. Dengan penerapan metode ini, potensi manipulasi nilai oleh pihak yang tidak berwenang dapat diminimalisasi, sekaligus meningkatkan kepercayaan pengguna terhadap sistem yang dibangun. Selain itu, penelitian ini juga membuktikan bahwa kriptografi simetris berbasis stream cipher dapat diterapkan dengan baik pada aplikasi pendidikan karena memiliki kecepatan pemrosesan yang tinggi serta kemudahan implementasi.

REFERENCES

[1] S. Chandra, S. Bhattacharyya, S. Paira, and S. Alam, “A study and analysis on symmetric cryptography,” in *2014 International Conference on Science Engineering and Management Research (ICSEMR)*, 2014, pp. 1–8. doi: 10.1109/ICSEMR.2014.7043664.

[2] J. Kapoor and D. Thakur, “Analysis of symmetric and asymmetric key algorithms,” in *ICT analysis and applications*, Springer, 2022, pp. 133–143. doi: https://doi.org/10.1007/978-981-16-5655-2_13.

[3] V. Rudnytskyi, O. Korchenko, N. Lada, R. Ziubina, L. Wieclaw, and L. Hamera, “Cryptographic encoding in modern symmetric and asymmetric encryption,” *Procedia Comput. Sci.*, vol. 207, pp. 54–63, 2022, doi: https://doi.org/10.1016/j.procs.2022.09.037.

[4] F. D. Yonathan, H. Nasution, and H. Priyanto, “Aplikasi Pengaman Dokumen Digital Menggunakan Algoritma Kriptografi Hybrid dan Algoritma Kompresi Huffman,” *JEPIN (Jurnal Edukasi dan Penelit. Inform.*, vol. 7, no. 2, pp. 181–195, 2021, doi: https://doi.org/10.26418/jp.v7i2.47077.

[5] H. Putri, L. Virna, T. Febrianti, and T. Sutabri, “Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA: Studi Kasus dan Analisis,” *J. Manaj. Inform. Teknol.*, vol. 5, no. 1, pp. 153–170, 2025, doi: https://doi.org/10.51903/rdbsne23.

[6] Z. Arif and A. Nurokhman, “Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi,” *J. Teknol. Sist. Inf.*, vol. 4, no. 2, pp. 394–405, 2023, doi: https://doi.org/10.35957/jtsi.v4i2.6077.

[7] S. K. Mousavi, A. Ghaffari, S. Besharat, and H. Afshari, “Security of internet of things based on cryptographic algorithms: a survey,” *Wirel. Networks*, vol. 27, no. 2, pp. 1515–1555, 2021, doi: https://doi.org/10.1007/s11276-020-02535-5.

[8] N. Febitri, H. Witriyono, M. Muntahanah, and M. Marhalim, “Application of AES 256 Cryptography Algorithm OCB Mode on Student Data,” *J. Komputer, Inf. dan Teknol.*, vol. 3, no. 2, pp. 423–432, 2023, doi: https://doi.org/10.53697/jkomitek.v3i2.1478.

[9] L. Judijanto, P. D. Persadha, I. Susilowati, H. K. Reza, and M. Susanti, “Analisis Keamanan Data dan Perlindungan Privasi dalam Pengelolaan Big Data: Tinjauan Teknologi Enkripsi dan Anonimisasi,” *J. Penelit. Inov.*, vol. 5, no. 2, pp. 991–1000, 2025, doi: https://doi.org/10.54082/jupin.1151.

[10] C. Kościelny, M. Kurkowski, and M. Srebrny, “Foundations of symmetric cryptography,” in *Modern Cryptography Primer: Theoretical Foundations and Practical Applications*, Springer, 2013, pp. 77–118. doi: https://doi.org/10.1007/978-3-642-41386-5_3.

[11] B. Mandal, S. Chandra, S. S. Alam, and S. S. Patra, “A comparative and analytical study on symmetric key cryptography,” in *2014 international conference on electronics, communication and computational engineering (ICECCE)*, IEEE, 2014, pp. 131–136. doi: 10.1109/ICECCE.2014.7086646.

[12] R. A. Manurung, S. Sutarman, and S. Efendi, “Comparative Analysis of the Performance of Four Symmetric Algorithms on Digital File Security,” *J. INFORMATICS Telecommun. Eng.*, vol. 8, no. 2, pp. 152–164, 2025, doi: 10.31289/jite.v8i2.13978.

[13] V. Kapoor and R. Gupta, “Hybrid symmetric cryptography approach for secure communication in web application,” *J. Discret. Math. Sci. Cryptogr.*, vol. 24, no. 5, pp. 1179–1187, 2021, doi:

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

https://doi.org/10.1080/09720529.2021.1936900.
[14] S. E. Noor, A. Ahmad, M. V. Martos Núñez, and M. J. Hornos Barranco, "Learning the basics of cryptography with practical examples," *REIDOCREA*, vol. 11, no. 24, pp. 274–281, 2022, doi: http://dx.doi.org/10.30827/Digibug.74740.
[15] A. Abuzaid, X. Yuan, H. Yu, and B. Chu, "The Design and Implementation of a Cryptographic Education Tool.," in *3rd International Conference on Computer Supported Education*, 2011, pp. 193–198. doi: 10.5220/0003301301930198.
[16] P. . Chakravarthy and T. Anjikumar, "A Novel Symmetric Key Cryptography using Multiple Random Secret Keys," *Int. J. Comput. Appl.*, vol. 80, no. 16, pp. 27–32, 2013, doi: 10.5120/13954-1890.
[17] M. B. Yassein, S. Aljawarneh, E. Qawasmeh, W. Mardini, and Y. Khamayseh, "Comprehensive study of symmetric key and asymmetric key encryption algorithms," in *2017 international conference on engineering and technology (ICET)*, IEEE, 2017, pp. 1–7. doi: 10.1109/ICEngTechnol.2017.8308215.
[18] A. S. Ellapalli and S. Varadarajan, "Information security with cryptography symmetric key encryption algorithms: a survey," *I-Manager's J. Commun. Eng. Syst.*, vol. 11, no. 1, p. 19, 2022, doi: 10.26634/jcs.11.1.18913.
[19] D. A. Meko, "Perbandingan Algoritma DES, AES, IDEA Dan Blowfish dalam Enkripsi dan Dekripsi Data," *J. Teknol. Terpadu*, vol. 4, no. 1, pp. 8–15, 2018, doi: https://doi.org/10.54914/jtt.v4i1.110.
[20] M. Abudalou, "Enhancing Data Security through Advanced Cryptographic Techniques," *Int. J. Comput. Sci. Mob. Comput.*, vol. 13, no. 1, pp. 88–92, 2024, doi: https://doi.org/10.47760/ijcsmc.2024.v13i01.007.
[21] S. Naeem, "Network security and cryptography challenges and trends on recent technologies," *J. Appl. Emerg. Sci.*, vol. 13, no. 1, pp. 1–8, 2023, doi: http://dx.doi.org/10.36785/jaes.131546.
[22] R. Hazra, P. Chatterjee, Y. Singh, G. Podder, and T. Das, "Data encryption and secure communication protocols," in *Strategies for E-Commerce Data Security: Cloud, Blockchain, AI, and Machine Learning*, IGI Global, 2024, pp. 546–570. doi: 10.4018/979-8-3693-6557-1.ch022.
[23] R. Banoth and R. Regar, "Asymmetric Key Cryptography," in *Classical and Modern Cryptography for Beginners*, Springer, 2023, pp. 109–165. doi: https://doi.org/10.1007/978-3-031-32959-3_4.
[24] M. S. Al-Batah, M. S. Alzboon, M. Alzyoud, and N. Al-Shanableh, "Enhancing image cryptography performance with block left rotation operations," *Appl. Comput. Intell. Soft Comput.*, vol. 2024, no. 1, pp. 1–19, 2024, doi: https://doi.org/10.1155/2024/3641927.
[25] C. Ubochi, B. Olaniyi, K. Ukagwu, and S. Nnamchi, "A comparative analysis of symmetric cryptographic algorithm as a data security tool: A survey," *NIPES-Journal Sci. Technol. Res.*, vol. 5, no. 3, pp. 144–168, 2023, doi: https://doi.org/10.5281/zenodo.8313097.
[26] A. Yeboah-Ofori, C. K. Agbodza, F. A. Opoku-Boateng, I. Darvishi, and F. Sbai, "Applied cryptography in network systems security for cyberattack prevention," in *2021 International Conference on Cyber Security and Internet of Things (ICSIoT)*, IEEE, 2021, pp. 43–48.
[27] S. Windarta, S. Suryadi, K. Ramli, B. Pranggono, and T. S. Gunawan, "Lightweight cryptographic hash functions: Design trends, comparative study, and future directions," *Ieee Access*, vol. 10, pp. 82272–82294, 2022, doi: https://doi.org/10.1109/ACCESS.2022.3195572.
[28] S. M. S. Eldin *et al.*, "Design and analysis of new version of cryptographic hash function based on improved chaotic maps with induced DNA sequences," *IEEE Access*, vol. 11, pp. 101694–101709, 2023, doi: https://doi.org/10.1109/ACCESS.2023.3298545.
[29] S. Bahri, F. Jihan, and B. Rudianto, "Implementasi Algoritma Super Enkripsi Vigenere Cipher Dan Route Cipher Pada Penyandian Pesan Teks," *J. Mat. UNAND*, vol. 12, no. 2, pp. 168–175, 2023, doi: https://doi.org/10.25077/jmua.12.2.168-175.2023.
[30] A. M. Supriyatno and E. Ardhianto, "Peningkatan Keamanan Pesan Teks Menggunakan Super Enkripsi Algoritma Caesar Cipher Standard Dan Vigenere Autokey," *J. Ilm. KOMPUTASI*, vol. 23, no. 2, pp. 167–172, 2024, doi: https://doi.org/10.32409/jikstik.23.2.3602.
[31] N. B. Putra, B. C. Andika, A. D. Purba, and M. Ridwan, "Implementasi Sandi Vigenere Cipher dalam Mengenkripsikan Pesan," *JOCITIS-Journal Sci. Infomatica Robot.*, vol. 1, no. 1, pp. 42–50, 2023, doi: https://jurnal.ittc.web.id/index.php/jct/article/view/25.
[32] I. Riadi, A. Fadlil, and F. A. Tsani, "Pengamanan citra digital berbasis kriptografi menggunakan algoritma Vigenere Cipher," *JISKA (Jurnal Inform. Sunan Kalijaga)*, vol. 7, no. 1, pp. 33–45, 2022, doi: https://doi.org/10.14421/jiska.2022.7.1.33-45.
[33] A. H. Hasugian, "Implementasi Algoritma Vigenere Cipher Untuk Keamanan Data Bantuan Sosial Di Desa," *Bull. Comput. Sci. Res.*, vol. 5, no. 4, pp. 317–328, 2025, doi: https://doi.org/10.47065/bulletincsr.v5i4.544.
[34] E. Irianti, D. F. Surianto, A. Z. Adistia, M. Juharman, and J. A. Safi'i, "Implementasi Kriptografi Vigenere Cipher untuk Keamanan Data Informasi Desa," *Progress. Information, Secur. Comput. Embed. Syst.*, vol. 1, no. 1, pp. 8–15, 2023, doi: https://doi.org/10.61255/pisces.v1i1.24.
[35] S. A. Zebua, "Modifikasi Algoritma Vigenere Cipher dengan Pembangkit Kunci Random Number Generator Dalam Pengamanan Citra Digital," *J. Comput. Informatics Res.*, vol. 1, no. 3, pp. 71–81, 2022, doi: https://doi.org/10.47065/comforch.v1i3.345.
[36] M. F. Siregar, A. H. Hasugian, and S. Suhardi, "Implementasi Kriptografi Kombinasi Algoritma Vigenere

ADA Journal of Information System Research
Volume 2, No 2, February 2025 Page: 77−85
ISSN 3025-9568 (media online)
DOI: doi.org/10.64366/adajisr.v2i2.78

Cipher Dan Reverse Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Pribadi Berbasis Android," *J. Sci. Soc. Res.*, vol. 7, no. 4, pp. 2121–2125, 2024, doi: https://doi.org/10.54314/jssr.v7i4.2359.