Jurnal Riset Mahasiswa Matematika
Volume 2(6) (2023), Pages 214-220
p-ISSN: 2808-1552; e-ISSN: 2808-4926

# Penyandian Pesan Hybrid dengan Myszkowski Cipher dan Rivest, Shamir, Adleman (RSA)

**Sukmawati Indah Safitri*, Muhammad Khudzaifah, Mohammad Nafie Jauhari**

* Program Studi Matematika, Fakultas Sains dan Teknologi, Universitas Islam Negeri Maulana Malik Ibrahim Malang, Indonesia

sukmawati.ss15@gmail.com*, khudzaifah@uin-malang.ac.id, nafie.jauhari@uin-malang.ac.id

**Abstrak**

Kriptografi klasik dan kriptografi modern memiliki sisi kelebihan dan kelemahan dalam mengamankan pesan teks. Algoritma *hybrid* dapat menggabungkan dua algoritma untuk menghasilkan tingkat keamanan pesan yang lebih tinggi jika dibandingkan dengan penggunaan satu jenis algoritma saja. Penelitian ini membahas tentang algoritma *hybrid* yang menggabungkan *Myszkowski Cipher* dan RSA yang merupakan kriptografi klasik dengan teknik transposisi serta kriptografi modern dengan teknik substitusi. Tujuan dilakukannya penelitian ini yaitu agar mendapatkan *ciphertext* yang lebih sulit dipecahkan oleh kriptanalisis. Proses algoritma *hybrid* dilakukan dengan mengenkripsi pesan teks dengan algoritma *Myszkowski Cipher* kemudian kata kunci yang digunakan dalam algoritma *Myszkowski Cipher* dienkripsi menggunakan algoritma RSA dengan persamaan $C = M^e \ mod \ N$. Maka akan diperoleh *ciphertext* dan *cipherkey* berbentuk numerik. Dalam proses dekripsinya dilakukan dengan mendekripsikan *cipherkey* dengan RSA terlebih dahulu dengan menentukan nilai $d$ sebagai kunci privat untuk mengamankan pesan sehingga $de = 1 \ (mod \ \phi(N))$ dengan menggunakan persamaan $d = \frac{1+(k.\phi(N)}{e}$. Selanjutnya yaitu dengan mencoba nilai $k = 1,2,3, \ldots$ hingga diperoleh nilai $d$ yang bulat, setelah itu dapat dilakukan dekripsi sesuai dengan persamaan $P = C^d \ mod \ N$, maka proses dekripsi *ciphertext* pesan menggunakan algoritma *Myszkowski Cipher* dapat dilakukan. Manfaat dari penelitian ini yaitu dapat meningkatkan keamanan pesan teks yang dikirimkan karena menerapkan keunggulan dari masing-masing algoritma dalam penyandiannya.

**Kata kunci**: *hybrid*; *myszkowski cipher*; algoritma; RSA.

**Abstract**

Classical and modern cryptography have advantages and disadvantages in securing text messages. Hybrid algorithms can combine two algorithms to produce a higher level of message security when compared to one type of algorithm. This study discusses a hybrid algorithm that combines Myszkowski Cipher and RSA. The purpose of this research is to obtain ciphertext that is more difficult to crack by cryptanalysis. The hybrid algorithm process is done by encrypting text messages with the Myszkowski Cipher algorithm then the key used in the Myszkowski Cipher algorithm are encrypted using the RSA algorithm with the equation $C = M^e \ mod \ N$. Then the ciphertext and cipherkey will be obtained in numerical. The decryption process is done by decrypting the cipherkey by specifying the value of $d$ as the private key so that $de = 1 \ (mod \ \phi(N))$ using the equation $d = \frac{1+(k.\phi(N)}{e}$. Next is by trying the value of $k = 1,2,3, \ldots$ until a $d$ value is obtained, after which decryption to the equation $P = C^d \ mod \ N$, then the process of decrypting ciphertext using Myszkowski Cipher can be done. The benefit of this research can improve the security of messages because it applies the advantages of each algorithm in its encoding.

**Keywords**: *hybrid*; *myszkowski cipher*; algorithm; RSA.

## PENDAHULUAN

Terdapat beberapa cara untuk mengamankan pesan dan salah satunya adalah dengan menerapkan ilmu kriptografi. Ilmu kriptografi adalah suatu teknik dalam matematika yang

Submitted: 12 Agustus 2022 Reviewed: 20 April 2023 Accepted: 26 Agustus 2023
Doi: http://dx.doi.org/10.18860/jrmm.v2i6.22017

mempelajari tentang proses keamanan pengiriman dan penerimaan informasi data, misalnya validitas data, kesatuan data, dan autentikasi data [1]. Menurut Meylisa Siska, ilmu kriptografi merupakan sebuah ilmu pengetahuan yang di dalamnya membahas tentang keamanan sebuah pesan yang ditujukan pengirim kepada penerima pesan agar sampai dengan selamat dan dapat terjaga keamanannya. Ilmu kriptografi adalah sebuah ilmu matematis yang bisa disebut sebagai ilmu kriptologi. Ilmu kriptologi ini memiliki tujuan untuk menjaga keamanan informasi yang ada di dalam sebuah data, sehingga informasi data yang dikirimkan itu tidak akan bisa diketahui oleh orang yang tidak berwenang.

*Myszkowski Cipher* merupakan salah satu jenis dari algoritma cipher transposisi kriptografi klasik. Algoritma transposisi ini memerlukan kata kunci dengan karakter yang berulang [2]. *Myszkowski Cipher* memiliki keunikan dan dapat dimodifikasi dengan mudah, algoritma cipher transposisi ini cukup menarik karena terdapat perbedaan dalam pembacaan dan penulisan *ciphertext* ketika memiliki nomor kunci yang sama [3]. Algoritma transposisi *Myszkowski Cipher* ini merupakan variasi dari Columnar Transposition yang diciptakan oleh tokoh yang bernama Émile Victor Théodore Myszkowski pada tahun 1902.

Berikut adalah beberapa penelitian terdahulu yang terkait di antaranya yaitu penelitian Khairina, pada penelitian ini peneliti memodifikasi algoritma *Myszkowski Transposition Cipher* dengan *Chess Board Pattern*. Enkripsi dan dekripsi dengan *Chess Board Pattern* dilakukan dengan mengikuti pola papan catur berwarna hitam putih. Kombinasi algoritma *Myszkowski* dengan *Chess Board Pattern* menghasilkan variasi pola enkripsi dan dekripsi yang beragam, sehingga proses enkripsi dan dekripsi menjadi lebih rumit [3]. Kemudian penelitian oleh Agustina, pada penelitian ini dilakukan suatu analisis dalam perspektif keamanan dokumen yang bertujuan untuk mengamankan dokumen menggunakan metode RSA. Untuk proses penerapannya suatu data yang dikirim terlebih dahulu dienkripsi oleh pengirim dan menghasilkan data terenkripsi selanjutnya akan dikirim kepada penerima untuk dilakukan proses dekripsi yang menghasilkan suatu data yang sebenarnya. Dari penelitian ini dapat disimpulkan bahwa tingkat keamanan dengan menggunakan metode RSA termasuk dalam kategori metode yang aman dipakai untuk proses pengamanan dokumen [4].

Kelemahan yang dimiliki oleh algoritma *Myszkowski Cipher* sebagai kriptografi klasik yaitu jika kita mengenkripsi pesan dengan menerapkan hanya satu algoritma saja akan mudah dipecahkan oleh kriptanalisis jika tidak digabung dengan algoritma lain, karena masih tergolong algoritma kriptografi dengan kunci simetris. Namun, penerapan algoritma kriptografi kunci simetris masih sering dilakukan karena bisa menjalankan proses enkripsi dan dekripsi pesan dalam waktu yang terbilang cukup efektif, akan tetapi perlindungan kunci pada algoritma kunci simetris ini masih kurang aman, sehingga untuk mengamankan isi pesan yang dikirim kunci yang digunakan harus sering diganti untuk mencegah penyerangan pada kriptografi oleh kriptanalisis. Sementara itu, kriptografi asimetris adalah kebalikannya, keamanan dari kunci yang digunakan pada algoritma asimetris sangat terjamin, akan tetapi proses ketika melakukan enkripsi dan dekripsi pesan akan lebih lambat karena masih memerlukan waktu yang lebih banyak dalam prosesnya.

*Hybrid* merupakan gabungan antara kriptografi yang memakai kunci simetris dan kriptografi yang memakai kunci asimetris. Dalam penggunaan algoritma *hybrid*, teknik enkripsi yang digunakan adalah enkripsi simetri di mana kunci dekripsi sama dengan kunci enkripsi. Untuk kunci publik kriptografi, diperlukan teknik enkripsi asimetris di mana kunci dekripsi tidak sama dengan kunci enkripsi [5]. Sistem enkripsi *hybrid* ini banyak digunakan selain dapat meningkatkan keamanan pesan teks dan kunci yang dikirimkan, algoritma *hybrid* juga akan melibatkan lebih banyak perhitungan jika dibandingkan dengan menggunakan satu algoritma saja. Penggunaan sistem enkripsi algoritma *hybrid* yang digunakan pada penelitian ini adalah suatu kombinasi dari kriptografi algoritma *Myszkowski Cipher* yang termasuk bagian dari algoritma kriptografi kunci simetris dan algoritma RSA yang termasuk bagian dari algoritma kriptografi kunci asimetris agar dapat meningkatkan perlindungan dari pesan teks dan akan menghasilkan *ciphertext* yang lebih sulit dipecahkan.

Algoritma RSA merupakan algoritma asimetris yang teruji sebagai sistem kriptografi yang aman karena kesulitan dalam proses memfaktorkan bilangan yang sangat besar [6]. Sehingga

penulis memutuskan untuk mengambil judul penelitian Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA untuk Mengamankan Pesan Teks.

## METODE

### Pendekatan Penelitian

Jenis penelitian ini adalah penelitian kualitatif dengan menggunakan studi kepustakaan untuk menambah pemahaman teori yang akan dikembangkan.

### Teknik Analisis

Terdapat beberapa langkah dalam tahapan penelitian yang dilakukan yaitu:

1. Penentuan algoritma yang sesuai untuk diterapkan pada proses enkripsi dan dekripsi pesan secara *hybrid*. Berdasarkan latar belakang dari penelitian ini maka akan digunakan suatu kombinasi *hybrid Myszkowski Cipher* dan algoritma RSA untuk pengamanan pesan teks.
2. Mengombinasikan kedua algoritma secara *hybrid* dengan mengenkripsi kata kunci yang digunakan pada *Myszkowski Cipher* dengan algoritma RSA menggunakan proses pembangkitan kunci dengan memanfaatkan bilangan prima sehingga kata kunci yang semula berbentuk alfabet setelah dienkripsi dengan RSA menjadi berbentuk angka melalui proses dekripsi [7].
3. Melakukan simulasi algoritma *hybrid* dengan menggunakan *Myszkowski Cipher* dan algoritma RSA sebagai berikut:
    a. Menentukan *plaintext* dan kunci untuk dienkripsi menggunakan algoritma *Myszkowski Cipher.*
    b. Setelah mendapatkan *ciphertext* hasil enkripsi dari algoritma *Myszkowski Cipher*, kemudian mengenkripsi kata kunci dengan algoritma RSA dengan menggunakan persamaan
    $$C = M^e \ mod \ N$$
    c. Dalam mengenkripsi kata kunci pada algoritma *Myszkowski Cipher* menggunakan algoritma RSA kita perlu membangkitkan kunci publik $(e, N)$ dan kunci privat $(d, N)$ terlebih dahulu [8].
    d. Kemudian mengenkripsi kata kunci pada algoritma *Myszkowski Cipher* dengan memanfaatkan kunci publik $(e, N)$ yang sudah ditetapkan pada algoritma RSA dengan persamaan
    $$C = M^e \ mod \ N$$
    yang akan menghasilkan *cipherkey* berbentuk angka.
    e. Selanjutnya pengirim akan membagikan kunci privat $(d, N)$ kepada penerima pesan untuk proses dekripsi kata kunci yang terenkripsi.
    f. Setelah kunci privat didapatkan, kata kunci dapat didekripsi dengan persamaan
    $$P = C^d \ mod \ N$$
    algoritma RSA untuk mendapatkan kata kunci berbentuk huruf yang digunakan dalam algoritma *Myszkowski Cipher*.
    g. Kemudian melakukan dekripsi pada pesan teks yang terenkripsi menggunakan kata kunci dalam algoritma *Myszkowski Cipher* yang telah didekripsi dari algoritma RSA sehingga diperoleh *plaintext* dari pesan yang dikirimkan [9].
    h. Mendapatkan *plaintext* dari pesan teks yang dikirimkan.

## HASIL DAN PEMBAHASAN

### *Enkripsi Algoritma Hybrid Menggunakan Myszkowski Cipher dan RSA*

Berikut akan dijelaskan tentang enkripsi algoritma *Hybrid*.

1. Memberikan penomoran pada kata kunci yang digunakan oleh algoritma *Myszkowski Cipher*.

2. Membuat kolom dengan ukuran sesuai banyak karakter kata kunci.
3. Menentukan jumlah baris yang harus dibuat yaitu dengan persamaan
$$\frac{\sum karakter\ ciphertext}{\sum karakter\ kata\ kunci} = \sum baris$$
4. Menuliskan *plaintext* pesan teks secara horizontal dari kiri ke kanan.
5. *Ciphertext* dibaca secara vertikal berdasarkan urutan kata kunci terkecil, untuk kata kunci yang memiliki penomoran sama maka *ciphertext* dibaca secara horizontal kemudian vertikal [10].
6. Selanjutnya kata kunci pada algoritma *Myzskowski Cipher* yang semula berbentuk alfabet akan dienkripsi dengan RSA supaya menjadi bentuk numerik, langkah pertama yaitu menentukan nilai $p$ dan $q$ dengan bilangan prima yang berbeda.
7. Setelah nilai $p$ dan $q$ ditentukan, akan didapatkan nilai $N$ yang merupakan hasil kali dari $p$ dan $q$ sesuai dengan persamaan
$$N = p\ x\ q$$
8. Kemudian menentukan nilai dari $\phi(N)$ dengan menggunakan persamaan
$$\phi(N) = (p - 1)\ (q - 1)$$
9. Selanjutnya adalah memilih sebarang bilangan untuk kunci publik atau nilai $e$ yang relatif prima terhadap $\phi(N)$ dan nilai $1 < e < \phi(N)$.
10. Setelah nilai $e$ diperoleh, maka akan ditentukan kunci privat yang disimbolkan dengan $d$ yang memenuhi syarat sesuai dengan persamaan $(e.d)\ mod\ \phi(N) = 1$. Maka diperoleh pasangan kunci publik dan kunci privat yang dapat dituliskan dengan $(e, N)$ untuk kunci publik dan $(d, N)$ untuk kunci privat [11].
11. Setelah semua langkah terpenuhi, dapat dilakukan enkripsi pada kata kunci yang digunakan pada algoritma *Myzskowski Cipher* dengan persamaan
$$C = M^e\ mod\ N.$$

**Simulasi Enkripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA**

*Plaintext* : TAHUN INI SIDANG SKRIPSI DAN LULUS
Kunci : MATEMATIKA
Proses enkripsi dapat dilakukan dengan cara menulis pesan teks secara horizontal dalam kolom dan baris yang telah disesuaikan dengan banyaknya karakter kunci.

**Tabel 1** Proses Enkripsi *Myszkowski Cipher*

| **M** | **A** | **T** | **E** | **M** | **A** | **T** | **I** | **K** | **A** |
|---|---|---|---|---|---|---|---|---|---|
| **5** | **1** | **6** | **2** | **5** | **1** | **6** | **3** | **4** | **1** |
| **T** | A | H | U | N | I | N | I | S | I |
| **D** | A | N | G | S | K | R | I | P | S |
| **I** | D | A | N | L | U | L | U | S | X |

Pada akhir kalimat dilakukan penambahan huruf X sebagai pelengkap pada kolom tabel enkripsi yang kosong, sehingga dapat memudahkan dalam pembacaan *ciphertext* saat dilakukan proses enkripsi tahap pertama pesan teks pada algoritma *Myszkowski Cipher* ini [12]. Berdasarkan tabel tersebut diperoleh hasil *ciphertext* yaitu **AIIAKSDUX UGN IIU SPS TNDSIL HNNRAL**. Pada proses enkripsi tahap kedua menggunakan algoritma RSA akan dilakukan enkripsi pada kata kunci yang telah digunakan pada algoritma *Myszkowski Cipher* sebelumnya.

1. Menentukan nilai $p$ dan $q$
$$p = 47, \quad q = 23$$

2. Menentukan nilai $N$

$$N = 1081$$

3. Menentukan $\phi(N)$

$$\phi(N) = 1012$$

4. Menentukan kunci publik $e$

Ambil $e = 17$, Lakukan pengecekan bahwa $GCD(17,1012) = 1$ dengan Euclid:

$$1012\ mod\ 17 = 9$$
$$17\ mod\ 9 = 8$$
$$9\ mod\ 8 = 1$$
$$8\ mod\ 1 = 0$$

sehingga $e = 17$ memenuhi syarat tersebut.

5. Menentukan kunci privat $d$

**Tabel 2** Penentuan Kunci Privat $d$

| $e.d$ | $e.d\ mod\ \phi(N)$ |
|---|---|
| 17.1 = 17 | 17 mod 1012 = 17 |
| 17.2 = 34 | 34 mod 1012 = 34 |
| 17.3 = 51 | 51 mod 1012 = 51 |
| ⋮ | ⋮ |
| 17.893 = 15181 | 15181 mod 1012 = 1 |

kunci publik $(e, N) = (17, 1081)$ dan kunci privat $(d, N) = (893, 1081)$.

Enkripsi kunci *Myszcowski Cipher* dengan algoritma RSA:

$$C = M^e\ mod\ N$$
$$C = M^{17}\ mod\ 1081$$
$$P\ =\ MATEMATIKA$$

Sehingga diperoleh *Ciphertext* $(C)$ = [**151 849 700 483 151 849 700 646 679 849**].

**Dekripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA**

Berikut akan dijelaskan tentang dekripsi algoritma *Hybrid*.

1. Melakukan pembagkitan kunci privat dari nilai $N$ yang telah diterima untuk memperoleh nilai $d$ sebagai kunci privat algoritma RSA [13].
2. Setelah didapatkan nilai $d$, maka dapat dilakukan proses perhitungan sesuai dengan persamaan $P\ =\ C^d\ mod\ N$ menggunakan *software Python*.
3. Kata kunci algoritma *Myzkowski Cipher* yang telah kembali ke bentuk alfabet dapat digunakan untuk mendekripsi pesan teks yang sebelumnya terenkripsi dengan algoritma *Myzkowski Cipher* .
4. Menentukan jumlah baris menggunakan persamaan:

$$\frac{\sum karakter\ ciphertext}{\sum karakter\ kata\ kunci} = \sum baris$$

5. Kemudian *ciphertext* pesan teks dituliskan secara vertikal berdasarkan urutan pada penomoran kata kunci, setelah itu *plaintext* dari pesan teks tersebut dibaca secara horizontal agar dapat kembali ke pesan awal [14].

**Simulasi Dekripsi Algoritma *Hybrid* Menggunakan *Myszkowski Cipher* dan RSA**

*Ciphertext* : AIIAKSDUX UGN IIU SPS TNDSIL HNNRAL
*Cipherkey* : [151 849 700 483 151 849 700 646 679 849]
Nilai $N\ =\ 1081$ dan $d\ =\ 893$ yang diperoleh berdasarkan persamaan

$$d = \frac{1 + (k.\phi(N)}{e}$$

dengan mencoba nilai $k = 1,2,3, \ldots$ hingga diperoleh nilai $d$ yang bulat.

Dalam melakukan dekripsi pada kunci dengan algoritma RSA dapat dilakukan dengan menggunakan persamaan berikut:

$$P = C^d \ mod \ N$$
$$P = C^{893} \ mod \ 1081$$

*Ciphertext* (C) = [151 849 700 483 151 849 700 646 679 849]

Sehingga diperoleh hasil dekripsi kunci sebagai berikut:

| **77** | **65** | **84** | **69** | **77** | **65** | **84** | **73** | **75** | **65** |
|---|---|---|---|---|---|---|---|---|---|
| M | A | T | E | M | A | T | I | K | A |

Dalam melakukan dekripsi menggunakan algoritma *Myszkowski Cipher*, perlu dilakukan perhitungan banyak baris pada tabel yang harus disediakan untuk penulisan *ciphertext* [15]. Maka, jumlah baris yang harus disediakan adalah 3 baris karena dalam menentukan banyak baris akan selalu dibulatkan ke bilangan yang lebih tinggi dan jumlah kolom mengikuti banyaknya jumlah karakter kata kunci yaitu sebanyak 10 kolom.

**Tabel 3** Proses Dekripsi Kunci Ke-6 *Myszkowski Cipher*

| **M** | **A** | **T** | **E** | **M** | **A** | **T** | **I** | **K** | **A** |
|---|---|---|---|---|---|---|---|---|---|
| 5 | 1 | 6 | 2 | 5 | 1 | 6 | 3 | 4 | 1 |
| T | A | **H** | U | N | I | **N** | I | S | I |
| D | A | **N** | G | S | K | **R** | I | P | S |
| I | D | **A** | N | L | U | **L** | U | S | X |

Dengan menghilangkan huruf X di akhir kalimat maka *plaintext* kembali seperti semula yaitu *P* = **TAHUN INI SIDANG SKRIPSI DAN LULUS**.

## KESIMPULAN

Berdasarkan hasil dan pembahasan di atas maka dapat diperoleh *ciphertext* yang terenkripsi secara transposisi dan *cipherkey* berbentuk numerik yang digunakan untuk mendekripsi pesan teks. Dengan menggunakan algoritma *hybrid*, keamanan pesan teks lebih terjaga karena pengirim hanya mengirimkan *ciphertext* pesan, *cipherkey* berbentuk angka dan nilai *N*.

## DAFTAR PUSTAKA

[1] A. N. Agustina, Aryanti, and Nasron, "Pengamanan Dokumen Menggunakan Kombinasi Metode Rsa (Rivest Shamir Adleman) Dan Vigenere Cipher," *Pros. Semin. Nas. Multi Disiplin Ilmu Call Pap. UNISBANK*, pp. 14–19, 2017.

[2] R. Alvionita, "Implementasi Algoritma Super Enkripsi (Affine Cipher dan Route Cipher) pada Pesan Teks," UNIVERSITAS ISLAM NEGERI MAULANA MALIK IBRAHIM MALANG, 2021.

[3] Basri, "Pendekatan Kriptografi Hybrid pada Keamanan Dokumen Elektronik dan HypertextTransfer Protocol Secure (HTTPS) (Analisis Potensi Implementasi Pada Sistem Keamanan)," *J. Ilmu Komput.*, vol. 1, no. 2, pp. 32–37, 2015.

[4] O. Ekwardo, "Modifikasi Columnar transposition Menggunakan Sebuah Fungsi Transposisi," *Tek. Inform. ITB*, pp. 1–4, 2018.

[5] A. Ginting, R. R. Isnanto, and I. P. Windasari, "Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email," *J. Teknol. dan Sist. Komput.*, vol. 3, no. 2, pp. 253–258, 2015, [Online]. Available: https://media.neliti.com/media/publications/144706-ID-implementasi-algoritma-kriptografi-rsa-u.pdf.

[6] D. B. Ginting, "Peranan Aritmetika Modulo dan Bilangan Prima pada Algoritma Kriptografi RSA (Rivest-Shamir-Adleman)," *Media Inform.*, vol. 9, no. 2, pp. 48–57, 2010.

[7] J. Jamaludin, "Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem," *Sink. J. dan Penelit. Tek. Inform.*, vol. 2, no. April 2018, 2018, [Online]. Available: https://jurnal.polgan.ac.id/index.php/sinkron/article/view/139.

[8] N. Khairina, "Modifikasi Myszkowski Transposition Cipher dengan Chess Board Pattern," *Pros. Semin. Nas. Teknol. Inform.*, vol. 2, no. 1, pp. 28–34, 2019.

[9] J. Alda, P. Sikumbang, A. Fauzi, and H. Khair, "Penerapan Algoritma RSA Keamanan Pesan Teks Dengan Memanfaatkan Steganografi LSB ( Least Significant Bit ) Citra," vol. 11, pp. 29–34, 2022.

[10] S. Ling and C. Xing, *Coding Theory A First Course*. Cambridge University Press, 2004.

[11] T. Rahajoeningroem and M. Aria, "Studi dan Implementasi Algoritma RSA untuk Pengamanan Data Transkrip Akademik Mahasiswa," *Maj. Ilm. Unikom*, vol. 8, no. 1, pp. 77–90, 2011, [Online]. Available: http://jurnal.unikom.ac.id/_s/data/jurnal/v08-n01/volume-81-artikel-9.pdf/pdf/volume-81-artikel-9.pdf.

[12] R. Y. Pohan, "Studi dan Perbadingan Berbagai Macam Algoritma Cipher Transposisi," *Informatika.Stei.Itb.Ac.Id*, pp. 1–5, 2007, [Online]. Available: https://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2007-2008/Makalah1/MakalahIF5054-2007-A-021.pdf.

[13] Y. Reswan, U. Juhardi, and B. T. Yuliansyah, "Implementasi Kompilasi Algoritma Kriptografi Transposisi Columnar Dan Rsa Untuk Pengamanan Pesan Rahasia," *J. Inform. Upgris*, vol. 4, no. 2, 2019, doi: 10.26877/jiu.v4i2.2812.

[14] Q. Kester, "A hybrid cryptosystem based on Vigenère cipher and columnar transposition cipher," *Int. J. Adv. Technol. Eng. Res.*, vol. 3, no. 1, pp. 141–147, 2013.

[15] J. A. Kusumaningtyas, "Analisa Algoritma Ciphers Transposition : Study Literature," *Multimatrix*, vol. I, no. 1, pp. 1–12, 2018, [Online]. Available: http://jurnal.unw.ac.id:1254/index.php/mm/article/view/152/106.