Jurnal Riset Mahasiswa Matematika
Volume 2(5) (2023), Pages 173-185
p-ISSN: 2808-1552; e-ISSN: 2808-4926

Modifikasi Vigenere Cipher Menggunakan Grup Simetri untuk Mengamankan Pesan Teks

Niken Dwi Cahyanti*, Turmudi, Muhammad Khudzaifah

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

cahyanti40@gmail.com*, turmudi_msi@mat.uin-malang.ac.id, khudzaifah@uin-malang.ac.id

Abstrak

Kriptografi banyak digunakan untuk mengatasi masalah keamanan informasi yang mengalami pertukaran pada jaringan internet. Salah satu algoritma dalam kriptografi adalah Vigenere Cipher, algoritma tersebut terkenal sebagai metode yang tangguh dan tidak mudah dipecahkan. Namun, algoritma Vigenere Cipher memiliki kelemahan yaitu kuncinya yang pendek dan digunakan berulang-ulang. Oleh karena itu, perlu dilakukan modifikasi terhadap Vigenere Cipher. Tujuan penelitian ini yaitu untuk mengetahui modifikasi Vigenere Cipher menggunakan grup simetri dan juga untuk mengetahui tingkat keamanan hasil enkripsi modifikasi Vigenere Cipher jika dibandingkan dengan Vigenere Cipher. Hasil yang diperoleh dari penelitian ini adalah suatu algoritma baru dari proses modifikasi Vigenere Cipher menggunakan grup simetri. Algoritma modifikasi Vigenere Cipher terbukti lebih kuat jika dibandingkan dengan Vigenere Cipher. Hal tersebut dikarenakan *plaintext* diacak terlebih dahulu menggunakan penyandian grup simetri, sehingga *plaintext* yang sebenarnya aman terhadap serangan metode Kasiski dan *exhaustive key search*. Selain itu, algoritma baru yang dihasilkan juga mendukung penggunaan huruf kapital, huruf kecil, angka, dan simbol.

Kata Kunci: Modifikasi; Vigenere Cipher; Grup Simetri

Abstract

Cryptography is widely used to overcome information security problems that are exchanged on the internet network. One of the algorithms in cryptography is the Vigenere Cipher, the algorithm is known as a robust method and is not easily solved. However, the Vigenere Cipher algorithm has a weakness, namely the key is short and is used repeatedly. Therefore, it is necessary to modify the Vigenere Cipher. The purpose of this study is to determine the modification of the Vigenere Cipher using a symmetric group and also to determine the level of security of the encryption results of Vigenere Cipher modification when compared to the Vigenere Cipher. The results obtained from this research is a new algorithm of the modification process of the Vigenere Cipher using symmetric groups. The modified Vigenere Cipher algorithm is proven to be stronger than the Vigenere Cipher. This is because the plaintext is scrambled first using a symmetric group encoding, so that the actual plaintext is safe against attacks by the Kasiski method and exhaustive key search. In addition, the resulting new algorithm also supports the use of capital letters, lowercase letters, numbers, and symbols.

Keywords: Modification; Vigenere Cipher; Symmetric Group

PENDAHULUAN

Semakin pesatnya perkembangan teknologi informasi pada zaman sekarang, semakin banyak pula tindakan kejahatan penyalahgunaan informasi melalui jaringan internet. Hal tersebut dapat terjadi karena jaringan internet sering kali digunakan untuk proses pertukaran informasi. Oleh sebab itu, diperlukan peningkatan keamanan terhadap kerahasiaan suatu informasi yang mengalami pertukaran pada jaringan internet. Salah satu informasi yang sering dipertukarkan yaitu data atau pesan dalam bentuk teks. Menjaga keamanan data dapat dilakukan menggunakan metode penyandian. Teknik menyandikan pesan teks digunakan dengan tujuan

Submitted: 6 Juli 2022 Reviewed: 20 Mei 2023 Accepted: 26 Juni 2023
Doi: http://dx.doi.org/10.18860/jrmm.v2i5.16791

supaya isi pesan tidak diketahui oleh orang yang tidak berwenang. Pesan rahasia tersebut sama halnya dengan amanat yang harus disampaikan kepada yang berhak menerimanya.

Menjaga keamanan informasi menjadi hal yang harus diperhatikan. Kriptografi sebagai salah satu metode pengamanan data untuk meminimalisir banyaknya tindak kejahatan penyalahgunaan informasi yang bersifat penting dan rahasia [1]. Kriptografi adalah seni dan ilmu yang digunakan untuk mengamankan pesan yang dikirim oleh pengirim dari suatu tempat ke tempat penerima, agar tidak jatuh ke tangan pihak yang tidak berwenang [2]. Menjaga keamanan menggunakan kriptografi, terdapat proses penyandian pesan yang disebut enkripsi yaitu dengan melakukan perubahan teks asli (*plaintext*) ke dalam bentuk teks sandi (*ciphertext*) dengan menggunakan suatu algoritma. Sedangkan proses untuk mengembalikan *ciphertext* ke dalam bentuk *plaintext* disebut dekripsi [3].

Proses enkripsi dan dekripsi membutuhkan suatu protokol perjanjian kunci yaitu kesepakatan mengenai kunci rahasia yang dilakukan oleh pihak pengirim dan pihak penerima pesan sehingga kedua belah pihak dapat menyepakati suatu kunci rahasia yang sama. Penelitian Stickel (2005) memperkenalkan algoritma protokol perjanjian kunci yang didasarkan pada grup non-komutatif. Salah satu contoh grup non-komutatif yang dapat digunakan pada protokol perjanjian kunci Stickel yaitu grup simetri-n. Penelitian dengan menerapkan grup simetri-n pada algoritma pembentukan kunci telah dilakukan sebelumnya oleh Wasiatun Rizkiyah (2016). Penelitian tersebut melakukan proses enkripsi dan dekripsi menggunakan teknik transposisi dengan kunci yang telah terbentuk melalui proses pembentukan kunci atas grup simetri-n.

Vigenere Cipher termasuk di dalam jenis algoritma kriptografi klasik yang juga algoritma simetris artinya pada proses penyandiannya digunakan kunci yang sama. Vigenere Cipher dulunya terkenal sebagai metode yang tangguh dan sulit dipecahkan, hingga akhirnya dapat dipecahkan menggunakan metode friedman dan kasiski [4]. Kedua metode tersebut dapat digunakan oleh seorang kriptanalis untuk mengetahui panjangnya kunci yang dipakai pada Vigenere Cipher. Setelah panjang kunci diketahui, maka kunci bisa ditemukan dengan metode *exhaustive key search* atau analisis frekuensi [5]. Selain itu, Vigenere Cipher memiliki kelemahan yaitu kuncinya yang pendek dan digunakan berulang-ulang [6]. Oleh sebab itu, sangat perlu melakukan modifikasi pada Vigenere Cipher untuk membuat keamanan lebih kuat dan tidak mudah dipecahkan.

Penelitian memodifikasi Vigenere Cipher sudah pernah dilakukan sebelumnya oleh Octavianingrum, Siambaton, & Dewi (2018). Penelitian tersebut memodifikasi Vigenere Cipher dengan pembuatan kunci geser dan teknik enkripsi blok pada proses enkripsinya. Penelitian lain juga dilakukan oleh Widarma, Siregar, & Irawan (2019). Penelitian tersebut menggabungkan Vigenere Cipher dan *Electronic Code Book* (ECB) untuk meningkatkan keamanan. Kedua penelitian tersebut menghasilkan algoritma baru yang lebih aman jika dibandingkan dengan Vigenere Cipher biasa. Akan tetapi, kedua penelitian tersebut hanya dapat mengenkripsi *plaintext* berupa huruf kapital saja. Karakter huruf kecil, angka dan simbol belum dibahas pada kedua penelitian tersebut.

Berbeda dengan penelitian Latifah, Ambo, dan Kurnia (2017) yang memodifikasi Caesar Cipher dan Reilfence Cipher. Penelitian tersebut memodikasi algoritma Caesar Cipher dengan menggunakan ASCII *printable characters* dan modulus 95. Penelitian tersebut juga melakukan perubahan pada rumus enkripsi dan dekripsi pada Caesar Cipher serta menggabungkan Caesar Cipher dengan algoritma lain. Penelitian tersebut menghasilkan algoritma baru yang lebih kuat dibandingkan Caesar Cipher biasa dan mampu mengenkripsi huruf kapital, huruf kecil, simbol dan angka. Caesar Cipher dan Vigenere Cipher memiliki rumus enkripsi dan dekripsi yang sama, walaupun memiliki perbedaan pada kuncinya baik Caesar Cipher maupun Vigenere Cipher kunci yang digunakan selalu dalam lingkup yang sama. Oleh karena itu, pada penelitian ini akan digunakan ASCII *printable characters* untuk menutupi kekurangan dari kedua penelitian sebelumnya.

Penelitian ini memodifikasi Vigenere Cipher menggunakan grup simetri untuk mengamankan pesan teks. Penyandian grup simetri digunakan untuk mengacak *plaintext* sebelum dioperasikan dengan kunci Vigenere Cipher. Hal tersebut bertujuan untuk menyembunyikan *plaintext* yang sebenarnya. Penelitian ini diharapkan mampu meningkatkan

keamanan pada algoritma Vigenere Cipher, sehingga menghasilkan algoritma baru yang lebih aman jika dibandingkan dengan Vigenere Cipher biasa.

METODE

Tahapan Penelitian

Secara umum tahapan penelitian yang dilakukan dalam penelitian ini yaitu:

1. Memaparkan teknik penyandian Vigenere Cipher sebelum dimodifikasi dan memaparkan modifikasi Vigenere Cipher menggunakan grup simetri.
2. Menyusun algoritma penyandian modifikasi Vigenere Cipher menggunakn grup simetri S_n dan penerapannya menggunakan grup simetri S_5
   a) Proses enkripsi menggunakan modifikasi Vigenere Cipher yaitu sebagai berikut:
      1) Setelah menentukan *plaintext* dapat dilakukan pembentukan kunci dengan algoritma protokol perjanjian kunci Stickel atas grup simetri
      2) Membagi *plaintext* menjadi blok-blok
      3) Mengenkripsi *plaintext* dengan kunci grup siemtri menggunakan teknik transposisi (permutasi) dan menghasilkan *ciphertext1*.
      4) Menentukan kunci grup simetri
      5) Mengkonversi *ciphertext1* dan kunci Vigenere Cipher ke dalam bentuk angka berdasarkan ASCII *printable characters*.
      6) *Ciphertext1* dan kunci Vigenere Cipher disubtitusikan ke dalam persamaan enkripsi Vigenere Cipher yang telah dimodifikasi dengan memanfaatkan ASCII *printable characters*.
      7) Hasil perhitungan pada *step* 6 dikembalikan dalam bentuk karakter berdasarkan ASCII *printable characters*, sehingga diperoleh *ciphertext* akhir.
   b) Proses dekripsi menggunakan modifikasi Vigenere Cipher yaitu sebagai berikut:
      1) Mengkonversi *ciphertext* akhir dan kunci Vigenere Cipher ke dalam bentuk angka berdasarkan ASCII *printable characters*.
      2) *Ciphertext* akhir dan kunci Vigenere Cipher disubtitusikan ke dalam persamaan dekripsi Vigenere Cipher yang telah dimodifikasi dengan memanfaatkan ASCII *printable characters*.
      3) Hasil perhitungan pada *step* 2 dikembalikan dalam bentuk karakter berdasarkan ASCII *printable characters*, sehingga diperoleh *ciphertext1*.
      4) Menginvers kunci grup simetri
      5) Membagi *ciphertext1* menjadi blok-blok
      6) Melakukan dekripsi *ciphertext1* dengan kunci grup simetri menggunakan teknik transposisi permutasi dan menghasilkan *plaintext*.
3. Melakukan uji kriptanalisis pada enkripsi modifikasi Vigenere Cipher kemudian dibandingkan dengan Vigenere Cipher.

HASIL DAN PEMBAHASAN

1. Algoritma Vigenere Cipher Sebelum Dimodifikasi

Algoritma dari proses enkripsi dan dekripsi menggunakan Vigenere Cipher sebelum dimodifikasi yaitu sebagai berikut:

1) Setelah menentukan *plaintext* dan kunci, selanjutnya mengkonversi karakter huruf alfabet pada *plaintext* dan kunci ke dalam bentuk angka.
2) Subtitusikan *plaintext* dan kunci ke dalam persamaan (2.2)

$$C_i = (P_i + K_r)\ mod\ 26$$

(Catatan: apabila kunci kurang dari *plaintext* maka kunci akan diulang hingga seluruh *plaintext* tersebut terpenuhi. Apabila kunci melebihi *plaintext*, maka kunci akan ditulis sesuai dengan panjang *plaintext* yang diperlukan)

3) Mengembalikan hasil perhitungan pada *step* 2 ke dalam bentuk huruf alfabet, sehingga diperoleh *ciphertext*.

Sedangkan tahapan dari proses dekripsi menggunakan Vigenere cipher yaitu sebagai berikut:

1) Mengkonversi karakter huruf alfabet pada *ciphertext* dan kunci ke dalam bentuk angka
2) Subtitusikan *ciphertext* dan kunci ke dalam persamaan (2.3)

$$P_i = (C_i - K_r)\ mod\ 26$$

3) Mengembalikan hasil perhitungan pada *step* 2 ke dalam bentuk huruf alfabet, sehingga diperoleh *plaintext* kembali.

Contoh : misalkan *plaintext* adalah `AS THE FORECAST BECAME MORE CERTAIN ACROSS THE WEEKEND THE GRAPICHS WERE USED EXTENSIVELY AS THE EXTENT OF THE SNOW FALL` dan kuncinya adalah `EASY`. Maka hasil enkripsinya adalah sebagai berikut:

Plaintext :	ASTHEFORECASTBECAMEMORECERTAINACROSSTHEWEEKENDTHEGRAPICHSWEREUSEDEXTENSIVELYASTHEEXTENTOFTHESNOWFALL
Kunci :	EASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASYEASY
Ciphertext :	ESLFIFGPICSQXBWAEMWKSRWAIRLYMNSAVOKQXHWUIECCRDLFIGJYTHAAWWWPIUKCH EPRINKGZEDWESLFIEPRINIMJTZCWNGUJADJ

2. Kelemahan Vigenere Cipher

Kelemahan Vigenere Cipher yaitu kuncinya yang pendek dan digunakan secara berulang-ulang. Kelemahan ini dapat dimanfaatkan untuk memecahkan Vigenere Cipher. Adapun metode yang digunakan yaitu metode Kasiski untuk menentukan panjang kunci yang digunakan. Selanjutnya kriptanalisis dapat dilakukan menggunakan metode analisis frekuensi atau secara *exhaustive key search*.

Contoh kriptanalisis Vigenere Cipher: Misalkan diberikan *ciphertext* yang diperoleh dari contoh penyandian Vigenere Cipher sebelumnya adalah

ES**LFI**FGPICSQXBWAEMWKSRWAIRLYMNSAVOKQXHWUIECCRD**LFI**GJYTHAAWWWPIUKCH**EP RIN**KGZEDWES**LFIEPRIN**IMJTZCWNGUJADJ

Terdapat kriptogram yang berulang yaitu **LFI** dan **EPRIN**. Jarak antara dua buah **LFI** yang berurutan adalah sebagai berikut:

Jarak **LFI** ke-1 dengan **LFI** ke-2 = 44
Jarak **LFI** ke-2 dengan **LFI** ke-3 = 32
Jarak antara dua buah perulangan **EPRIN** adalah 16

Faktor pembagi 44 adalah { 2, 4, 11, 44 }, faktor pembagi 32 adalah {2, 4, 8, 16, 32}, dan faktor pembagi 16 adalah { 2, 4, 8,16 }, irisan dari ketiga himpunan ini adalah 2 dan 4. Jadi, dapat diperkirakan panjang kunci yang digunakan adalah 2 atau 4. Kita asumsikan terlebih dahulu panjang kunci adalah 4 huruf (tanpa mengabaikan kemungkinan panjang kuncinya 2). Kemudian untuk menentukan kemungkinan karakter kunci digunakan analisis frekuensi. Langkah awal yang dilakukan yaitu mengelompokan *ciphertext* menjadi empat bagian berdasarkan karakter kunci ke-1, kunci ke-2, kunci ke-3, kunci-4.

Tabel 1. Pengelompokkan *Ciphertext*

Kelompok	*Ciphertext*	Huruf Paling Sering Muncul
1	EIIXESIMVXIRITWIHIZEIIJWJ	I
2	SFCBMRRNOHEDGHWUENESENTNA	E
3	LGSWWWLSKWCLJAWKPKDLPIZGD	W, L
4	FPQAKAYAQUCFYAPCRGWFRMCUJ	A

Diketahui bahwa 10 huruf yang paling sering muncul dalam Bahasa Inggris adalah E, T, A, O, I, N, S, H, R, D, L, dan trigram yang paling sering muncul adalah THE. Karena kriptogram LFI paling sering muncul di dalam *ciphertext*, maka dari 10 huruf tersebut kemungkinan kata 3-huruf dibentuk dan kita dapat menerka LFI adalah THE. Berdasarkan hal tersebut dapat dibuat tabel yang memetakan karakter *plaintext* dengan *ciphertext*, kemudian menentukan karakter kuncinya.

Tabel 2. Penerkaan Karakter Kunci

Kelompok	Huruf Plainteks	Huruf Cipherteks	Kunci
1	E	I	E
2	*	*	*
3	T	L	S
4	H	F	Y

Selanjutnya dilakukan penerkaan untuk karakter kunci lainnya yang belum diketahui (*). **Tabel 1** memperlihatkan bahwa pada kelompok 2 huruf paling sering muncul adalah huruf E. Sedangkan pada frekuensi kemunculan huruf paling tinggi dalam Bahasa Inggris adalah huruf E. Asumsikan bahwa setiap karakter huruf E pada *plaintext* dienkripsi menjadi huruf E. Sehingga kemungkinan besar kunci yang belum diketahui adalah huruf A. Jadi, kuncinya mungkin EASY. Lakukan dekripsi menggunakan kunci tersebut untuk memastikan apakah kunci EASY merupakan kunci yang benar, dan periksa apakah hasil dekripsi merupakan pesan bermakna. Setelah dilakukan dekripsi diperoleh pesan sebagai berikut:
AS THE FORECAST BECAME MORE CERTAIN ACROSS THE WEEKEND THE GRAPICHS WERE USED EXTENSIVELY AS THE EXTENT OF THE SNOW FALL
Ternyata benar bahwa EASY adalah kunci yang digunakan.

3. Modifikasi Vigenere Cipher Menggunakan Grup Simetri

Modifikasi Vigenere Cipher yang dilakukan yaitu dengan tidak membuang spasi pada *plaintext* dan mengacak *plaintext* terlebih dahulu menggunakan penyandian grup simetri S_n sebelum dioperasikan dengan kunci Vigenere Cipher. Selain itu, digunakan ASCII *printable characters* yang bertujuan agar algoritma Vigenere Cipher mendukung penggunaan huruf kapital, huruf kecil, angka dan simbol.

Pembuktian penyandian grup simetri :

Teknik penyandian grup simetri yaitu penyandian pesan yang perhitungannya menggunakan grup simetri dalam pembentukan kunci, sedangkan untuk proses enkripsi dan dekripsinya digunakan teknik transposisi (permutasi). Teknik transposisi yaitu dengan melakukan permutasi k terhadap *plaintext*, sedangkan untuk dekripsinya dilakukan dengan invers permutasi k^{-1} terhadap *ciphertext*. Maka akan dibuktikan bahwa *plaintext* yang dienkripsi menggunakan teknik transposisi (permutasi) akan menghasilkan *ciphertext* yang apabila didekripsi akan kembali ke *plaintext*.

Misalkan permutasi k: $\Omega \to \Omega$ dituliskan sebagai berikut

$$\begin{pmatrix} 1 & 2 & 3 & \dots & n \\ a(1) & a(2) & a(3) & \dots & a(n) \end{pmatrix}$$

Baris pertama pada permutasi k berisi semua anggota domain Ω sementara baris kedua berisi $a(i)$ anggota kodomain Ω, untuk semua $i \in \Omega$. Permutasi k memetakan $1 \mapsto a(1), 2 \mapsto a(2), 3 \mapsto a(3), \dots, n \mapsto a(n)$.

Berdasarkan **Definisi Permutasi** Permutasi dari suatu himpunan Ω adalah suatu fungsi dari Ω ke Ω yang satu-satu dan pada (bijektif). Sehingga setiap anggota himpunan Ω selalu memiliki pasangan tepat satu di himpunan Ω. Misalkan masing-masing karakter pada *plaintext* merupakan anggota dari domain Ω, maka karakter *ciphertext* merupakan anggota kodomain himpunan Ω. Dapat disimpulkan bahwa *ciphertext* yang dihasilkan dari proses enkripsi merupakan perubahan posisi dari *plaintext* berdasarkan pemetaan dari Ω ke Ω.

Fungsi invers adalah sebuah fungsi yang berkebalikan dari fungsi aslinya. Berdasarkan **Definisi Fungsi Invers** jika suatu fungsi bijektif maka fungsi tersebut memiliki invers. Karena permutasi merupakan fungsi bijektif maka permutasi memiliki invers. Perhatikan kembali

permutasi k, permutasi yang memetakan $1 \leftrightarrow a(1), 2 \leftrightarrow a(2), 3 \leftrightarrow a(3), \dots, n \leftrightarrow a(n)$ disebut invers permutasi k dan dapat dinotasikan dengan permutasi k^{-1}. Dengan kata lain, enkripsi dilakukan dengan permutasi k terhadap *plaintext*, sedangkan dekripsi dilakukan dengan invers permutasi k^{-1} pada *ciphertext*.
Perhatikan bahwa,
Permutasi k = kunci (K)
Invers permutasi k^{-1} = invers kunci (K^{-1})
Misalkan kunci K dari himpunan $\{P_1, P_2, P_3, P_4\}$ dengan menetapkan
$K(P_1) = P_2, K(P_2) = P_4, K(P_3) = P_1, K(P_4) = P_3$ atau dapat dituliskan dalam bentuk sebagai berikut:

$$K = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \\ K(P_1) & K(P_2) & K(P_3) & K(P_4) \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \\ P_2 & P_4 & P_1 & P_3 \end{pmatrix}$$

dan kunci invers K^{-1} dari himpunan $\{C_1, C_2, C_3, C_4\}$, dimana $\{C_1, C_2, C_3, C_4\} = \{P_1, P_2, P_3, P_4\}$, kedua himpunan tersebut sama tetapi memiliki urutan elemen yang berbeda. Sehingga,
$K^{-1}(C_1) = C_3,\ K^{-1}(C_2) = C_1,\ K^{-1}(C_3) = C_4,\ K^{-1}(C_4) = C_2$, atau bisa ditulis menjadi

$$K^{-1} = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 \\ C_3 & C_1 & C_4 & C_2 \end{pmatrix}$$

keterangan P_i = karakter *plaintext* ke – i, , untuk $i = 1,2,3,4$
C_i = karakter *ciphertext* ke – i, untuk $i = 1,2,3,4$
Misalkan diberikan *plaintext* = COBA, maka

$$K = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \\ P_2 & P_4 & P_1 & P_3 \end{pmatrix} = \begin{pmatrix} P_1 & P_2 & P_3 & P_4 \\ C & O & B & A \\ P_2 & P_4 & P_1 & P_3 \\ O & A & C & B \end{pmatrix}$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$
$$C_1 \quad C_2 \quad C_3 \quad C_4$$

Sehingga diperoleh *ciphertext* = OACB

$$K^{-1} = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 \\ C_3 & C_1 & C_4 & C_2 \end{pmatrix} = \begin{pmatrix} C_1 & C_2 & C_3 & C_4 \\ O & A & C & B \\ C_3 & C_1 & C_4 & C_2 \\ C & O & B & A \end{pmatrix}$$

$$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$$
$$P_1 \quad P_2 \quad P_3 \quad P_4$$

Sehingga teks sandi (*ciphertext*) kembali ke bentuk *plaintext* = COBA
Jadi terbukti bahwa *plaintext* yang dienkripsi menggunakan teknik transposisi (permutasi) akan menghasilkan *ciphertext* yang apabila didekripsi akan kembali ke *plaintext*.

Pembuktian penyandian Vigenere Cipher yang Memanfaatkan ASCII *Printable Characters* :

Berikut adalah persamaan untuk enkripsi pesan menggunakan algoritma Vigenere Cipher yang memanfaatkan *ASCII printable characters*:

$$C_i = \big((P_i - 32 + K_r)\ mod\ 95\big) + 32 \qquad (4.1)$$

Sedangkan untuk proses dekripsi dapat menggunakan persamaan berikut:

$$P_i = \big((C_i - 32 - K_r)\ mod\ 95\big) + 32 \qquad (4.2)$$

Keterangan:
C_i = *ciphertext* ke- i
P_i = *plaintext* ke- i
K_r = kunci ke – r
32 = karakter spasi pada tabel ASCII.

Karakter dalam ASCII *printable characters* yaitu dari karakter dengan angka desimal 32 sampai 126, yang seluruhnya berjumlah 95 karakter. Sehingga digunakan modulus 95. Sedangkan penambahan 32 dilakukan supaya nilai C_i kembali berada di interval 32-126.

Pembuktian untuk persamaan (4.1) dan (4.2) dapat dilakukan dengan mengembalikan rumus enkripsi ke rumus dekripsi dan sebaliknya, sehingga:

$C_i = \big((P_i - 32 + K_r)\ mod\ 95\big) + 32$
$(C_i - 32) = (P_i - 32 + K_r)\ mod\ 95$ ... ... 32 dipindah ruas
$95|(C_i - 32) - (P_i - 32 + K_r)$ ... ... sesuai definisi kongruensi
$(C_i - 32) - (P_i - 32 + K_r) = 95.k$ ... ... berdasarkan definisi keterbagian
$C_i - 32 - P_i + 32 - K_r = 95.k$ ... ... sifat distributif
$-C_i + 32 + P_i - 32 + K_r = 95.(-k)$ ... ...dikalikan (-1)
$(P_i - 32) - (C_i - 32 - K_r) = 95.(-k)$ ... ... Sifat distributif
$95|(P_i - 32) - (C_i - 32 - K_r)$ ... ... Berdasarkan definisi keterbagian
$(P_i - 32) = (C_i - 32 - K_r)\ mod\ 95$ ... . berdasarkan definisi kongruensi
$P_i = \big((C_i - 32 - K_r)\ mod\ 95\big) + 32$ ... ... 32 dipindah ruas

Sedangkan pembuktian rumus dekripsi, yaitu mengembalikan persamaan (4.2) ke persamaan (4.1) adalah sebagai berikut:

$P_i = \big((C_i - 32 - K_r)\ mod\ 95\big) + 32$
$(P_i - 32) = (C_i - 32 - K_r)\ mod\ 95$ ... ... 32 dipindah ruas
$95|(\ P_i - 32) - (C_i - 32 - K_r)$ ... ... sesuai definisi kongruensi
$(P_i - 32) - (C_i - 32 - K_r) = 95.(-k)$ ... ... sesuai defensisi keterbagian
$P_i - 32 - C_i + 32 + K_r = 95.(-k)$ ... ... Sifat distributif
$-P_i + 32 + C_i - 32 - K_r = 95.(k)$ ... ... dikalikan (-1)
$(C_i - 32) - (P_i - 32 + K_r) = 95.(k)$ ... ... sifat distributif
$95|(C_i - 32) - (P_i - 32 + K_r)$ ... ... sesuai definisi keterbagian
$(C_i - 32) = (P_i - 32 + K_r)\ mod\ 95$ ... ... sesuai definisi kongruensi
$C_i = \big((P_i - 32 + K_r)\ mod\ 95\big) + 32$

Jadi terbukti bahwa persamaan (4.1) dan (4.2) dapat digunakan untuk proses enkripsi dan dekripsi Vigenere Cipher berdasarkan ASCII *printable characters*.

4. Teknik Penyandian Modifikasi Vigenere Cipher Menggunakan Grup Simetri S_n

Grup simetri S_n merupakan salah satu grup non-komutatif yang dapat digunakan pada protokol perjajian kunci Stickel. Cara menentukan S_n yang digunakan untuk pembentukan kunci grup simetri yaitu pilih sebarang n, dengan $n \geq 3$ (karena S_n yang digunakan haruslah tidak komutatif) dan n kurang dari atau sama dengan banyaknya *plaintext*.

A. Proses enkripsi:

Setelah menentukan *plaintext* dapat dilakukan proses enkripsi menggunakan algoritma modifikasi Vigenere Cipher sebagai berikut ini:

1. Pembentukan kunci grup simetri.

   Berikut proses pembentukan kunci yang dimulai dengan pihak pengirim dan penerima pesan menyepakati dua elemen dari grup simetri S_n yaitu:

   pilih σ_1 dan σ_2 adalah elemen dari S_n, dengan $\sigma_1 \circ \sigma_2 \neq I$ (I adalah permutasi identitas) dan $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$, sedemikian hingga $K \neq I$ (K adalah kunci grup simetri).

$$\sigma_1 = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma_1(a_1) & \sigma_1(a_2) & \dots & \sigma_1(a_n) \end{pmatrix}$$
$$\sigma_2 = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ \sigma_2(a_1) & \sigma_2(a_2) & \dots & \sigma_2(a_n) \end{pmatrix}$$

   Kemudian tentukan R yang merupakan orde dari σ_1 dan S adalah orde dari σ_2.

   (i) Pengirim pesan memilih bilangan asli $M < R$ dan $N < S$ dan mengirim
   $r = {\sigma_1}^M \circ {\sigma_2}^N$

   (ii) Penerima pesan memilih bilangan asli $P < R$, $Q < S$ dan mengirim
   $s = {\sigma_1}^P \circ {\sigma_2}^Q$

(iii) Pengirim pesan menerima s dari pihak penerima
(iv) Penerima pesan menerima r dari pihak pengirim
(v) Pengirim pesan menghitung
$K_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$
(vi) Penerima pesan menghitung
$K_2 = {\sigma_1}^P \circ r \circ {\sigma_2}^Q$

Sehingga dapat diperoleh kunci rahasia yang telah disepakati oleh kedua pihak yaitu

$$\begin{aligned} K_1 &= {\sigma_1}^M \circ s \circ {\sigma_2}^N \\ &= {\sigma_1}^M \circ {\sigma_1}^P \circ {\sigma_2}^Q \circ {\sigma_2}^N \\ &= {\sigma_1}^{M+P} \circ {\sigma_2}^{Q+N} \\ &= {\sigma_1}^P \circ {\sigma_1}^M \circ {\sigma_2}^N \circ {\sigma_2}^Q \\ &= {\sigma_1}^P r {\sigma_2}^Q \\ &= K_2 \end{aligned}$$

Jadi, $K = K_1 = K_2$

2. Membagi *plaintext* menjadi blok-blok. Setiap bloknya berisi karakter sebanyak n, dan apabila terdapat karakter spasi pada *plaintext* maka spasinya tidak dihilangkan karena merupakan salah satu karakter dalam Tabel ASCII *printable characters*. Sehingga karakter spasi dapat dituliskan dengan sp. Sedangkan untuk kekurangan pada blok dapat ditambahkan dengan karakter yang disukai seperti $\emptyset$.
3. Setiap blok *plaintext* akan dipermutasikan dengan kunci grup simetri seperti berikut ini:

Blok: $K = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ k(a_1) & k(a_2) & \dots & k(a_n) \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ P_1 & P_2 & \dots & P_n \\ k(a_1) & k(a_2) & \dots & k(a_n) \\ k(P_1) & k(P_2) & \dots & k(P_n) \end{pmatrix}$

$\downarrow \quad \downarrow \quad \downarrow \quad \downarrow$

$C_1 \quad C_2 \quad \dots \quad C_n$

Keterangan: $P_i =$ karakter *plaintext* ke- i
$C_i =$ karakter *ciphertext* ke- i

Setelah semua blok selesai dipermutasikan, maka karakter-karakter pada *plaintext* akan teracak.

4. Menentukan Kunci Vigenere Cipher
(Catatan: apabila banyak karakter pada kunci kurang dari *plaintext* maka kunci akan diulang hingga seluruh *plaintext* tersebut terpenuhi. Apabila kunci melebihi *plaintext*, maka kunci akan ditulis sesuai dengan panjang *plaintext* yang diperlukan)
5. *Plaintext* yang telah dipermutasikan menjadi *ciphertext1* dan kunci Vigenere Cipher dikonversi ke dalam bentuk angka desimal dengan melihat Tabel ASCII *printable characters* (Lampiran 2).
6. *Ciphertext1* dan kunci Vigenere Cipher akan disubtitusikan ke dalam persamaan (4.1):

$$C_i = \left((P_i - 32 + K_r) \; mod \; 95\right) + 32$$

(Catatan: apabila terdapat karakter $\emptyset$ pada *ciphertext* maka tidak ikut dienkripsi namun tetap ditulis di posisinya)
7. Hasil perhitungan dari *step* 6 dikembalikan ke dalam bentuk karakter berdasarkan ASCII *printable characters*, sehingga diperoleh *ciphertext* akhir.

B. Proses dekripsi

1. Mengkonversi karakter-karakter pada *ciphertext* akhir dan kunci Vigenere Cipher ke dalam bentuk angka dengan melihat tabel ASCII *printable characters* (Lampiran 2).
2. *Ciphertext* akhir dan kunci Vigenere Cipher akan disubtitusikan ke dalam persamaan (4.2):

$$P_i = \left((C_i - 32 - K_r) \; mod \; 95\right) + 32$$

(Catatan: apabila terdapat karakter $\emptyset$ pada *ciphertext* maka tidak ikut didekripsi namun tetap ditulis di posisinya)
3. Hasil perhitungan pada *step* 2 akan dikembalikan ke dalam bentuk karakter berdasarkan ASCII *printable characters,* sehingga diperoleh *ciphertext1*.
4. Menginvers kunci grup simetri

$$K^{-1} = \begin{pmatrix} k(a_1) & k(a_2) & \dots & k(a_n) \\ a_1 & a_2 & \dots & a_n \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ k^{-1}(a_1) & k^{-1}(a_2) & \dots & k^{-1}(a_n) \end{pmatrix}$$

5. Membagi *ciphertext1* menjadi blok-blok
6. Setiap blok *ciphertext1* dipermutasikan dengan kunci invers grup simetri seperti berikut ini:

   Blok: $K^{-1} = \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ k^{-1}(a_1) & k^{-1}(a_2) & \dots & k^{-1}(a_n) \end{pmatrix}$

   $$= \begin{pmatrix} a_1 & a_2 & \dots & a_n \\ C_1 & C_2 & \dots & C_n \\ k^{-1}(a_1) & k^{-1}(a_2) & \dots & k^{-1}(a_n) \\ k^{-1}(C_1) & k^{-1}(C_2) & \dots & k^{-1}(C_n) \end{pmatrix}$$

   $P_1 \quad P_2 \quad \dots \quad P_n$

   Keterangan: $P_i =$ karakter *plaintext* ke- i

   $C_i =$ karakter *ciphertext* ke- i

   Setelah semua blok selesai dipermutasikan, maka diperoleh *plaintext* yang sebenarnya.

5. Proses Enkripsi dan Dekripsi Modifikasi Vigenere Cipher Menggunakan Grup Simetri S_5

A. Proses enkripsi:

Misalkan *plaintext* adalah `AS THE FORECAST BECAME MORE CERTAIN ACROSS THE WEEKEND THE GRAPICHS WERE USED EXTENSIVELY AS THE EXTENT OF THE SNOW FALL` dan kuncinya adalah `EASY`. Maka proses enkripsinya adalah sebagai berikut:

1) Membentuk kunci grup simetri

Berikut proses pembentukan kunci yang dimulai dengan pihak pengirim dan penerima pesan menyepakati dua elemen dari grup simetri S_5 yaitu:
pilih σ_1 dan σ_2 adalah elemen dari S_5, dengan $\sigma_1 \circ \sigma_2 \neq I$ (I adalah permutasi identitas) dan $\sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1$, sedemikian hingga $K \neq I$ (K adalah kunci grup simetri).

$$\sigma_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix} = (13524)$$

$$\sigma_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_5 & a_4 & a_2 & a_3 \end{pmatrix} = (1)(2534)$$

Kemudian tentukan R yang merupakan orde dari σ_1 dan S adalah orde dari σ_2

$R = |(13524)| =$ KPK dari 5 adalah 5

$S = |(1)(2534)| =$ KPK dari 1 dan 4 adalah 4

- Pengirim memilih dua bilangan asli M = 4 , N = 1 dan mengirim $r = {\sigma_1}^M \circ {\sigma_2}^N$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 \\ a_1 & a_5 & a_4 & a_2 \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_5 & a_1 & a_2 & a_3 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_5 & a_4 & a_2 & a_3 \end{pmatrix}$$

$$r = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_3 & a_2 & a_5 & a_1 \end{pmatrix}$$

- Pihak pengirim pesan menerima s dari penerima pesan
- Pengirim pesan menghitung kunci

$K_1 = {\sigma_1}^M \circ s \circ {\sigma_2}^N$

$$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}^4 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_1 & a_5 & a_3 & a_4 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_5 & a_4 & a_2 & a_3 \end{pmatrix}^1$$

$$K_1 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_2 & a_1 & a_4 & a_3 \end{pmatrix}$$

- Penerima juga melakukan hal yang sama, memilih bilangan asli P = 3 , Q = 1 dan mengirim

$s = {\sigma_1}^P \circ {\sigma_2}^Q$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \\ a_1 & a_5 & a_4 & a_2 & \end{pmatrix}$$

$$= \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_3 & a_4 & a_5 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_1 & a_5 & a_4 & a_2 & a_3 \end{pmatrix}$$

$$s = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_2 & a_1 & a_5 & a_3 & a_4 \end{pmatrix}$$

- Pihak penerima pesan menerima r dari pengirim pesan
- Penerima pesan menghitung

$K_2 = {\sigma_1}^P \circ r \circ {\sigma_2}^Q$

$$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_3 & a_4 & a_5 & a_1 & a_2 \end{pmatrix}^3 \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_4 & a_3 & a_2 & a_5 & a_1 \end{pmatrix} \circ \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & \\ a_1 & a_5 & a_4 & a_2 & \end{pmatrix}$$

$$K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_2 & a_1 & a_4 & a_3 \end{pmatrix}$$

Jadi kunci yang disepakati oleh kedua belah pihak yaitu

$$K = K_1 = K_2 = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_2 & a_1 & a_4 & a_3 \end{pmatrix}$$

2) Membagi *plaintext* menjadi blok-blok, setiao blok berisi lima karakter

AS*sp*TH	EFORE	CAST*sp*	BECAM
E*sp*MOR	E*sp*CER	TAIN*sp*	ACROS
S*sp*THE	*sp*WEEK	END*sp*T	HE*sp*GR
APHIC	S*sp*WER	E*sp*USE	D*sp*EXT
ENSIV	ELY*sp*A	S*sp*THE	*sp*EXTE
NT*sp*OF	*sp*THE*sp*	SNOW*sp*	FALLØ

3) Setelah itu setiap blok diubah menjadi seperti di bawah ini dengan menggunakan kunci grup simetri yang telah disepakati.

Blok 1: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_2 & a_1 & a_4 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ A & S & sp & T & H \\ a_5 & a_2 & a_1 & a_4 & a_3 \\ H & S & A & T & sp \end{pmatrix}$

Blok 2: $K = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ a_5 & a_2 & a_1 & a_4 & a_3 \end{pmatrix} = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 \\ E & F & O & R & E \\ a_5 & a_2 & a_1 & a_4 & a_3 \\ E & F & E & R & O \end{pmatrix}$

Demikian seterusnya untuk blok-blok lainnya.

Sehingga diperoleh *ciphertext1* yaitu

HSAT*sp* EFERO *sp*ACTS MEBAC R*sp*EOM R*sp*EEC *sp*ATNI SCAOR
E*sp*SHT KW*sp*EE TNE*sp*D REHG*sp* CPAIH R*sp*SEW E*sp*ESU T*sp*DXE
VNEIS ALE*sp*Y E*sp*SHT EE*sp*TX FTNO*sp* *sp*T*sp*EH *sp*NSWO ØAFLL

4) Setelah karakter-karakter pada *plaintext* teracak menjadi *ciphertext1,* selanjutnya menentukan kunci Vigenere Cipher. Kunci Vigenere Cipher yang digunakan yaitu EASY.
5) Mengkonversi karakter-karakter pada *ciphertext*1 dan kunci Vigenere Cipher ke dalam bentuk angka desimal dengan melihat tabel ASCII *Printable Characters.* Kemudian subtitusikan *ciphertext1* dan kunci Vigenere Cipher ke dalam persamaan (4.1)

$$C_i = \big((P_i - 32 + K_r)\ mod\ 95\big) + 32$$

Selanjutnya, hasil perhitungannya dikembalikan ke dalam bentuk karakter

Sehingga diperoleh ciphertext akhir adalah

.55Ne':?81s;)6GG+$5=8a9I34s?+%s;:$=M)#CL+aGB:-
Ky+'HH+a8L+*;y)25C.4sM+99y+5INe&L?
\09C9#@?e[9y9*H?+aHr,6BIeaHy+*sH99CØ;,.@

Sedangkan untuk proses dekripsinya dapat dilakukan dengan mengikuti algoritma modifikasi Vigenere Cipher menggunakan grup simetri $\boldsymbol{S_n}$.

6. Uji Hasil Enkripsi Algoritma Modifikasi Vigenere Cipher

Berikut merupakan uji hasil enkripsi algoritma modifikasi Vigenere Cipher kemudian dibandingkan dengan algoritma Vigenere Cipher Biasa. Pengujian dilakukan menggunakan metode Kasiski untuk menemukan panjang kuncinya dan metode *exhaustive key search* untuk mengetahui kemungkinan kunci yang digunakan.

Tabel 3. Hasil Enkripsi Algoritma Modifikasi Vigenere Cipher

Ciphertext Algoritma Modifikasi Vigenere Cipher	Kunci	Ciphertext Algortima Vigenere Cipher
.55**Ne':**?81**s;**)6GG+$5=8a9I3 4s?+%**s;:**$=M)#CL**+a**GB:-K**y+'** HH**+a**8**L+***;y)25C.4sM+**99y+**5I **Ne**&L?\0**9C**9#@?e[**9y**9*H?**+a**Hr **,**6BIeaHy**+***sH**99C**Ø;,.@	EASY	ES**LFI**FGPICSQXBWAEMWKSRWAIRL YMNSAVOKQXHWUIECCRD**LFI**GJYTH AAWWWWIUKCH**EPRIN**KGZEDWES**LFI** **EPRIN**IMJTZCWNGUJADJ

Perhatikan **Tabel 3** terlihat bahwa hasil enkripsi modifikasi Vigenere Cipher terdapat huruf kapital, huruf kecil, angka, dan simbol. Hal tersebut menunjukkan bahwa algoritma modifikasi Vigenere Cipher dapat mendukung penggunaan huruf kapital, huruf kecil, angka, dan simbol. Namun juga masih terlihat adanya perulangan kriptogram pada *ciphertext* modifikasi Vigenere Cipher. Berikut tabel yang memuat beberapa kriptogram yang sering muncul, beserta jarak antar kriptogram dan faktor pembaginya.

Tabel 4. Metode Kasiski

Kriptogram	Jarak	Faktor pembagi
Ne	72	2, 3, 4, 6, 8, 9, 12, 14, 24, 36, 72
s;	20	2, 4, 5, 10, 20
+a (1)	12	2, 3, 4, 6, 12
+a (2)	44	2, 4, 11. 22, 44
y+	24	2, 3, 4, 6, 8, 12, 24
y+	36	2, 3, 4, 9, 12, 18, 36
L+	16	2, 4, 8, 16
99	43	43
9y	20	2, 4, 5, 10, 20
9C	29	29
+*	52	2, 4, 13, 26, 52

Berdasarkan **Tabel 4** terlihat bahwa irisan paling banyak dari semua faktor pembagi adalah 2 dan 4. Jadi, dapat diperkirakan panjang kunci yang digunakan adalah 2 atau 4. Kita asumsikan terlebih dahulu panjang kunci adalah 4 karakter (tanpa mengabaikan kemungkinan panjang kuncinya 2 karakter). Kemudian untuk menentukan kemungkinan karakter kunci digunakan metode *exhaustive key search* yaitu dengan mencoba semua kemungkinan kunci yang panjangnya 4 karakter. Karena yang digunakan pada modifikasi Vigenere Cipher berdasarkan ASCII *printable characters* yang memiliki karakter sebanyak 95 karakter. Sehingga cara ini membutuhkan usaha percobaan sebanyak 95^p , untuk p adalah panjang kunci. Jadi, terdapat $95^4 = 8.145.065$ kemungkinan kunci. Sedangkan pada Vigenere Cipher biasa $26^4 = 456.976$. Hal tersebut membuktikan bahwa modifikasi Vigenere Cipher lebih aman jika dibandingkan dengan Vigenere Cipher biasa. Walaupun demikia n masih terdapat kemungkinan untuk terpecahkan, oleh sebab itu *plaintext* yang sebenarnya disembunyikan menggunakan penyandian grup simetri. Jadi, apabila dilakukan pembobolan menggunakan metode Kasiski dan *exhaustive key search* tidak akan dapat menemukan *plaintext* yang sebenarnya.

KESIMPULAN

Berdasarkan hasil pembahasan dapat ditarik kesimpulan sebagai berikut: (1) Modifikasi Vigenere cipher yang telah dilakukan yaitu dengan mengacak *plaintext* menggunakan penyandian grup simetri S_n sebelum dioperasikan dengan kunci Vigenere Cipher. (2) Algoritma baru yang dihasilkan terbukti lebih kuat jika dibandingkan dengan Vigenere Cipher. Hal tersebut dikarenakan *plaintext* diacak terlebih dahulu menggunakan penyandian grup simetri, sehingga *plaintext* yang sebenarnya aman terhadap serangan metode kasiski dan *exhaustive key search*. Selain itu, algoritma baru yang dihasilkan juga mendukung penggunaan huruf kapital, huruf kecil, angka, dan simbol.

DAFTAR RUJUKAN

[1] A. Hariati, K. Hardiyanti and W. Putri, "Kombinasi Algoritma Playfair Cipher dengan Metode Zig-Zag dalam Penyandian Teks," *Sinkron,* pp. 13-17, 2018.

[2] H. Mukhtar, Kriptografi untuk Keamanan Data, Yogyakarta: Deepublish, 2018.

[3] D. Rachmawati, M. A. Budiman and I. Aulia, "Super-Encryption Using Monoalphabetic Algorithm dan XOR Algorithm for Data Security," *Journal of Physic: Conference Series 979,* 2018.

[4] A.-A. M. Aliyu and A. Olaniyan, "Vigenere Cipher: Trends, Review and Possible Modifications," *International Journal of Computer Application,* pp. 46-50, 2016.

[5] R. Munir, Kriptografi, Bandung: Informatika Bandung, 2019.

[6] D. Ariyus, Pengantar Ilmu Kriptografi Teori Analisis dan Implementasi, Yogyakarta: C.V ANDI OFFSET, 2008.