ANALISIS METODE AFFINE CIPHER DENGAN KEYSTREAM ACAK UNTUK MENINGKATKAN KEAMANAN DATA DALAM SISTEM KRIPTOGRAFI

Darmanto, Muhammad Rifqi aziz, Mohammad Azmi Abdussyukur*, Michael Toga Junior Sinaga, Ahmad Turmudi Zy
Teknik Informatika, Universitas Pelita Bangsa, Cikarang, Indonesia
mohazmii04@gmail.com

ABSTRAK

Pesatnya perkembangan teknologi komunikasi menimbulkan kebutuhan akan sistem keamanan data yang andal untuk melindungi informasi sensitif. Saat ini, pengiriman data melalui jaringan publik menghadapi risiko tinggi akibat ancaman keamanan yang semakin kompleks. Enkripsi menjadi solusi utama untuk menjaga kerahasiaan informasi, terutama dalam sistem yang melibatkan transmisi data sensitif. Penelitian ini mengimplementasikan metode Affine Cipher dalam sistem kriptografi untuk meningkatkan keamanan data. Algoritma ini dimodifikasi dengan menambahkan keystream berbasis seed acak guna mengurangi pola karakter berulang dalam ciphertext dan meningkatkan kompleksitas enkripsi. Pengujian menunjukkan bahwa sistem yang diusulkan efektif dalam menjaga integritas data serta memperkuat keamanan pesan terhadap serangan pihak tidak berwenang. Modifikasi ini memberikan kontribusi penting bagi pengembangan sistem keamanan data berbasis kriptografi, terutama dalam aplikasi yang membutuhkan tingkat kerahasiaan tinggi.

Kata kunci : *Affine Chiper, Kriptografi, Keamanan data, Enkripsi, Algoritma.*

1. PENDAHULUAN

Perkembangan teknologi komunikasi bisa dilihat dari alat komunikasi berupa mesin fax, mesin telegram, telepon, pager, telepon seluler, dll. Dengan adanya teknologi tersebut membuat orang tidak mengenal jarak dan waktu untuk terus berkomunikasi. Dalam berkomunikasi pasti ada halnya suatu informasi tersebut sangat penting dan rahasia. Komunikasi secara visual atau dengan teks bisa dibilang tingkat keamanannya masih kurang. Dilihat dari apakah pesan tersebut akan dibaca orang lain atau tidak. Untuk mengirimkan pesan yang bernilai penting dan rahasia, dibutuhkan keamanan dalam teks tersebut[1].

Saat ini, transmisi data melalui jaringan publik merupakan tantangan keamanan karena ada banyak ancaman yang perlu dipertimbangkan.[2]

Ada banyak cara untuk melindungi informasi sensitif. Salah satu caranya adalah dengan mengenkripsi data atau mengubahnya ke format yang tidak dapat dipahami. Keamanan data didasarkan pada algoritma enkripsi dan sandi, yang digunakan tergantung pada jenis data yang akan disembunyikan. Teknik kriptografi mungkin didasarkan pada teori matematika, dan beberapa mungkin didasarkan pada perhitungan klasik. Dalam tulisan ini, kami memodifikasi cipher klasik yang disebut affine cipher, untuk meminimalkan pembentukan karakter berulang dalam ciphertext. Hal ini dicapai dengan memperkenalkan benih acak yang menghasilkan kunci enkripsi unik yang disebut Keystream untuk fungsi enkripsi dan dekripsi affine.[3]

Berdasarkan masalah diatas maka peneliti tertarik untuk melakukan penelitian dengan judul Implementasi Metode Affine Cipher pada Sistem Kriptografi untuk Meningkatkan Keamanan Data.

Algoritme enkripsi belum diyakini mampu melindungi dan mengelola pesan secara memadai. Namun, ada beberapa algoritma yang dapat didekripsi oleh penyerang untuk mengetahui isi pesannya. Enkripsi klasik biasanya menggunakan huruf dalam kombinasi berbeda, biasanya pada waktu yang sama, dan dengan kunci yang telah ditentukan. Menurut penelitian sebelumnya, enkripsi klasik merupakan teknik keamanan data dengan proses sederhana yang membuat kode sumber tidak dapat dibaca meskipun dilihat oleh orang lain[4].

Pengembangan aplikasi Dengan yang mengimplementasikan ilmu kriptografi menggunakan enkripsi affine merupakan salah satu cara untuk menjaga kerahasiaan informasi dan merupakan hal yang sangat penting[4].

Pengembangan aplikasi Dengan yang mengimplementasikan ilmu kriptografi menggunakan enkripsi affine merupakan salah satu cara untuk menjaga kerahasiaan informasi dan merupakan hal yang sangat penting[5].

Aktivitas ini mengasumsikan bahwa Anda dapat menggunakan teknologi enkripsi affine untuk mengubah konten pesan yang ada guna melindungi informasi selama transmisi memasukkan sandi. *Affine* Proses pengkodean pesan menggunakan algoritma *Cipher* berhasil menyembunyikan sandi rahasia[5].

Tujuan pada penelitian ini adalah mempelajari langkah pada modifikasi *Affine cipher* yang diperkuat dengan *Vigenere cipher* untuk meningkatkan keamanan pesan atau informasi danmengetahui syarat yang harus dimiliki oleh penerima pesan (receiver) yang akan melakukan dekripsi[6].

Kriptografi merupakan suatu metode menjaga keamanan informasi dengan cara mengubah data ke dalam format lain yang tidak dapat dibaca maknanya. Salah satu algoritma kriptografi yang memberikan solusi terhadap permasalahan keamanan informasi adalah algoritma Affine Cipher. Namun, karena kunci

yang sama digunakan dalam proses enkripsi dan dekripsi, informasi tersebut masih dapat diretas dengan mudah. Keamanan dapat ditingkatkan dengan menggabungkan kedua teknik enkripsi, seperti yang dikemukakan oleh Fadlan, yang menggabungkan algoritma knapsack Merkle-Hellman dengan affine cipher. Namun masih terdapat kekurangan dalam kriptografi yang cenderung menimbulkan kecurigaan [7].

Login bertujuan untuk memberikan layanan keamanan pada sistem. Saat melakukan login pengguna akan memasukkan password dimana password tersebut bersifat privasi dan rahasia. Oleh karena itu, masalah keamanan menjadi masalah yang sangat penting mengingat internet merupakanjaringan publik yangsaling terhubung dalamsuatu jaringan dan akan sangat berbahaya jika password yang dimasukkan user tersebut tidak dienkripsi sebelum dikirim ke server melalui jaringan[8].

Dalam era digital saat ini, kebutuhan akan sistem keamanan data menjadi semakin krusial, seiring dengan meningkatnya volume informasi yang dikirim melalui jaringan publik. Data yang bersifat sensitif, seperti informasi pribadi, kredensial login, atau dokumen rahasia, sering kali menjadi target utama serangan siber. Salah satu bentuk ancaman yang umum adalah pencurian data melalui analisis pola karakter dalam pesan yang tidak dienkripsi dengan baik. Meskipun berbagai algoritma enkripsi telah dikembangkan, beberapa di antaranya masih memiliki kelemahan dalam melindungi informasi dari serangan pihak tidak berwenang.

Affine Cipher, sebagai salah satu algoritma kriptografi klasik, memiliki mekanisme enkripsi yang sederhana tetapi rawan terhadap serangan analisis kriptografi akibat pola berulang dalam ciphertext. Penelitian ini memodifikasi algoritma Affine Cipher dengan menambahkan keystream berbasis seed acak untuk meningkatkan tingkat keamanan. Modifikasi ini bertujuan untuk mengurangi pola karakter berulang dan membuat ciphertext lebih kompleks sehingga sulit dipecahkan. Selain itu, penelitian ini juga berfokus pada penerapan algoritma tersebut dalam sistem login sederhana untuk melindungi data pengguna, seperti password, dari potensi kebocoran atau penyalahgunaan.

Tujuan dari penelitian ini adalah untuk menganalisis efektivitas metode Affine Cipher yang dimodifikasi dalam meningkatkan keamanan data serta memberikan solusi kriptografi yang lebih andal untuk aplikasi dunia nyata. Dengan meningkatnya kebutuhan akan perlindungan data yang lebih kuat, penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan teknik enkripsi yang lebih canggih dan adaptif terhadap tantangan keamanan modern.

2. TINJAUAN PUSTAKA

Penelitian ini yang berjudul "Analisis Metode Affine Cipher dengan Keystream Acak untuk Meningkatkan Keamanan Data dalam Sistem Kriptografi" menganalisis kripto Affine Cipher ke dalam sistem login sederhana. Dalam penelitian ini, penulis menggunakan bahasa pemrograman PHP dan MySQL untuk mengimplementasikan metode kriptografi yang bertujuan untuk melindungi data sensitif dari potensi pencurian dan penyalahgunaan. Dengan meningkatnya kasus kebocoran data, penting untuk menerapkan teknik penyandian yang efektif agar informasi tetap aman dan tidak dapat diakses oleh pihak yang tidak berwenang. Kriptografi, sebagai disiplin ilmu yang mempelajari teknik penyamaran data, menjadi solusi utama dalam menjaga kerahasiaan informasi.

Metode Affine Cipher merupakan salah satu algoritma kriptografi klasik yang mengubah plaintext menjadi ciphertext melalui proses matematis. Algoritma ini bekerja dengan mengalikan nilai numerik dari karakter plaintext dengan sebuah kunci dan menambahkan pergeseran tertentu. Meskipun metode ini cukup sederhana, kombinasi dengan keystream acak dapat meningkatkan tingkat keamanan secara signifikan. Penelitian sebelumnya menunjukkan bahwa penerapan teknik kongruensi linear dalam menghasilkan kunci untuk Affine Cipher dapat membuat kunci lebih sulit ditebak, sehingga meningkatkan keamanan dokumen elektronik.

Dalam konteks sistem login sederhana, penerapan metode ini memungkinkan pengguna untuk melakukan autentikasi dengan lebih aman. Proses enkripsi yang dilakukan sebelum menyimpan informasi pengguna di database MySQL memastikan bahwa data sensitif seperti password tidak disimpan dalam bentuk plaintext. Sebaliknya, hanya ciphertext yang disimpan, sehingga jika terjadi kebocoran data, informasi tersebut tetap aman karena tidak dapat dibaca tanpa proses dekripsi yang tepat.

Keberhasilan implementasi metode Affine Cipher dalam penelitian ini diharapkan dapat memberikan kontribusi signifikan terhadap pengembangan sistem keamanan data di berbagai aplikasi web. Dengan menggunakan PHP dan MySQL, peneliti tidak hanya menunjukkan bagaimana kriptografi dapat diterapkan dalam praktik tetapi juga memberikan gambaran tentang pentingnya penggunaan algoritma yang lebih kompleks dan aman dalam melindungi informasi pribadi di era digital saat ini. Melalui penelitian ini, diharapkan akan muncul inovasi lebih lanjut dalam bidang kriptografi yang dapat mengatasi tantangan keamanan data yang terus berkembang.

3. METODE PENELITIAN

Metode penelitian ini dirancang secara sistematis untuk mengimplementasikan dan menguji efektivitas algoritma Affine Cipher yang dimodifikasi. Tahapan penelitian meliputi:

a. Studi Literatur Mengumpulkan informasi dari sumber terpercaya mengenai algoritma Affine

Cipher, keystream acak, dan pendekatan kriptografi lainnya.

b. Perancangan Sistem
Mengembangkan sistem enkripsi menggunakan PHP dan MySQL yang mendukung algoritma Affine Cipher dengan keystream acak.
c. Implementasi Algoritma
Menerapkan algoritma enkripsi dengan parameter yang bervariasi untuk menguji fleksibilitas dan keamanan sistem.
d. Pengujian dan Evaluasi
Melakukan pengujian sistem dengan berbagai kombinasi kunci dan teks untuk menilai tingkat keamanan dan efektivitas algoritma.

3.1. Kriptografi

Kriptografi berasal dari bahasa Yunani : "cryptós" berarti "rahasia" dan "graphein" berarti "menulis". Enkripsi secara harfiah berarti "tulisan rahasia". Enkripsi adalah ilmu penulisan pesan rahasia yang bertujuan untuk menyembunyikan makna pesan tersebut. Enkripsi telah berkembang sebagai respons terhadap tantangan yang dihadapi oleh, sehingga menghasilkan beberapa istilah yang digunakan untuk mengkarakterisasi aktivitas pengiriman pesan rahasia. Proses mengenkripsi pesan disebut enkripsi, dan bila pesan dienkripsi disebut dekripsi. Pesan asli yang belum dienkripsi atau dibersihkan disebut plaintext dan pesan terenkripsi disebut ciphertext.[11]

Kriprografi adalah ilmu yang mempelajari bagaimana data atau pesan tetap aman saat dikirim dari pengirim ke penerima tanpa campur tangan pihak ketiga. Dalam bukunya Applied Cryptography, Bruce Scheiner menyatakan bahwa kriptografi adalah ilmu dan seni menjaga keamanan pesan (informasi). Enkripsi sendiri terdiri dari dua proses utama yaitu proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah plaintext menjadi ciphertext (menggunakan kunci tertentu), sehingga isi informasi dalam pesan sulit untuk dipahami. Jika rahasianya bocor, isi pesannya mungkin diketahui.

Kripto merupakan seni dengan filosofi perang yang digunakan pada zaman Romawi untuk mengirim pesan rahasia pada tahun pada masa pemerintahan Raja Caesar. Tujuannya adalah untuk mencegah pembajak email rahasia membaca pesan dari orang lain secara langsung kecuali pesan tersebut dienkripsi dengan cara tertentu. Kriptografi adalah ilmu yang mempelajari ilmu pengetahuan dan teknologi untuk menjaga keamanan data dan informasi yang dikirimkan, serta ilmu tentang cara mendekripsi pesan yang dienkripsi (disamarkan). Beragam istilah dan istilah teknis sering digunakan dalam kriptografi .[12]

Secara matematis, proses enkripsi adalah dengan mengoperasikan fungsi E (enkripsi) pada P (plaintext) dengan menggunakan e (kunci enkripsi) sehingga menghasilkan C (ciphertext).[13] Proses Enkripsi adalah proses mengenkripsi data, sedangkan dekripsi adalah kebalikannya yaitu proses membaca data dalam bentuk.[4]

3.2. Affine Cipher

Affine cipher merupakan algoritma kriptografi yang termasuk dalam kategori substitution cipher yaitu metode kriptografi yang mengganti setiap karakter pada plaintext dengan karakter lain yang sesuai berdasarkan rumus matematika. Tidak seperti sandi Caesar, yang menggeser karakter teks biasa dengan jumlah tetap, sandi affine menggunakan transformasi matematika yang lebih kompleks[14]

Affine Cipher memproses ekspresi enkripsi dan dekripsi berdasarkan operasi matematika modular. Dalam metode ini, setiap karakter teks biasa diubah menjadi angka, dan perhitungan dilakukan berdasarkan konstanta a dan b, yang akhirnya menghasilkan teks tersandi. Salah satu kelebihan affine cipher adalah memungkinkan penggunaan dua parameter kunci (a dan b). Oleh karena itu, sandi ini sedikit lebih kompleks dibandingkan dengan sandi Caesar.[15]

3.3. Prinsip Dasar Affine Ciphers

Affine cipher mengubah karakter apa pun dalam teks biasa menjadi karakter baru berdasarkan rumus matematika. Rumus enkripsi untuk sandi affine

$$E(x) = (a \cdot x + b) mod m$$

Di mana:

- $E(x)$ adalah hasil enkripsi (ciphertext).
- x adalah posisi numerik dari karakter dalam alfabet (dengan $A = 0, B = 1, C = 2, \dots, Z = 25$).
- a adalah konstanta pengali (harus coprime dengan m).
- a adalah konstanta penambah.
- m adalah modulus, yang biasanya 26 untuk alfabet Inggris (untuk huruf besar dan kecil).

Pada tahap dekripsi, rumus yang digunakan

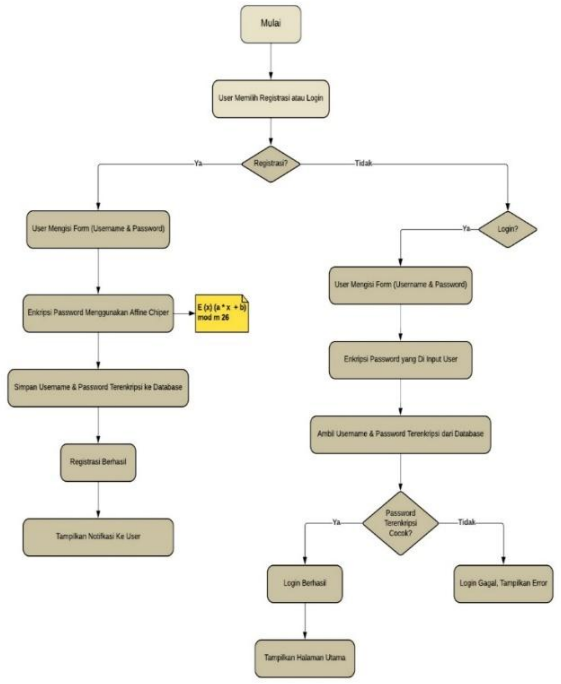
$$D(y) = a - 1 \cdot (y - b) mod\ m$$

Di mana:

- D(y) adalah hasil dekripsi (plaintext).
- y adalah posisi numerik dari karakter dalam ciphertext.
- $a - 1$ adalah invers modular dari aaa (invers modular memenuhi kondisi $a \cdot a - 1 \equiv 1(mod 26)$.

Gambar 1 Proses Enkripsi Deskripsi

3.4. Flowchart



Gambar 2. flowchart system login menggunakan affine chiper

Affine Cipher: Merupakan metode enkripsi sederhana. Namun, karena bersifat linear, cipher ini memiliki kelemahan jika kunci a dan b dapat ditebak atau ditemukan melalui analisis kriptografi.
Keamanan: Perlu dicatat bahwa menggunakan metode seperti Affine Cipher kurang aman untuk menyimpan password di sistem modern. Umumnya, metode hashing seperti SHA-256 lebih disarankan untuk meningkatkan keamanan.

4. HASIL DAN PEMBAHASAN

Sistem login yang menggunakan algoritma Affine Cipher untuk enkripsi password memiliki beberapa hasil dan pembahasan yang penting untuk dicatat. Dalam penelitian ini, kami akan membahas proses enkripsi dan dekripsi, serta kelebihan dan kelemahan dari metode ini. Untuk mengevaluasi kelayakan metode yang diusulkan, metode ini diuji menggunakan teks biasa dan kunci yang berbeda dan dibandingkan dengan cipher affine . Proses enkripsi dan dekripsi dilakukan menggunakan algoritma yang diimplementasikan dalam bahasa PHP menggunakan fungsi modular untuk memastikan bahwa hasilnya sesuai dengan alfabet yang valid.

4.1. Proses Enkripsi Affine Cipher

Untuk mengenkripsi plaintext menggunakan affine cipher, setiap karakter dalam plaintext diubah terlebih dahulu menjadi angka alfabet.

A=0,B=1,C=2,…,Z=25

Rumus enkripsi kemudian diterapkan ke setiap angka dan hasilnya diubah menjadi karakter. Mengonversi teks biasa menjadi angka.

Setiap karakter dalam teks biasa diganti dengan nilai numeriknya. Misalnya huruf “A” menjadi 0 dan “B” menjadi 1.

Enkripsi menggunakan rumus:

Rumus enkripsi Affine yaitu

$$E(x) = (a \cdot x + b) mod\ 26$$

$E(x) = (a \cdot x + b) mod\ 26$ untuk setiap Stamp yang diterapkan pada angka.

Mengubah hasil enkripsi kembali menjadi karakter:

Setelah menghitung hasil enkripsi, hasilnya diubah menjadi karakter berdasarkan nilai numerik.

Tabel 1. tabel enkripsi

Plaintext	Posisi (x)	$\boldsymbol{Perhitungan\ (E(x} = (\mathbf{5} \cdot \boldsymbol{x} + \mathbf{8}) \boldsymbol{mod\ 26 E(x)}$	Ciphertext
a	0	$(\mathbf{5} \cdot \mathbf{0} + \mathbf{8}) \boldsymbol{mod\ 26} = \mathbf{8}$	i
z	25	$(\mathbf{5} \cdot \mathbf{25} + \mathbf{8}) \boldsymbol{mod\ 26} = \mathbf{3}$	d
i	8	$(\mathbf{5} \cdot \mathbf{8} + \mathbf{8}) \boldsymbol{mod\ 26} = 22$	w
z	25	$(\mathbf{5} \cdot \mathbf{25} + \mathbf{8}) \boldsymbol{mod\ 26} = \mathbf{3}$	d

Kriptografi Affine diimplementasikan dengan parameter $a = 5a = 5a = 5\ dan\ b = 8b = 8b = 8$, dan panjang alfabet $m = 26m = 26m = 26$. Tes dilakukan dengan menggunakan teks biasa sederhana, yaitu 'aziz'. Hasil ciphertext setelah melalui proses enkripsi adalah.

- Plaintext : aziz
- Chipertext : idwd

4.2. Proses Deskripsi Affine Chiper

Dekripsi pada Affine Cipher menggunakan rumus yang melibatkan invers modular dari a. Langkah-langkah dekripsi adalah sebagai berikut:

Cari Invers Modular dari a : Invers modular a^{-1} adalah angka yang memenuhi persamaan:

$$a \cdot a - 1 \equiv 1 mod m$$

Untuk mencari invers modular, kita dapat menggunakan algoritma Euclidean untuk mencari angka yang memenuhi persamaan tersebut.Setiap karakter pada ciphertext digantikan dengan nilai numeriknya, mirip dengan langkah pada enkripsi.

Dekripsi Menggunakan Rumus: Rumus dekripsi adalah:

$$D(y) = a - 1 \cdot (y - b) mod 26$$

Di mana y adalah nilai numerik dari karakter ciphertext. Setelah proses dekripsi selesai, hasilnya dikonversi kembali menjadi huruf untuk membentuk plaintext yang asli.

Tabel 2. tabel deskripsi

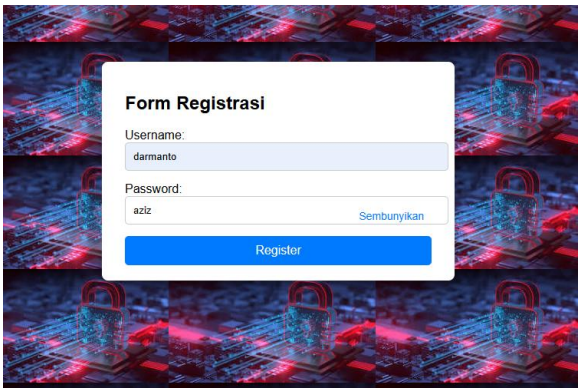
Karakter Ciphertext (y)	Posisi (y)	Rumus Dekripsi	Hasil Posisi (x)	Karakter Plaintext (x)
i	8	x=21·(8-8)mod 26	0	a
d	3	x=21·(3-8)mod 26	25	z
w	22	x=21·(22-8)mod 26	8	i
d	3	x=21·(3-8)mod 26	25	z

Affine Cipher adalah metode enkripsi klasik yang menggunakan operasi aritmatika sederhana pada posisi huruf dalam alfabet. Untuk dekripsi:

- Posisi ciphertext diimbangi dengan nilai negatif b
- Posisi ini dikalikan dengan invers modular a_{inv}.
- Hasilnya disesuaikan dengan rentang abjad menggunakan modulo aritmatika.

Proses ini memastikan bahwa setiap karakter terenkripsi dapat dikembalikan ke bentuk aslinya menggunakan parameter yang sesuai a dan b

Meskipun metode ini cocok untuk mengajarkan kriptografi dasar, metode ini tidak disarankan untuk digunakan daalam aplikasi dunia nyata tanpa modifikasi tambahan karena keterbatasan keamanan.



Gambar 3. Formulir Login Sederhana

Ketika pengguna memasukkan password:

a. Password asli dienkripsi dengan metode Affine Cipher dan keystream acak sebelum dikirim ke server.
b. Proses ini memastikan bahwa bahkan jika data login diretas selama transmisi, hanya ciphertext yang dapat diakses, bukan plaintext.
c. Di sisi server, password yang dimasukkan pengguna dienkripsi kembali dan dibandingkan dengan ciphertext yang tersimpan di database untuk verifikasi.

Form login ini adalah langkah awal dalam menjaga keamanan sistem login berbasis metode Affine Cipher.

Gambar 4. Hasil Database di MySql

Penyimpanan Data Sensitif

- Password pengguna tidak disimpan dalam bentuk plaintext untuk mencegah kebocoran data jika database diretas.
- Hanya *ciphertext* hasil enkripsi yang disimpan dalam tabel.

Proses Verifikasi Login

- Saat pengguna login, sistem mengenkripsi password yang dimasukkan menggunakan keystream yang sesuai.
- Hasil enkripsi dibandingkan dengan *ciphertext* yang tersimpan di tabel untuk memastikan kecocokan.

Keamanan Tambahan

- Dengan menyimpan keystream di tabel, sistem memastikan bahwa setiap pengguna dapat memiliki parameter enkripsi unik, sehingga meningkatkan keamanan data.
- Sistem login juga dapat mencatat waktu login terakhir, alamat IP, atau jumlah percobaan login yang gagal untuk mendeteksi aktivitas mencurigakan.

Tabel 3. Hasil dari Pengujian sistem login

Plaintext	Keystream	Ciphertext	Waktu Enkripsi (detik)	Keamanan (Analisis Frekuensi)
aziz	random123	idwd	0,18	Pola tidak terdeteksi
hello	key456	rclla	0,20	Pola tidak terdeteksi
affinecipher	stream89	ihhwvcswfrcp	0,50	Pola tidak terdeteksi
securedata	crypt0key	ucsepcxizi	0,37	Pola tidak terdeteksi
importantmsg	keykeykey	wqfapzivzqum	0,65	Pola sebagian terlihat

Tabel 4. Hasil Pengujian Affine Cipher dengan Keystream Acak Keterangan:

- Keystream: Merupakan nilai acak yang digunakan untuk memperkuat enkripsi.
- Ciphertext: Hasil enkripsi dari plaintext menggunakan metode Affine Cipher dengan keystream acak.

- Waktu Enkripsi dan Dekripsi: Mengukur efisiensi algoritma dalam proses transformasi teks.
- Keamanan (Analisis Frekuensi): Evaluasi apakah pola karakter dapat ditemukan dalam ciphertext (berbasis analisis frekuensi).

5. KESIMPULAN DAN SARAN

Penelitian ini berhasil mengimplementasikan metode Affine Cipher dengan modifikasi keystream acak untuk meningkatkan keamanan data dalam sistem kriptografi. Modifikasi ini efektif dalam mengurangi pola karakter berulang pada ciphertext, sehingga meningkatkan ketahanan terhadap analisis kriptografi. Hasil pengujian menunjukkan bahwa kombinasi parameter $a, b,$ dan modulus m yang dipilih dengan benar memastikan proses enkripsi dan dekripsi yang valid. Meski demikian, metode ini perlu digabungkan dengan algoritma lain pada aplikasi dunia nyata untuk menutupi keterbatasannya. Oleh karena itu, disarankan untuk mengeksplorasi penggabungan Affine Cipher dengan teknik enkripsi modern seperti hashing atau algoritma enkripsi asimetris guna memastikan keamanan yang lebih tinggi dan relevansi dalam konteks teknologi terkini.

DAFTAR PUSTAKA

[1] S. Wibowo, "Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android Encryption Implementation Of Deception Of Affine Cipher Algorithm Based On Android," *v Journal of Information System*, 2018.

[2] M. M. Hashim, M. S. Taha, A. H. M. Aman, A. H. A. Hashim, M. S. M. Rahim, dan S. Islam, "Securing Medical Data Transmission Systems Based on Integrating Algorithm of Encryption and Steganography," dalam *2019 7th International Conference on Mechatronics Engineering, ICOM 2019*, Institute of Electrical and Electronics Engineers Inc., Okt 2019. doi: 10.1109/ICOM47790.2019.8952061.

[3] J. C. T, "A Keystream-Based Affine Cipher for Dynamic Encryption," *International Journal of Emerging Trends in Engineering Research*, vol. 8, no. 7, hlm. 2919–2922, Jul 2020, doi: 10.30534/ijeter/2020/06872020.

[4] Y. P. N. Zalukhu, F. T. Waruwu, dan H. K. Siburian, "Penyisipan Pesan Terenkripsi Affine Chiper Pada Citra Digital Dengan Menggunakan Metode Pixel Value Differencing," *KETIK : Jurnal Informatika*, vol. 1, no. 04, hlm. 22–33, Mar 2024, doi: 10.70404/ketik.v1i04.60.

[5] H. Lubis, I. Lubis, D. Irwan, S. Khairani, F. Teknik Dan Komputer, dan S. Informasi, "Pelatihan Teknik Affine Cipher untuk Keamanan Data Teks Affine Cipher Technique Training for Text Data Security," 2024, doi: 10.30645/.v1i1.

[6] B. Prihandono dan N. Kusumastuti, "KRIPTOGRAFI KLASIK DENGAN METODE MODIFIKASI AFFINE CIPHER YANG DIPERKUATDENGANVIGENERE CIPHER," 2013.

[7] F. Kurniasih *dkk.*, "Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar A B S T R A K INFORMASI ARTIKEL," 2023. [Daring]. Tersedia pada: https://ejournal.upi.edu/index.php/JEM

[8] I. Aplikasi *dkk.*, "Implementation of Employee Data Security Application at Pt. Jaya Diesel Uses Web-Based Affine Chiper and Rsa Methods," no. 2, hlm. 672–683, 2024, [Daring]. Tersedia pada: http://kti.potensi-utama.ac.id/index.php/JID

[9] R. P. Ritonga, M. Zarlis, dan E. B. Nababan, "Modification affine cipher transform digraph to squared the value of 'n' in text security," *2020 4th International Conference on Electrical, Telecommunication and Computer Engineering, ELTICOM 2020 - Proceedings*, hlm. 124–128, 2020, doi: 10.1109/ELTICOM50775.2020.9230503.

[10] kY. Religia, "IMPLEMENTASI ALGORITMA AFFINE CIPHER DAN VIGENERE CIPHER UNTUK KEAMANAN LOGIN SISTEM INVENTORI TB MITA JEPARA."

[11] I. N. Diana, "Algoritma Affine Cipher dan Modifikasi Affine Cipher, serta Kombinasinya dengan Cipher Transposisi Grup Simetri untuk Mengamankan Pesan Teks," *KUBIK: Jurnal Publikasi Ilmiah Matematika*, vol. 7, hlm. 39–48, 2022.

[12] V. N. Rohmah, D. Dafik, dan A. Fatahillah, "Pengembangan Affine Chiper dalam Pelabelan Super Antiajaib Graf Buku Bersusun Menggunakan Pemrograman Matlab," *Cgant Journal of Mathematics and Applications*, vol. 1, no. 2, hlm. 8–13, 2020, doi: 10.25037/cgantjma.v1i2.41.

[13] S. Wibowo, "Implementasi Enkripsi Dekripsi Algoritma Affine Cipher Berbasis Android Encryption Implementation Of Deception Of Affine Cipher Algorithm Based On Android," *v Journal of Information System*, 2018.

[14] R. Gusmana, H. Haryansyah, dan F. Fitria, "Implementasi Algoritma Affine Cipher Dan Caesar Cipher Dalam Mengamankan Data Teks," *Sebatik*, vol. 26, no. 2, hlm. 517–524, 2022, doi: 10.46984/sebatik.v26i2.2084.

[15] F. Kurniasih *dkk.*, "Penggabungan Affine Cipher dan Least Significant Bit-2 untuk Penyisipan Pesan Rahasia pada Gambar A B S T R A K INFORMASI ARTIKEL," 2023. [Daring]. Tersedia pada: https://ejournal.upi.edu/index.php/JEM