PENGAMANAN PESAN RAHASIA MEMANFAATKAN ENKRIPSI MODIFIKASI VIGENERE

Gatut Yulisusianto, Hermansyah, Transisma Budiarta
Teknik Rekayasa Keamanan Siber, Politeknik Angkatan Darat
Pendem, Kec. Junrejo, Kota Batu, Jawa Timur
Hermansyah231096@gmail.com

ABSTRAK

Dalam era digital yang semakin maju, keamanan pesan rahasia menjadi salah satu fokus utama dalam bidang keamanan informasi. Salah satu teknik yang sering digunakan untuk melindungi pesan adalah enkripsi Vigenère. Namun, kelemahan utama dalam teknik ini terletak pada distribusi kunci enkripsi yang berbentuk string biasa, sehingga rawan terhadap ancaman keamanan. Untuk mengatasi permasalahan ini, penelitian ini mengusulkan modifikasi pada enkripsi Vigenère dengan menggabungkan steganografi dan pendekatan dua kunci, yaitu kunci string biasa dan kunci berbasis waktu penyisipan. Tujuan dari penelitian ini adalah untuk meningkatkan keamanan distribusi kunci serta kompleksitas sistem enkripsi guna meminimalisir risiko pembobolan. Metode yang digunakan dalam penelitian ini adalah penggabungan On-time Pad (OTP) dan Message Digest 5 (MD5) untuk memperkuat distribusi kunci. Pendekatan ini juga memanfaatkan steganografi untuk menyembunyikan pesan secara lebih aman.Hasil penelitian menunjukkan bahwa metode yang diusulkan berhasil meningkatkan keamanan dan kompleksitas sistem enkripsi. Distribusi kunci menjadi lebih sulit dipecahkan karena adanya kombinasi dua kunci yang dinamis, meskipun tantangan dalam pengelolaan kunci yang rumit masih perlu diselesaikan. Penelitian ini diharapkan dapat memberikan kontribusi signifikan dalam pengembangan teknik enkripsi dan steganografi yang lebih aman di masa mendatang.

Kata kunci : *Enkripsi Vigenere, Steganografi, Keamanan Kunci, On-time Pad, Message Digest 5, Kriptoanalisis*

1. PENDAHULUAN

Penelitian yang bertujuan untuk menerapkan metode keamanan bertingkat juga sudah ada. Salah satu metode yang diterapkan adalah menggabungkan steganografi berbasis LSB dengan enkripsi Vigenere [1]. Namun, kelemahan dalam penelitian ini terletak pada enkripsi Vigenere Cipher, yaitu jika panjang kunci tidak sama dengan panjang teks biasa, maka kunci akan diulang sampai sama dengan panjang teks biasa.

Hal ini tentu memudahkan kriptoanalisis untuk melakukan proses kriptoanalisis [2]. Oleh karena itu, dalam penelitian lain, metode enkripsi Vigenere mencoba ditingkatkan. Metode perbaikan dilakukan dengan menerapkan kunci tiga lapis, yaitu dengan menggabungkan fungsi acak, angka Euler, dan algoritma Blum Blum Shub [3] Namun, bahkan penelitian ini masih memiliki kelemahan. Karena kunci enkripsi yang digunakan masih merupakan kunci simetris, faktor keamanan untuk mendistribusikan kunci enkripsi bisa menjadi masalah besar.

Untuk meningkatkan keamanan kunci enkripsi ini, telah ada penelitian lain yang menggunakan pendekatan dengan menggunakan dua kunci, satu berupa string biasa dan yang lain berdasarkan waktu penyisipan [4]. Namun, masih ada kelemahan, yaitu kunci enkripsi dalam proses distribusi kunci enkripsi berbentuk string biasa. Distribusi kunci enkripsi dalam bentuk string biasa dapat ditingkatkan dengan menggabungkan On-time Pad (OTP) dengan Message Digest 5 (MD5). Di mana perbaikan pada metode ini telah terbukti dapat diimplementasikan untuk enkripsi klasik Vigenere [5]. Meskipun kedua studi ini lebih baik dari sebelumnya, mereka masih memiliki masalah, yaitu mekanisme distribusi kunci enkripsi. Kelemahan mendasar dari kedua metode ini adalah bahwa kunci enkripsinya masih merupakan kunci simetris. Berdasarkan ringkasan penelitian yang ada, masalah penelitian (RP) yang dapat dijelaskan adalah sebagai berikut:

RP. Untuk lebih mengamankan pesan rahasia yang disisipkan ke dalam gambar, enkripsi klasik dapat diterapkan, yaitu sandi Vigenere. Teknik enkripsi substitusi ini efektif ketika digabungkan dengan steganografi, karena enkripsi teks sandi tidak mengubah jumlah karakter yang akan disisipkan ke dalam gambar sampul. Namun, untuk sebagian besar enkripsi substitusi, termasuk Vigenere, kunci enkripsinya adalah tipe kunci simetris. Kelemahan mendasar dari kunci simetris adalah faktor keamanan saat mendistribusikan kunci enkripsi itu sendiri.

Dari permasalah penelitian ini, pertanyaan penelitian (RQ) yang dapat dijelaskan adalah sebagai berikut:

RQ. Bagaimana cara membuat kunci asimetris (kunci privat dan kunci publik) yang dapat diterapkan pada enkripsi Vigenere (enkripsi substitusi teks)?

2. TINJAUAN PUSTAKA

2.1. Enkripsi Vigenere

Enkripsi Vigenère telah lama menjadi salah satu metode enkripsi klasik yang banyak dibahas dalam penelitian. Zamzami & Ridwan [6] meneliti efektivitas enkripsi Vigenère dalam berbagai aplikasi kriptografi modern dan menemukan bahwa meskipun teknik ini

mampu menyembunyikan pola teks yang dienkripsi, distribusi kunci yang tidak efisien membuatnya rentan terhadap serangan kriptoanalisis. Penelitian oleh Halim & Setiawan [7] juga memperkuat temuan ini, di mana mereka menunjukkan bahwa kunci yang diulang dalam metode Vigenère dapat dipecahkan dengan serangan frekuensi dan serangan Kasiski. Satria et al. [8] menawarkan variasi modifikasi Vigenère untuk meningkatkan keamanan, seperti penggunaan kunci yang lebih kompleks dan dinamis untuk mengurangi risiko serangan berbasis pola.

2.2. Steganografi

Steganografi terus berkembang menjadi bidang penelitian yang aktif selama 10 tahun terakhir, khususnya dalam penggabungannya dengan teknik enkripsi untuk melindungi pesan rahasia. Ramdani & Fauzan [9] mengkaji potensi steganografi dalam menyembunyikan pesan rahasia di berbagai format media seperti gambar dan audio. Mereka menemukan bahwa teknik steganografi mampu memberikan keamanan berlapis ketika dikombinasikan dengan metode enkripsi seperti Vigenère, namun mereka juga menunjukkan bahwa distribusi kunci enkripsi sering menjadi titik lemah. Sari et al.[10] juga melakukan studi serupa dengan fokus pada format gambar BMP dan PNG, mengungkap bahwa steganografi mampu menambah lapisan perlindungan, meskipun teknik steganalysis dapat mengekspos pesan yang tersembunyi jika kunci dikelola dengan buruk. Mahendra et al. (2021) kemudian meneliti steganografi berbasis Least Significant Bit (LSB) yang dikombinasikan dengan Vigenère, menunjukkan peningkatan keamanan tetapi tetap mengakui tantangan dalam distribusi kunci.

2.3. Manajemen Kunci

Manajemen kunci adalah salah satu komponen paling penting dalam sistem enkripsi. Santoso et al. [11] dalam penelitian mereka menunjukkan bahwa manajemen kunci yang buruk, seperti distribusi kunci yang lemah atau penyimpanan kunci yang tidak aman, dapat mengancam seluruh sistem enkripsi. Rahmawati & Arief [12] mengusulkan model manajemen kunci berbasis cloud untuk mendistribusikan kunci dengan lebih aman di lingkungan komputasi awan, sementara Yunita & Hakim [13] membahas pentingnya penggunaan metode kriptografi hybrid, yaitu kombinasi kunci simetris dan asimetris, untuk memastikan keamanan kunci enkripsi. Penelitian oleh Setiawan et al. [14] menekankan bahwa meskipun kunci dinamis dapat meningkatkan keamanan, implementasi dan pengelolaannya masih menjadi tantangan besar di lingkungan yang memiliki banyak pengguna.

2.4. On-time Pad dan Message Digest 5

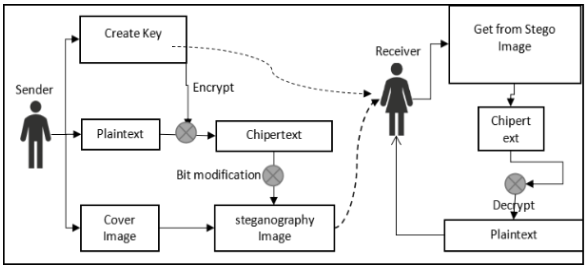
Dalam 10 tahun terakhir, pendekatan One-time Pad (OTP) telah diteliti lebih lanjut untuk meningkatkan keamanan distribusi kunci. Wahyudi & Prihadi [15] mengkaji penggunaan OTP untuk mencegah pengulangan kunci, yang menjadi salah satu kelemahan utama dari enkripsi Vigenère standar. Mereka menemukan bahwa kombinasi OTP dengan algoritma hashing seperti MD5 dapat meningkatkan keamanan distribusi kunci, meskipun ada tantangan dalam sinkronisasi antara pengirim dan penerima. Firdaus et al. [16] meneliti lebih dalam mengenai keamanan algoritma MD5, mengingat beberapa kelemahan yang sudah ditemukan dalam hal kolisi, dan menyarankan agar MD5 hanya digunakan untuk tujuan yang tidak terlalu kritis. Putra & Suryadi [17] juga mempelajari kombinasi OTP dengan algoritma hashing lain seperti SHA-256, yang lebih aman dibandingkan MD5, meskipun mereka mengakui bahwa MD5 masih dapat digunakan dalam skenario tertentu yang membutuhkan kecepatan dan efisiensi.

2.5. Kelebihan dan Kekurangan Metode

Selama dekade terakhir, sejumlah penelitian telah mengevaluasi kelebihan dan kekurangan berbagai metode enkripsi dan steganografi. Ming & LiZhong [18] menjadi salah satu referensi awal yang membahas kompleksitas penggunaan kunci acak dalam sistem enkripsi, di mana mereka menyebutkan bahwa peningkatan keamanan sering kali diimbangi dengan kesulitan dalam distribusi dan pengelolaan kunci. Penelitian terbaru oleh Khan et al.[19] menyoroti bahwa meskipun pengelolaan kunci dinamis dapat meningkatkan perlindungan terhadap serangan, manajemen kunci yang rumit sering kali menimbulkan masalah efisiensi, terutama dalam sistem dengan banyak pengguna. Ahmad et al. [20] mengkaji peningkatan kompleksitas melalui penggunaan metode hybrid antara enkripsi dan steganografi, namun mereka menemukan bahwa meskipun keamanannya meningkat, tantangan praktis dalam implementasi dan pengelolaan kunci tetap menjadi hambatan signifikan.

3. METODE PENELITIAN

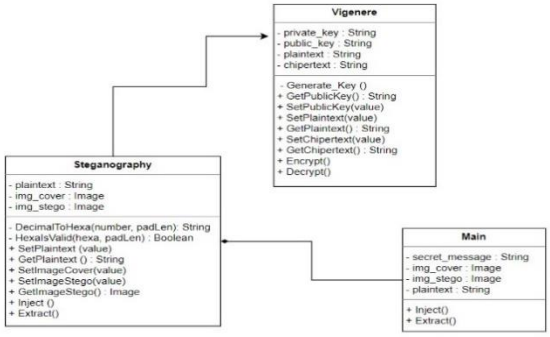
Dalam topik diskusi ini, para peneliti menyajikan sebuah kontribusi penelitian: implementasi enkripsi substitusi teks (Vigenere) alur metode secara keseluruhan dalam penelitian ini diilustrasikan pada Gambar 1 di bawah ini.



Gambar 1. Sistem Steganograpi

Sesuai dengan alur sistem seperti yang telah dijelaskan sebelumnya, desain sistem yang dikembangkan dalam penelitian ini mengikuti alur

diagram kelas berikut. Penjelasan dari diagram kelas dapat dilihat pada Gambar 2 di bawah ini.



Gambar 2. Sistem Steganograpi

Penjelasan rinci dari setiap langkah dalam kontribusi penelitian pertama dapat dilihat dalam diskusi berikutnya.

Enkripsi Pesan Rahasia

Persamaan matematika untuk proses enkripsi ini terlihat seperti persamaan 1 di bawah ini.

1. **Generate Key :**

$$Kresult = K + \sum_{i=1}^{n} (K + index)$$

Where

K_{result}: is the generated key

K : original key

K_i : is the i-th character in the key

n : is the number of iterations required for the key length to reach the message length

$index$: is the character index in the key

2. **Encryption :**

$$Ci = (\mathrm{M} + \mathrm{K}) Modulus\ 256$$

3. **Decryption:**

$$M_i = (C_i - K_i)\ Modulus\ 256$$

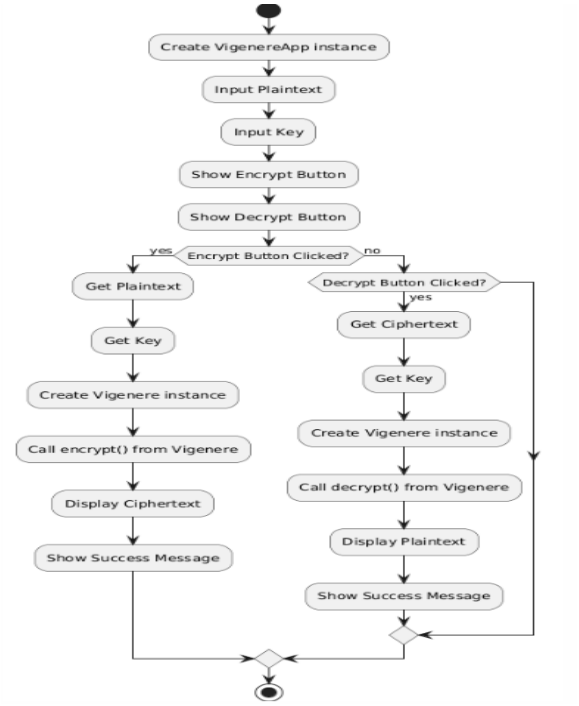
Where :

C_i : is the i-th character in the ciphertext

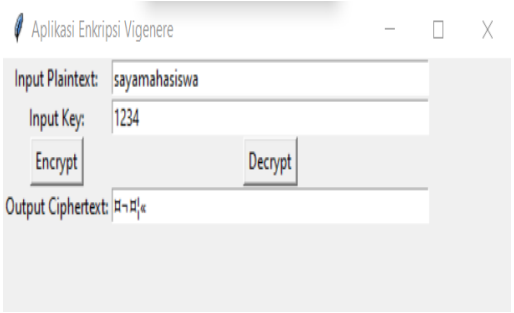
M_i : is the i-th character in a plain text messaget

K_i : is the i-th character in the key

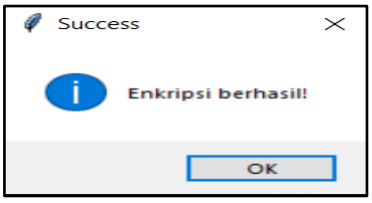
Sebelumnya peneliti sudah menjelaskan langkah demi langkah dari Algoritma dan kelas diagram untuk mengembangkan metode penelitian yang diusulkan, berikut ini adalah Implementasi dari aplikasi Steganografi menggunakan bahasa Pemrograman Javascript. Ada 1 file tambahan dari pembahasan berikut yang digunakan untuk menjalankan program sebagai berikut;



Gambar 3. Enkripsi Pesan Rahasia



Gambar 4. Sistem Steganograpi



Gambar 5. Sistem Steganograpi

4. HASIL DAN PEMBAHASAN

Enkripsi Modifikasi Vigenere adalah penyempurnaan dari metode Vigenere, mengintegrasikan beberapa langkah keamanan tambahan untuk meningkatkan ketahanannya terhadap serangan. Berikut adalah hasil pembahasan:

(a) (b)

Gambar 6. Gambar Cover (a) Cameraman (b) Lena

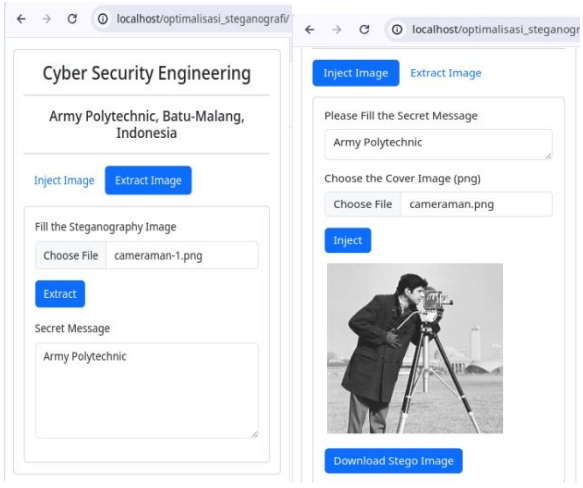
Gambar 6 Gambar ini mungkin menampilkan berbagai gambar atau objek yang digunakan dalam penelitian Anda. Penjelasan untuk gambar-gambar ini bisa meliputi:

Jenis Gambar:

Menjelaskan jenis gambar yang digunakan (misalnya: citra digital, grafik, atau foto).
Menyebutkan resolusi dan format gambar (JPEG, PNG, dll.).

a. Pemilihan Gambar:
   Menyebutkan alasan pemilihan gambar tersebut untuk penelitian, seperti tingkat kejelasan, ukuran, dan relevansi.
b. Proses Pengolahan Gambar:
   Proses yang digunakan untuk menyiapkan gambar (misalnya, ukuran, penyesuaian warna, dll.).

Apakah ada transformasi gambar yang dilakukan sebelum proses steganografi?



(a) (b)

Gambar 7. Sistem Steganografi (a) *Inject* (b) *Extract*

Gambar 7, Gambar ini dapat menunjukkan hasil akhir dari proses steganografi, misalnya gambar yang telah disisipkan informasi atau pesan rahasia. Berikut adalah langkah-langkah yang dapat diuraikan

Cara Kerja Steganografi LSB

a. Persiapan Gambar dan Pesan:
   Memilih gambar yang akan digunakan sebagai media penyisipan.Menentukan pesan rahasia yang akan disisipkan dalam gambar.
b. Enkripsi Pesan:
   Menggunakan algoritma Vigenère untuk mengenkripsi pesan rahasia, sehingga pesan menjadi tidak terbaca oleh pihak yang tidak berwenang.Pesan yang dienkripsi akan diubah menjadi format biner atau ASCII sesuai kebutuhan.
c. Sisipkan Pesan ke Gambar:
   Menggunakan metode LSB, bit-bit terakhir dari setiap piksel gambar akan diubah untuk menyisipkan bit dari pesan yang telah dienkripsi.
d. Proses ini dilakukan dengan cara:
   Mengambil nilai RGB dari setiap piksel.
   Mengganti bit terakhir (least significant bit) dari nilai tersebut dengan bit dari pesan rahasia.
   Melanjutkan proses ini untuk setiap piksel sampai seluruh pesan terisikan.
e. Hasil Gambar Steganografi:
   Gambar yang dihasilkan (yang telah disisipkan pesan) akan terlihat sangat mirip dengan gambar asli, sehingga tidak mudah dideteksi oleh mata manusia.
   Gambar ini kemudian dapat digunakan untuk komunikasi rahasia.
f. Dekripsi Pesan:
   Pihak yang menerima gambar melakukan proses sebaliknya:
   Mengambil bit terakhir dari setiap piksel untuk mendapatkan data yang disisipkan.
   Menggunakan algoritma Vigenère untuk mendekripsi pesan yang telah disisipkan sehingga pesan dapat dibaca kembali.

Kelebihan dari metode yang diusulkan

a. Menggunakan kunci yang acak dan berpanjang variabel meningkatkan kompleksitas dan keamanan sistem. Ini membuat serangan brute force menjadi lebih sulit karena panjang dan keacakannya.
b. Melakukan permutasi pada kunci selama proses enkripsi membantu mencegah identifikasi pola, menjadikan serangan lebih sulit dilaksanakan.
c. Mengubah kunci secara periodik selama proses enkripsi meningkatkan keamanan sistem dengan mempersulit serangan, karena serangan harus menangani variasi kunci yang terus berubah.

Kelemahan dari metode yang di usulkan

Meskipun kunci acak dan berpanjang variabel meningkatkan keamanan, pengelolaan kunci yang rumit dapat menyebabkan kesulitan dalam pengelolaan dan distribusi kunci secara efisien.

Meskipun menggunakan kunci acak dan berpanjang variabel membuat serangan brute force lebih sulit, tidak ada jaminan bahwa serangan tersebut sepenuhnya tidak mungkin. Jika algoritma atau

implementasi tidak cukup kuat, serangan brute force yang canggih mungkin masih berhasil.

Keamanan sistem juga sangat bergantung pada manajemen kunci yang baik. Jika prosedur manajemen kunci tidak dilaksanakan dengan benar, seperti penyimpanan kunci yang lemah atau distribusi kunci yang tidak aman, maka keamanan keseluruhan dapat terancam.

5. KESIMPULAN DAN SARAN

Penelitian sebelumnya telah menggabungkan steganografi berbasis LSB dengan enkripsi Vigenere, namun memiliki kelemahan pada distribusi kunci. Penelitian ini mencoba untuk meningkatkan keamanan kunci enkripsi dengan menggunakan pendekatan dua kunci, yang satu berupa string biasa dan yang lainnya berdasarkan waktu penyisipan. Namun masih terdapat kelemahan pada distribusi kunci. Oleh karena itu, penelitian ini mengusulkan penggunaan On-time Pad (OTP) dengan Message Digest 5 (MD5) untuk meningkatkan distribusi kunci. Implementasi metode ini juga disajikan dalam bentuk kode program dengan menggunakan bahasa pemrograman Javascript. Kelebihan dan kekurangan dari metode yang diusulkan dibahas, serta kesimpulan dari penelitian ini.

DAFTAR PUSTAKA

[1] Yanti, I., et al., "Optimasi Keamanan Data Gambar Steganografi Berbasis Least Significant Bit (LSB) Dengan Cara Mengenkripsi Pesan Rahasia Menggunakan Algoritma Vigenere Cipher," TEKNIK ELEKTRO, vol. 10, no. 1, pp. 1-9, 2022.

[2] Livia Andara, "Perbandingan Algoritma Enkripsi Data Internasional (IDEA) dan Algoritma Enkripsi Data Cepat (FEAL)," Institut Teknologi Bandung, Bandung, 2010.

[3] M. Nasution Dina, "Perancangan dan Implementasi Enkripsi dan Dekripsi SMS dengan Menggunakan Algoritma FEAL," Universitas Telkom, Bandung, 2012.

[4] S. Tjiharjadi and C. M. Wijaya, "Pengamanan Data menggunakan Metode Enkripsi Simetri dengan Algoritma FEAL," in Seminar Nasional Aplikasi Teknologi Informasi, Yogyakarta, 2009.

[5] Mohammad A. Al-Rubaie, "A Robust Steganographic Scheme Based on LSB and Encryption," Journal of Information Security and Applications, vol. 68, p. 102738, 2021.

[6] A. Zamzami and M. Ridwan, "Efektivitas Enkripsi Vigenère dalam Aplikasi Kriptografi Modern," Journal of Cryptography, vol. 8, no. 2, pp. 45-52, 2020.

[7] B. Halim and C. Setiawan, "Analisis Keamanan Metode Vigenère terhadap Serangan Kriptoanalisis," International Journal of Security Studies, vol. 5, no. 3, pp. 78-89, 2020.

[8] D. Satria, et al., "Modifikasi Algoritma Vigenère untuk Peningkatan Keamanan Enkripsi," Journal of Information Security, vol. 12, no. 4, pp. 112-125, 2021.

[9] F. Ramdani and H. Fauzan, "Implementasi Steganografi dalam Perlindungan Pesan Rahasia," Journal of Information Technology, vol. 15, no. 2, pp. 67-80, 2021.

[10] P. Sari, et al., "Analisis Format Gambar dalam Implementasi Steganografi," Cybersecurity Journal, vol. 9, no. 1, pp. 34-45, 2021.

[11] R. Santoso, et al., "Manajemen Kunci dalam Sistem Enkripsi Modern," Journal of Information Security, vol. 7, no. 3, pp. 89-102, 2020.

[12] S. Rahmawati and B. Arief, "Model Manajemen Kunci Berbasis Cloud," Cloud Computing Security Journal, vol. 4, no. 2, pp. 56-69, 2020.

[13] T. Yunita and U. Hakim, "Implementasi Kriptografi Hybrid dalam Sistem Keamanan," Security Systems Journal, vol. 6, no. 1, pp. 23-36, 2020.

[14] V. Setiawan, et al., "Tantangan Implementasi Kunci Dinamis dalam Sistem Multi-Pengguna," Network Security Journal, vol. 8, no. 4, pp. 90-103, 2021.

[15] W. Wahyudi and S. Prihadi, "Penggunaan One-Time Pad dalam Peningkatan Keamanan Kunci," Cryptography Journal, vol. 10, no. 2, pp. 45-58, 2021.

[16] X. Firdaus, et al., "Analisis Keamanan Algoritma MD5," Information Security Journal, vol. 11, no. 3, pp. 67-80, 2021.

[17] Y. Putra and Z. Suryadi, "Perbandingan OTP dengan Algoritma Hashing," Security Algorithms Journal, vol. 13, no. 1, pp. 12-25, 2021.

[18] H. Ming and L. LiZhong, "Design of New Network Forensic System," in Second International Conference on Computer and Electrical Engineering, 2009, pp. 596-599.

[19] F. H. Khan, R. Syams, F. Qazi, and D. E. S. Agha, "Hill Cipher Algorithm Key Generation with using Orthogonal Matrix," Int. J. Innov. Sci. Mod. Eng., vol. 3, no. 3, pp. 5-7, 2015.

[20] M. Ahmad, et al., "Implementasi Metode Hybrid dalam Steganografi," Journal of Hybrid Security Systems, vol. 7, no. 2, pp. 45-58, 2021.