Jurnal Matematika UNAND
Vol. **12** No. **2** Hal. 168 – 175
ISSN : 2303–291X
e-ISSN : 2721–9410

IMPLEMENTASI ALGORITMA SUPER ENKRIPSI VIGENERE *CIPHER* DAN *ROUTE CIPHER* PADA PENYANDIAN PESAN TEKS

SUSILA BAHRI*, FITRAHUL JIHAN, BUDI RUDIANTO

Departemen Matematika dan Sains Data,
Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Andalas,
Kampus UNAND Limau Manis Padang, Indonesia,
email : susilabahri@sci.unand.ac.id, fitrahuljihan@gmail.com, budirudianto@sci.unand.ac.id

Diterima 18 Januari 2022 Direvisi 21 Januari 2023 Dipublikasikan 21 Oktober 2023

Abstrak. Kemajuan teknologi diiringi dengan meningkatnya ancaman terhadap keamanan serta kerahasiaan informasi pada pesan. Salah satu cara untuk mengamankan pesan dapat menggunakan teknik super enkripsi. Super enkripsi merupakan suatu konsep yang menggunakan kombinasi dari *cipher* substitusi dan *cipher* transposisi untuk meningkatkan keamanan pesan. *Cipher* substitusi adalah metode untuk merubah setiap karakter pesan melalui operasi matematika. *Cipher* transposisi adalah metode untuk merubah susunan setiap karakter pesan. Pada penelitian ini, Vigenere *cipher* sebagai *cipher* substitusi dan *route cipher* sebagai *cipher* transposisi. Penelitian ini bertujuan untuk mengimplementasikan algoritma super enkripsi Vigenere *cipher* dan *route cipher* pada penyandian pesan teks. Penyandian pesan dimulai dengan enkripsi menggunakan persamaan Vigenere *cipher* kemudian dienkripsi kembali menggunakan *route cipher* dengan merubah susunan karakter pesan sesuai rute kunci. Pengembalian pesan atau dekripsi dimulai dengan *route cipher* lalu didekripsi kembali menggunakan Vigenere *cipher*. Proses penyandian dan pengembalian pesan akan diimplementasikan menggunakan bahasa program PHP.

Kata Kunci: Super enkripsi, Vigenere cipher, Route cipher, Enkripsi, Dekripsi

1. Pendahuluan

Kriptografi adalah ilmu tentang teknik matematika yang berhubungan dengan keamanan informasi yang ditujukan untuk menjaga kerahasiaan pesan, integritas data dan autentikasi [1]. Kriptografi merupakan salah satu solusi alternatif untuk keamanan data atau pesan digital, yang dapat menyandikan informasi menjadi bentuk lain [2]. Secara umum, kriptografi terdiri atas dua bagian utama yaitu bagian enkripsi dan bagian dekripsi. Dalam prosesnya, pengirim dan penerima informasi akan menyepakati sebuah kunci untuk melakukan proses enkripsi dan proses dekripsi [3]. Pada proses enkripsi, pengirim mengubah pesan dalam bentuk informasi (*plaintext*) menjadi pesan dengan bentuk lain yang sulit dipahami (*ciphertext*) dengan menggunakan kunci tersebut sedangkan proses dekripsi adalah proses

*Penulis Korespondensi

mengembalikan pesan yang sulit dipahami menjadi informasi yang dipahami dengan suatu kunci [4].

Salah satu jenis kriptografi adalah kriptografi klasik. Kriptografi ini menggunakan teknik penyandian yang sangat sederhana sehingga memiliki tingkat keamanan yang relatif rendah dan mudah dibobol oleh pihak yang tidak bertanggung jawab [5]. Untuk mengatasi masalah ini, maka diperlukan teknik penyandian yang dapat meningkatkan keamanan pesan yaitu teknik Super Enkripsi. Teknik ini merupakan kombinasi dari teknik penyandian substitusi dan teknik penyandian transposisi. Dalam penelitian ini, *Vigenere Cipher* yang merupakan teknik penyandian substitusi dikombinasikan dengan *Route Cipher* yang merupakan teknik penyandian transposisi. Kedua teknik ini dipilih selain dapat melipatgandakan tingkat keamanan pesan, juga relatif mudah diaplikasikan pada komputer [6]. Pada penelitian ini, algoritma super enkripsi *Vigenere Cipher* dan *Route Cipher* akan diimplementasikan menggunakan software atau bahasa pemograman PHP [7,8].

2. Landasan Teori

2.1. *Kriptografi*

Kriptografi merupakan ilmu yang membahas metode pengiriman pesan secara rahasia dalam bentuk tersandi atau tersamar sehingga hanya penerima yang dituju yang dapat membaca pesan [4]. Kriptografi dapat dinyatakan secara matematis sebagaimana definisi berikut. Misalkan P adalah himpunan pesan dan C adalah himpunan *ciphertext*. Fungsi enkripsi E_e merupakan fungsi bijektif:

$$E_e : P \to C, 5$$

dimana $e \in K$ adalah kunci yang menentukan E_e yang sesuai dengan pesan $p \in P$ untuk menghasilkan *ciphertext* $c \in C$. Fungsi deskripsi D_d merupakan fungsi bijektif:

$$D_d : C \to P,$$

yang ditentukan oleh kunci $d \in K$ yang dioperasikan pada *ciphertext* $c \in C$ untuk mendapatkan *plaintext* $D_d(c) = p$. Pengaplikasian E_e terhadap p atau $E_e(p)$ disebut enkripsi atau penyandian $p \in P$, sedangkan pengaplikasian D_d terhadap c atau $D_d(c)$ disebut dekripsi atau penguraian $c \in C$ [3].

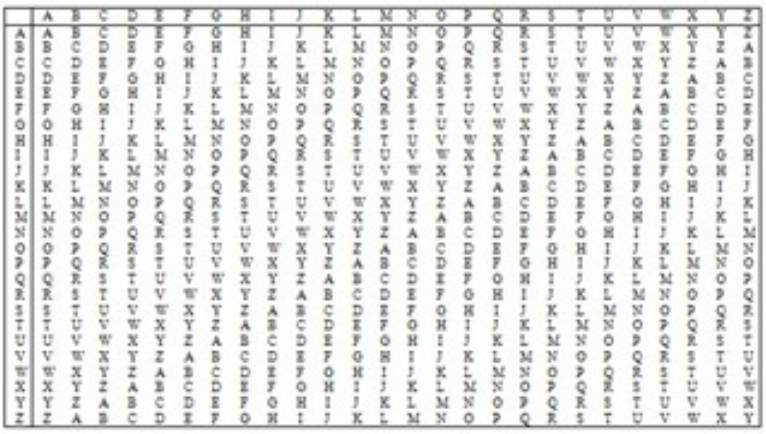
2.2. *Vigenere Cipher*

Vigenere *cipher* adalah *cipher* dengan substitusi polialfabetik yang dilakukan dengan menambahkan setiap indeks karakter *plaintext* ke indeks karakter kunci berdasarkan *Vigenere square* atau *Tablo Vigenere* [9]. Pada Gambar 1 diberikan ilustrasi Vigenere Square.

Proses enkripsi dan dekripsi menggunakan *Vigenere Cipher* dapat dinyatakan berturut-turut sebagai berikut :

$$C_i = E_k(P_i) = (P_i + K_i) \mod 26, \tag{2.1}$$

$$P_i = D_k(C_i) = (C_i - K_i) \mod 26, \tag{2.2}$$



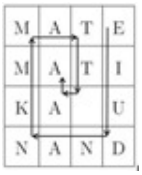
Gambar 1. Vigenere Square

dimana C_i adalah karakter *ciphertext* ke-i, P_i adalah karakter *plaintext* ke-i, dan K_i adalah karakter kunci ke-i. E adalah fungsi enkripsi, dan D adalah fungsi dekripsi [10].

2.3. *Route Cipher*

Pada proses penyandian *Route Cipher*, pesan ditulis ke dalam array kemudian dibaca dalam urutan yang ditentukan oleh rute [11]. Berikut proses penyandian *Route Cipher*.

Plaintext : MATEMATIKA UNAND
Kunci : 4, spiral ke dalam searah jarum jam, dimulai dari kanan atas.



Dari proses penyandian tersebut dihasilkan **EIUDNANKMMATT AA**.

Penulisan *plaintext* dimulai dari kiri ke kanan pada setiap baris, sedangkan cara pembacaan *ciphertext* adalah dengan memutar searah jarum jam dan dimulai dari kanan atas. Pada contoh di atas, angka 4 berarti banyaknya baris dan kolom pada penulisan *plaintext*.

3. Hasil dan Pembahasan

3.1. *Aplikasi Algoritma Vigenere Cipher*

Proses penyandian *Vigenere Cipher* dilakukan dengan mengoperasikan kode pesan dan kode kunci yang didapat dari tabel ASCII [9]. Karena karakter teks (*printable characters*) yang ada pada tabel ASCII terdiri dari 95 karakter, yang dimulai dari nomor 32 sampai 127, maka pesan (*plaintext*) dan kunci yang ditetapkan di awal akan dioperasikan menggunakan beberapa persamaan berikut.

(1) Enkripsi
Dengan menggunakan *Vigenere Cipher*, maka persamaan untuk mengenkripsi pesan menjadi *ciphertext* adalah

$$\begin{aligned} C_i &= ((P_i - 32) + (K_i - 32)) \mod 95 + 32, \\ C_i &= ((P_i + K_i - 64) \mod 95) + 32, \end{aligned} \tag{3.1}$$

dimana C_i adalah karakter *ciphertext* ke-i, P_i adalah karakter *plaintext* ke-i, dan K_i adalah karakter kunci ke-i.

(2) Dekripsi
Persamaan untuk dekripsi *ciphertext* menjadi *plaintext* yaitu:

$$\begin{aligned} P_i &= (((C_i - 32) - (K_i - 32)) \mod 95) + 32, \\ P_i &= ((C_i - 32 - K_i + 32) \mod 95) + 32 \\ P_i &= ((C_i - K_i) \mod 95) + 32, \end{aligned} \tag{3.2}$$

dimana P_i adalah karakter *plaintext* ke-i, C_i adalah karakter *ciphertext* ke-i, dan K_i adalah karakter kunci ke-I [9].

3.2. *Aplikasi Algoritma Route Cipher*

Proses penyandian *Route Cipher* menggunakan kunci searah jarum jam, yaitu dimulai dengan membuat matriks yang berisi karakter *plaintext*, kemudian *ciphertext* dibaca dari sisi kanan atas matriks dan berputar searah jarum jam. Selanjutnya, pada proses dekripsi, matriks diisi dengan karakter *ciphertext* lalu *plaintext* dibaca sesuai dengan rute kunci sehingga diperoleh pesan teks awal sebelum disandikan [12].

3.3. *Aplikasi Algoritma Super Enkripsi Vigenere Cipher dan Route Cipher*

3.3.1. *Proses Enkripsi*

Berikut ini proses enkripsi menggunakan algoritma superenkripsi *Vigenere Cipher* dan *Route Cipher*. Proses enkripsi ini dimulai dengan algoritma *Vigenere Cipher* kemudian dilanjutkan dengan algoritma *Route Cipher*.

(1) *Vigenere Cipher*

(a) Menetapkan *plaintext* dan kunci yang akan diubah.
Plaintext : FITRAHUL JIHAN 1710433004

Kunci *Vigenere* : UAm@th17
Kunci *route* : 5

(b) Mengubah pesan dan kunci menjadi karakter ASCII. Berikut adalah hasil substitusi ke dalam bentuk ASCII.
- Pesan text

P_i	F	I	T	R	A	H	U	L		J	I	H	A
ASCII	65	70	73	84	82	65	72	85	76	32	74	73	72
P_i	N		1	7	1	0	4	3	3	0	0	4	
ASCII	78	32	49	55	49	48	52	51	51	48	48	52	

- Kunci Kunci berulang sebanyak karakter pesan.

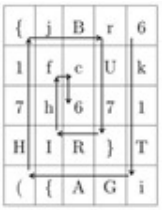
K_i	U	A	m	@	t	h	1	7
ASCII	85	65	109	64	116	104	49	55

(c) Mengubah karakter pesan menjadi bentuk lain menggunakan persamaan (3.1), sehingga diperoleh hasil $\{jBr61fcUk7h671HIR\}T(\{AGi.$

(2) *Route Cipher*

(a) Membuat matriks dengan jumlah baris dan kolom sebanyak kunci yaitu 4. Matriks tersebut diisi dengan hasil enkripsi sebelumnya.

(b) Membaca *ciphertext* dimulai dari kanan atas lalu melingkar searah jarum jam.



Akibatnya, pada proses enkripsi yang menggunakan algoritma super enkripsi ini diperoleh $6k1TiGA\{(H71\{jBrU7\}RIhfc6$

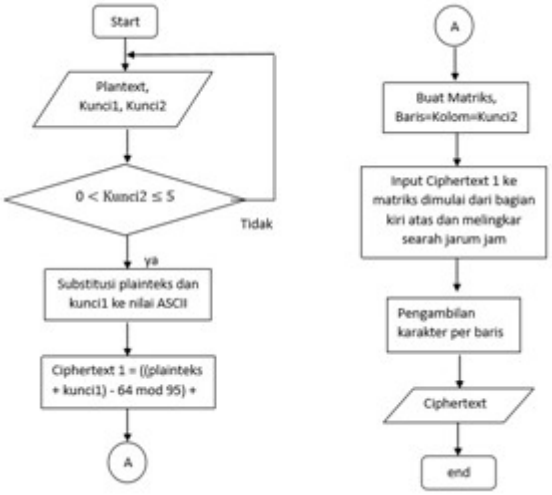
3.3.2. *Proses Dekripsi*

Proses dekripsi dimulai dengan algoritma *route cipher* dan kemudian dilanjutkan dengan algoritma *Vigenere Cipher*. Proses ini mengubah hasil enkripsi sebelumnya menjadi pesan asal dengan algoritma yang sama seperti proses enkripsi [10].

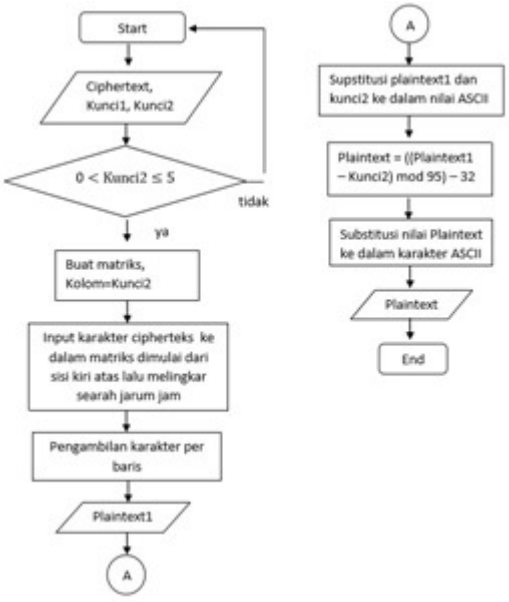
3.4. *Implementasi Super Enkripsi Vigenere Cipher dan Route Cipher Menggunakan PHP*

Berikut ini adalah *flowchart* dari algoritma super enkripsi *vigenere cipher* dan *route cipher* yang telah dibahas sebelumnya.

(1) *Flowchart* Enkripsi.

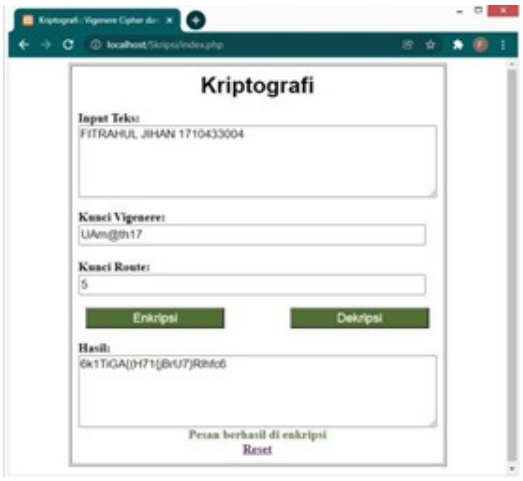


(2) *Flowchart* Dekripsi.



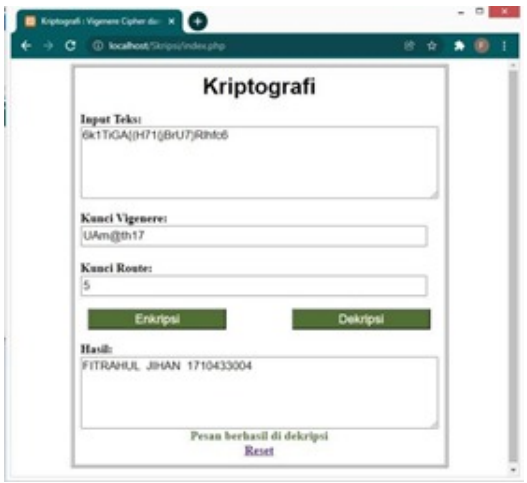
Berikut adalah hasil implementasi enkripsi dan dekripsi dengan menggunakan software dan Bahasa program PHP.

(1) Hasil Enkripsi.



Gambar 2. Form HTML dengan Hasil Enkripsi

(2) Hasil Dekripsi.



Gambar 3. Form HTML dengan Hasil Dekrpsi

4. Kesimpulan

Secara umum, proses penyandian pesan dengan algoritma super enkripsi *Vigenere cipher* dan *route cipher* dapat dilakukan dengan menggunakan persamaan *Vigenere cipher* yaitu $C_i = ((P_i + K_i - 64) \mod 95) + 32$. Kemudian hasil enkripsi tersebut dienkripsi atau disandikan kembali menggunakan *Route cipher* dengan metode pembacaan karakter searah jarum jam. Selanjutnya untuk proses dekripsi atau pengembalian pesan, dilakukan dengan menggunakan *Route cipher* yang kemudian didekripsikan kembali menggunakan *Vigenere cipher* dengan persamaan $P_i = ((C_i - P_i) \mod 95) + 32$. Selanjutnya, proses penyandian dan pengiriman pesan ini menjadi mudah dilakukan dengan menggunakan software PHP yang telah dikonstruksi.

Daftar Pustaka

[1] Hananto, A. L., Solehudin, A., Irawan, A. S. Y., Priyatna, B., 2019, Analyzing the Kasiski method against Vigenere cipher, *arXiv preprint arXiv:1912.04519*

[2] Ariyus, D., 2008, *Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi*, Yogyakarta: C.V Andi Offset

[3] Mollin, R.A., 2006, *An Introduction to Cryptography*, 2^{nd} ed., New York: Chapman and Hall

[4] Saputra, I., Hasibuan, N. A., Rahim, R., 2017, Vigenere cipher algorithm with grayscale image key generator for secure text file. *International Journal of Engineering Research and Technology (IJERT)*, **6**(1): 266–269

[5] Serge, V. 2006. *A Classical Introduction to Cryptography Applications for Communications Security.* Springer Science Business Media, Inc

[6] Kusumaningtyas, J. A., 2018, Analisa Algoritma Cipher Transposition: Study Literature Multimatrix, *Jurnal Ilmu Komputer Universitas Ngudi Waluyu* Vol. **1**(1): 1–12

[7] Solichin, A., 2005, *Pemograman Web dengan PHP dan MySQL*, Jakarta: Universitas Budi Luhur

[8] Niaga Hoster, 2020, Pengertian PHP, Fungsi dan Sintaks Dasarnya, diakses melalui *http://niaga.hoster.co.id* pada 19 Agustus 2021

[9] Aliyu, A.M.,2016, Vigenere Cipher: Trends, Review, and Possible Modifications, *International Journal of Computer Applications* Vol. **135**(11): 09758887

[10] Soofi, A. A., Riaz, I., Rasheed, U., 2016, An enhanced vigenere cipher for data security. *Int. J. Sci. Technol. Res*, **5**(3): 141 – 145

[11] Stephens, R., 2013, *Essential Algorithms: A Practical Approach to Computer Algorithms*, New York: Wiley

[12] Irdayani, I., 2019, Keamanan Citra Menggunakan Algoritma Route Chiper, *Informasi dan Teknologi Ilmiah (INTI)* Vol. **6**(2): 246 – 249