KOMBINASI AUTOKEY CIPHER DAN TRANSPOSISI KOLOM DALAM MODEL SUPER ENKRIPSI

L. Budi Handoko[1], Chaerul Umam[2]

Universitas Dian Nuswantoro
Jl. Imam Bonjol No. 207, Semarang, Indonesia
[1]handoko@dsn.dinus.ac.id, [2]chaerul@dsn.dinus.ac.id

ABSTRAK

Kriptografi modern dibangun berdasarkan banyak konsep yang diperkenalkan dalam kriptografi klasik. Penelitian ini mengevaluasi efektivitas penggunaan metode Autokey Cipher dan Transformasi Kolom dalam melindungi keamanan data sensitive. Tranposisi kolom merupakan jenis trabnsposisi cipher yang mudah dan sederhana. Dengan menerapkan metode enkripsi Autokey Cipher menggunakan kunci 'FIKUNGGUL' dan transformasi kolom dengan kunci 'JAYA', teks asli 'UDINUSSMG' berhasil diubah menjadi teks sandi yang kompleks dan sulit diprediksi. Hasil penelitian menunjukkan bahwa penggunaan kedua teknik kriptografi ini secara signifikan meningkatkan tingkat keamanan data terhadap serangan brute force dan akses tidak sah. Proses enkripsi dan dekripsi yang kompleks dari kedua metode kriptografi tersebut berhasil mencegah penyerang untuk dengan mudah mendapatkan akses ke informasi yang dilindungi, serta memberikan lapisan keamanan tambahan yang efektif.
Kata Kunci: *Data Security, Autokey,* Transformasi Kolom, *Data Hiding*

ABSTRACT

Modern cryptography is built on many of the concepts introduced in classical cryptography. This research evaluates the effectiveness of using the Autokey Cipher and Column Transformation methods in protecting the security of sensitive data. Column transposition is an easy and simple type of cipher transposition. By applying the Autokey Cipher encryption method using the 'FIKUUNGGUL' key and column transformation with the 'JAYA' key, the original text 'UDINUSSMG' was successfully converted into a complex and difficult to predict cipher text. The research results show that the use of these two cryptographic techniques significantly increases the level of data security against brute force attacks and unauthorized access. The complex encryption and decryption processes of both cryptographic methods successfully prevent attackers from easily gaining access to protected information, as well as providing an effective additional layer of security.
Key Word: *Data Security, Autokey, Column Transform, Data Hiding*

PENDAHULUAN

Keamanan data dalam kriptografi adalah praktik dan studi tentang teknik-teknik yang digunakan untuk melindungi informasi dari akses yang tidak sah atau modifikasi, serta untuk memastikan kebenaran dan otentikasi data yang ditransmisikan (Ali et al., 2023; Wazid et al., 2022). Ini melibatkan penggunaan algoritma matematika, protokol keamanan, dan strategi lainnya untuk mengenkripsi data sehingga hanya pihak yang dituju yang dapat mengakses informasi yang dikirim (Lone et al., 2022). Tujuan utama dari kriptografi adalah untuk menjaga kerahasiaan, integritas, otentikasi, dan non-repudiasi data selama penyimpanan, pengiriman, dan pengolahan.

Sebuah isu di mana penyerang menggunakan metode brute force, keunggulan dari sistem super enkripsi yang melibatkan dua tahap enkripsi menjadi sangat signifikan. Dengan kemampuan untuk mengenkripsi data secara berulang menggunakan metode seperti *Autokey Cipher* dan Transposisi Kolom, sistem super enkripsi ini memperumit proses dekripsi bagi peretas dengan meningkatkan kompleksitas algoritma yang harus mereka pecahkan. Dengan melakukan dua tahap enkripsi, peretas tidak hanya dihadapkan pada tantangan untuk menemukan kunci yang tepat untuk satu metode, tetapi juga untuk mengidentifikasi urutan langkah enkripsi yang tepat. Hal ini menyulitkan upaya peretasan dengan brute force, karena waktu dan sumber daya yang diperlukan untuk menguji setiap kombinasi kunci secara signifikan meningkat. Dengan demikian, sistem super enkripsi ini memberikan perlindungan tambahan terhadap serangan brute force yang bertujuan untuk merusak keamanan data sensitif, mencegah penyerang untuk dengan mudah mendapatkan akses ke

p-ISSN:2527-5321
e-ISSN:2527-5941

informasi yang dilindungi (Jan et al., 2022; Lone et al., 2022).

Untuk mengatasi isu tersebut, salah satu penerapan keamanan data yaitu menerapkan model super enkripsi yang menggabungkan *Autokey Cipher* dan Transposisi Kolom. Dengan memanfaatkan *Autokey Cipher* yang menggunakan kunci rahasia yang terus berkembang seiring dengan teks terenkripsi, informasi rahasia dapat dijaga dengan ketat dari ancaman pihak yang tidak berwenang (Umam et al., 2022). Sementara itu, teknik Transposisi Kolom memungkinkan penataan ulang karakter-karakter dalam teks asli dengan menggunakan pola tertentu, menghasilkan hasil akhir yang sulit ditafsirkan tanpa pengetahuan tentang susunan yang benar. Gabungan kedua algoritma ini memberikan lapisan keamanan yang kuat, meminimalkan risiko kebocoran informasi sensitif serta upaya peretasan yang berpotensi merusak integritas data (Elkandoz & Alexan, 2022; Taha et al., 2019).

METODE PENELITIAN

Autokey Cipher

Autokey, seperti yang dijelaskan dalam Soni et al. (2022), adalah stream cipher yang tidak sinkron. Nama sandi menjelaskan fungsinya. Basis, atau kunci dasar K′, dicocokkan seluruhnya dengan semua huruf teks biasa P untuk dienkripsi dengan menambahkan teks biasa itu sendiri ke akhir K′. Rangkaian K'+P akan dikenal di seluruh tulisan ini sebagai K, kunci lengkapnya.

Enkripsi diselesaikan dengan menggeser semua karakter teks biasa ke depan sebanyak karakter yang cocok dengannya di K. Karena setiap karakter di P harus digeser oleh setiap karakter di K, karakter tambahan dalam kunci yang baru dibuat melebihi panjang P terpotong dan tidak digunakan. Hal ini menandakan bahwa panjang P adalah panjang batas atas untuk setiap K′ yang digunakan dalam enkripsi atau dekripsi.

Transposisi Kolom

Cipher transposisi mengubah posisi karakter dalam teks biasa alih-alih mengubahnya secara langsung. Teks biasa dililitkan di sekitar kunci setelah diisi. Kemudian huruf-huruf kunci tersebut diurutkan beserta kolom-kolom *plaintext*-nya. *Ciphertext* pada dasarnya diperoleh dengan membaca karakter sepanjang baris.

Pertama, kunci transposisi harus dipilih, dan harus diketahui oleh pihak pengirim yang harus mengenkripsi pesan dan pihak penerima yang harus mendekripsinya. Kunci transposisi terdiri dari serangkaian angka, yang menentukan bagaimana kolom teks biasa harus diubah urutan atau permutasinya. Kunci ini dapat diturunkan dari sebuah kata kunci (biasanya untuk kunci yang pendek) atau untuk kunci yang lebih panjang, dari frase kunci, karena kunci tersebut lebih mudah dihafal dibandingkan kunci numerik. Jika kata kunci (atau frase kunci) digunakan, kunci numerik yang setara diekstraksi dengan menetapkan setiap huruf dari kata kunci nilai numerik yang mencerminkan posisi relatif huruf dalam alfabet “A-to-Z”.

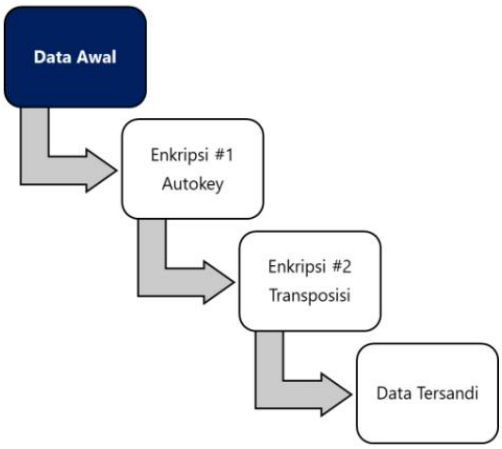
Untuk mengenkripsi teks biasa, pertama-tama kita salin teks biasa tersebut, baris demi baris, ke dalam persegi panjang. Lebar persegi panjang sama dengan panjang kuncinya. Di atas persegi panjang, kami menuliskan kata kunci, dan di atas kata kunci, kami menuliskan kunci numerik yang setara. Perhatikan bahwa baris terakhir persegi panjang tidak lengkap, dan oleh karena itu tiga kolom pertama persegi panjang transposisi, sebelum transposisi, lebih panjang (satu baris) dibandingkan empat kolom lainnya. Kasus ini disebut sebagai persegi panjang transposisi tidak lengkap atau transposisi kolom tidak beraturan (ICT). Kasus dimana semua kolom memiliki panjang yang sama dan semua baris lengkap disebut sebagai transposisi kolom lengkap (CCT).

Skema Penelitian

Dalam metode penelitian, tahap awal dilakukan dengan tahap enkripsi. Tahap enkripsi memadukan *Autokey Cipher*, selanjutnya diikuti oleh tahap Transposisi Kolom, diperoleh hasil enkripsi yang dapat diandalkan untuk mengamankan data. Dengan menerapkan *Autokey Cipher* terlebih dahulu, teks asli diubah secara dinamis menggunakan kunci yang terus berkembang, menambah tingkat keamanan dan kompleksitas enkripsi secara keseluruhan (Soni et al., 2022). Tahap berikutnya, yaitu Transposisi Kolom, memanfaatkan pola tertentu untuk mengacak urutan karakter dalam teks terenkripsi, menciptakan lapisan keamanan tambahan

p-ISSN:2527-5321
e-ISSN:2527-5941

yang sulit dipecahkan tanpa pengetahuan tentang susunan yang benar.

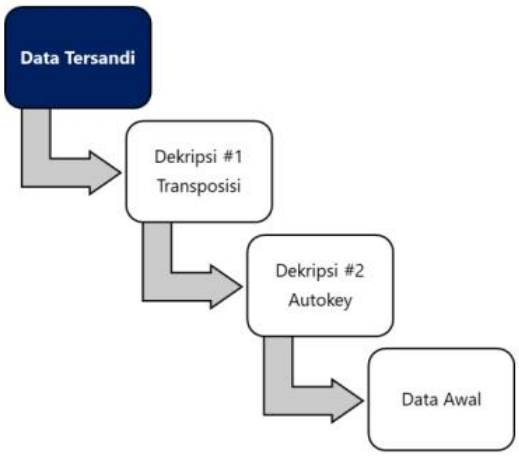


Gambar 1. Tahap enkripsi

Berdasarkan Algoritma Autokey, untuk persamaan dari Algoritma tersebut dapat dilihat pada persamaan dibawah ini:

$$C(i) = (p(i) + k(i)) \bmod m \qquad (1)$$

Tahap kedua dari penelitian ini yaitu dekripsi (kebalikan dari model enkripsi) dimana bertujuan untuk mengembalikan kedalam betuk teks semula. Tahpan ini dapat dilihat pada Gambar 1 dibawah ini.



Gambar 2. Tahap dekripsi

Langkah pertama melibatkan pengurutan ulang karakter-karakter berdasarkan pola tertentu yang diketahui oleh pihak yang berwenang, memungkinkan rekonstruksi urutan yang tepat dari data yang teracak. Setelah itu, Autokey Cipher digunakan dengan kunci yang sesuai untuk memulihkan teks asli dari hasil transposisi kolom (Budi Handoko, 2022). Dengan pendekatan ini, data dapat dipulihkan ke bentuk semula, memastikan aksesibilitas dan keaslian data yang terlindungi sebelumnya.

HASIL DAN PEMBAHASAN

Berdasarkan tahapan pada Gambar 1. Sebelum melakukan tahap enkripsi, dilakukan inisialisasi teks awal ‘UDINUSSMG’ dengan kunci autokey ‘FIKUNGGUL’, dan kunci transformasi kolom ‘JAYA’. Tahap awal dilakukan metode enkripsi *autokey*, *autokey* adalah sebuah teknik kriptografi di mana setiap karakter dari teks plainteks ditambahkan dengan karakter dari kunci yang bersesuaian (Purba et al., 2019). Proses ini menghasilkan teks sandi yang unik dan lebih sulit diprediksi. Setiap karakter dienkripsi secara berurutan dengan memperhitungkan karakter dari kunci yang terus bergeser sejalan dengan panjang teks asli (Aung & Hla, 2019). Langkah *auto key* dapat dilihat pada Tabel 1 berikut.

Tabel 1. Enkripsi autokey

Plain Text	Key	Chiper Text
U	F	W
D	I	N
I	K	Q
N	U	B
U	N	G
S	G	Y
S	G	Y
M	U	S
G	L	P

Tabel 2. Enkripsi transformasi kolom

J	**A**	**Y**	**A**
3	**1**	**4**	**2**
W	N	Q	B
G	Y	Y	S
P			

Berdasarkan Tabel 1. Tahap berikutnya dari proses enkripsi melibatkan transformasi kolom dari teks sandi yang dihasilkan sebelumnya. Dalam upaya ini, setiap karakter dalam teks sandi "WNQBGYYSP" diatur ulang berdasarkan susunan kolom yang telah ditentukan, menciptakan susunan baru yang sulit dipahami tanpa pengetahuan tentang pola transposisi yang benar.

Dengan menerapkan transformasi kolom menggunakan kunci ‘JAYA’ pada teks sandi ‘WNQBGYYSP’, didapatkan hasil baru dalam bentuk ciphertext ‘**NYBSWGPQY**’.

p-ISSN:2527-5321
e-ISSN:2527-5941

Melalui langkah transformasi kolom ini, karakter-karakter dalam teks sandi berhasil diatur ulang sesuai dengan pola yang ditetapkan oleh kunci, menciptakan susunan baru yang sulit dipahami tanpa pengetahuan tentang aturan transformasi yang benar. Tahap akhir dilakukan dekrip dari ciphertext 'NYBSWGPQY' menuju ke plain text yaitu 'UDINUSSMG'.

Tabel 3. Dekrip transformasi kolom

J	A	Y	A
3	**1**	**4**	**2**
W	N	Q	B
G	Y	Y	S
P			

Tabel 3 merupakan tahap awal dari dekrip (Transformasi Kolom), langkah dekrip pada algoritma transformasi kolom diambil dari kiri ke kanan dari susunan warna berikut:

Tabel 4. Tranformasi sesuai urutan kolom

W	N	Q	B
G	Y	Y	S
P			

Pengambilan text dekrip berbasis transformasi kolom, diambil dari kuning kiri ke kanan, hijau kiri ke kanan, dan biru seperti pada Tabel 4. Sehingga didapatkan hasil dekrip yang pertama yaitu **'WNQBGYYSP'.** Setelah itu dilakukan dekrip dengan algoritma awal yaitu autokey. Dengan key 'FIKUNGGUL' didapatkan hasil plain text awal yaitu '**UDINUSSMG'.**

Luaran dari penelitian ini yaitu jurnal Sinta 2, pada pembahsan jurnal Sinta 2 mendatang dilakukan evaluasi berbasis *Avalanche Effe*ct (AE) dengan mempertimbangkan input key yang serupa. Avalanche Effect merupakan ukuran yang penting dalam kriptografi yang mengevaluasi sejauh mana perubahan kecil pada input dapat menyebabkan perubahan signifikan pada output enkripsi. Dengan menggunakan key yang serupa dalam evaluasi ini, peneliti dapat mengukur sejauh mana kecilnya perbedaan pada key yang menghasilkan perubahan besar pada teks sandi, menunjukkan tingkat keamanan dan kompleksitas algoritma yang digunakan.
Melalui evaluasi ini, penelitian ini bertujuan untuk mengevaluasi tingkat kekuatan enkripsi yang dicapai oleh kombinasi Autokey Cipher dan Transposisi Kolom, serta memastikan bahwa sistem enkripsi yang dikembangkan dapat memenuhi standar keamanan yang diperlukan dalam melindungi data sensitif dari ancaman peretasan dan akses yang tidak sah.

SIMPULAN DAN SARAN

Berdasarkan langkah-langkah enkripsi dan dekripsi yang telah dilakukan menggunakan metode Autokey Cipher dan Transformasi Kolom, dapat disimpulkan bahwa kedua teknik kriptografi tersebut secara efektif memberikan lapisan keamanan yang tinggi terhadap data sensitif. Melalui proses Autokey Cipher, teks asli berhasil diubah menjadi teks sandi yang kompleks dan sulit diprediksi, sementara proses Transformasi Kolom berhasil mengacak urutan karakter teks sandi, menambahkan tingkat keamanan yang lebih tinggi. Penggunaan kunci yang berbeda, yaitu 'FIKUNGGUL' untuk enkripsi dan 'JAYA' untuk transformasi kolom, telah membuktikan keefektifannya dalam menjaga keamanan data dari akses yang tidak sah.

Dalam rangka meningkatkan keamanan sistem, disarankan untuk memperhatikan faktor keamanan tambahan, seperti rotasi kunci yang lebih kompleks dan penggunaan algoritma enkripsi yang lebih canggih. Selain itu, penting untuk mempertimbangkan penggunaan metode kriptografi yang diverifikasi dan diuji secara luas oleh komunitas keamanan cyber.

UCAPAN TERIMAKASIH

Terima kasih penulis ucapkan kepada LPPM Universitas Dian Nuswantoro atas Hibah Penelitian Dasar Perguruan Tinggi (PDPT 2023) bidang kajian kriptografi.

DAFTAR PUSTAKA

Ali, A., Al-rimy, B. A. S., Alsubaei, F. S., Almazroi, A. A., & Almazroi, A. A. (2023). HealthLock: Blockchain-Based Privacy Preservation Using Homomorphic Encryption in Internet of Things Healthcare Applications. *Sensors*, *23*(15). https://doi.org/10.3390/s23156762

Aung, T. M., & Hla, N. N. (2019). A Complex Polyalphabetic Cipher Technique Myanmar Polyalphabetic Cipher. *2019 International Conference on Computer Communication and Informatics*

(ICCCI), 1–9. https://doi.org/10.1109/ICCCI.2019.8821797

Budi Handoko, L. (2022). *SEKURITI TEKS MENGGUNAKAN VIGENERE CIPHER DAN HILL CIPHER* (Vol. 19, Issue 1).

Elkandoz, M. T., & Alexan, W. (2022). Image encryption based on a combination of multiple chaotic maps. *Multimedia Tools and Applications*, *81*(18), 25497–25518. https://doi.org/10.1007/s11042-022-12595-8

Jan, A., Parah, S. A., Hussan, M., & Malik, B. A. (2022). Double layer security using crypto-stego techniques: a comprehensive review. In *Health and Technology* (Vol. 12, Issue 1, pp. 9–31). Springer Science and Business Media Deutschland GmbH. https://doi.org/10.1007/s12553-021-00602-1

Lone, P. N., Singh, D., Stoffová, V., Mishra, D. C., Mir, U. H., & Kumar, N. (2022). Cryptanalysis and Improved Image Encryption Scheme Using Elliptic Curve and Affine Hill Cipher. *Mathematics*, *10*(20). https://doi.org/10.3390/math10203878

Purba, E. Y., Efendi, S., Sirait, P., & Sihombing, P. (2019). Collaboration of RSA Algorithm Using EM2B Key with Word Auto Key Encryption Cryptography Method in Encryption of SQL Plaintext Database. *Journal of Physics: Conference Series*, *1230*(1). https://doi.org/10.1088/1742-6596/1230/1/012009

Soni, D., Srivastava, D., Bhatt, A., Aggarwal, A., Kumar, S., & Shah, M. A. (2022). An Empirical Client Cloud Environment to Secure Data Communication with Alert Protocol. *Mathematical Problems in Engineering*, *2022*. https://doi.org/10.1155/2022/4696649

Taha, M. S., Mohd Rahim, M. S., Lafta, S. A., Hashim, M. M., & Alzuabidi, H. M. (2019). Combination of Steganography and Cryptography: A short Survey. *IOP Conference Series: Materials Science and Engineering*, *518*(5). https://doi.org/10.1088/1757-899X/518/5/052003

Umam, C., Handoko, L. B., Sari, C. A., Rachmawanto, E. H., & Hakim, L. A. R. (2022). Kombinasi Vigenere dan Autokey Cipher dalam Proses Proteksi SMS Berbasis Android. *Prosiding Sains Nasional Dan Teknologi*, *12*(1), 492. https://doi.org/10.36499/psnst.v12i1.7108

Wazid, M., Das, A. K., Chamola, V., & Park, Y. (2022). Uniting cyber security and machine learning: Advantages, challenges and future research. In *ICT Express* (Vol. 8, Issue 3, pp. 313–321). Korean Institute of Communication Sciences. https://doi.org/10.1016/j.icte.2022.04.007