
MODIFIKASI ALGORITMA VIGENERE CIPHER UNTUK PENGAMANAN FILE TEKS

Eliasta Ketaren¹⁾, Tohap Manurung²⁾, Harni Seven Adinata³⁾

Program Studi Sistem Informasi¹⁾

Program Studi Matematika²⁾

Program Studi Teknik Informatika³⁾

Universitas Sam Ratulangi Manado

Bahu, Kec. Malalayang, Kota Manado, Sulawesi Utara

email: eliasketaren@unsrat.ac.id¹⁾, tohapm@unsrat.ac.id²⁾, seven@unsrat.ac.id³⁾

Abstrak

Kerahasiaan pesan atau data yang dimiliki oleh seseorang merupakan hal yang penting dalam pengiriman pesan agar pesan tersebut hanya dapat diberikan oleh orang-orang tertentu saja yang dapat mengakses informasi tersebut. Kriptografi adalah ilmu yang mempelajari bagaimana cara mengamankan data atau pesan dengan tujuan agar tidak diketahui oleh orang lain yang ingin mengetahui isinya, dengan menggunakan kode-kode dan aturan-aturan tertentu serta cara-cara lain sehingga hanya orang yang berhak saja yang dapat mengetahui isi pesan yang sebenarnya. Pada algoritma Vigenere Cipher, pengamanan pesan hanya menggunakan kunci tunggal dan abjad sebagai kunci penyandian untuk mengganti atau mensubstitusi karakter pesan yang membuat kekuatan dalam pengamanan pesan hanya terbatas pada penggunaan abjad. Pada penelitian ini dilakukan modifikasi algoritma Vigenere Cipher dengan menggunakan kunci sebanyak 3 buah kunci dan memodifikasi tabel vigenere cipher dengan menambahkan angka dan 10 buah simbol sehingga karakter penyusun tabel menjadi 46 karakter dari yang sebelumnya hanya 26 karakter. Hasil percobaan algoritma ini mampu mengenkripsi pesan rahasia dan mendekripsinya kembali menjadi pesan asli.

Kata Kunci: Kriptografi, File Teks, Vigenere Cipher, Kunci.

1. Pendahuluan

Penggunaan teknologi komputer sebagai salah satu aplikasi teknologi informasi dan pengelolaan data sudah menjadi kebutuhan saat ini, karena banyak pekerjaan yang dapat dilakukan dengan cepat, akurat dan efisien. Dengan demikian, perlu diterapkan prosedur keamanan terhadap informasi yang akan dikirimkan. Ada berbagai macam cara untuk mengatasi masalah keamanan data, yang pada intinya adalah bagaimana mencegah orang yang tidak berkepentingan untuk membaca, mengubah atau bahkan menghancurkan data yang bukan miliknya atau ditujukan kepadanya, yang disebut dengan Kriptografi. Tentu saja hal ini akan sangat berguna untuk menjaga kerahasiaan data atau informasi tertentu.

Pada penelitian Nurnawati, E. K. (2008) yang berjudul Analisis Kriptografi Menggunakan Algoritma Vigenere Cipher dengan Mode Operasi Cipher Block Chaining (CBC), dilakukan kombinasi kriptografi algoritma Vigenere Cipher dengan mengadopsi mode operasi Cipher Block Chaining (CBC). Hasil dari percobaan tersebut adalah pada saat proses enkripsi dan dekripsi dibutuhkan memori yang sangat besar sehingga mengakibatkan proses yang lama. Untuk alasan ini, penulis membatasi panjang kunci hingga 10 karakter. Algoritma Vigenere Cipher yang asli hanya mengakomodasi 26 huruf dalam bentuk huruf kecil sedangkan tanda baca lainnya tidak dapat dibaca. Sehingga perlu dilakukan evaluasi, yaitu dengan memperluas jangkauan dari 26 abjad menjadi 256 karakter ASCII.

Caesar cipher dan Vigenere Cipher adalah contoh metode kriptografi dengan model keamanan substitusi karakter. Metode Caesar Cipher menggunakan kunci berupa angka sebagai nilai untuk menggantikan karakter pesan dengan karakter lain. Yang berbeda dari Vigenere Cipher adalah hanya menggunakan alfabet sebagai kunci penyandian untuk mengganti atau mensubstitusi karakter pesan, yang membuat kekuatan pesan hanya terbatas pada penggunaan alfabet tersebut.

Melihat keterbatasan tersebut, penulis memutuskan untuk membahas teknik kriptografi yang sudah ada ini untuk dikembangkan dengan tujuan menambah fleksibilitas dan kekuatan dalam mengamankan informasi, dengan harapan suatu saat dapat digunakan baik untuk penulis sendiri maupun orang lain. Judul penelitian yang diangkat adalah “Modifikasi Algoritma Vigenere Cipher untuk Pengamanan File Teks”.

2. Landasan Teori

Algoritma Vigenere Cipher

Vigenere Cipher merupakan jenis cipher abjad majemuk yang paling sederhana. Vigenere cipher menerapkan metode substitusi poli alfabetik dan termasuk ke dalam kategori kunci simetris dimana kunci yang digunakan untuk proses enkripsi adalah sama dengan kunci yang digunakan untuk proses dekripsi. Vigenere Cipher ditemukan pertama kali oleh Giovan Battista Bellaso. Beliau menuliskan metode enkripsi yang kita kenal sebagai Vigenere Cipher ini pada bukunya yang berjudul La Cifradel. Sig. Giovan Battista Bellaso pada tahun 1553. Namun, nama “Vigenere” pada Vigenere Cipher diambil dari seorang yang bernama Blaise de Vigenere.

Enkripsi dengan menggunakan algoritma Vigenere Cipher pada dasarnya adalah menggunakan prinsip Caesar Cipher, yaitu melakukan enkripsi karakter pada plainteks menjadi karakter lain pada cipherteks. Perbedaan antara Caesar Cipher dan Vigenere Cipher adalah huruf yang sama pada plainteks tidak selalu dienkripsi menjadi huruf yang sama pada cipherteks. Hal ini terjadi karena pada Vigenere Cipher, pergeseran karakternya ditentukan oleh karakter yang ada pada kata kunci dan kata ini selalu diulang. Akibatnya, karakter yang sama pada plainteks boleh jadi memiliki karakter yang berbeda pada cipherteksnya. Karena hal inilah, Vigenere Cipher merupakan cipher substitusi abjad-majemuk. Tujuan utama dari Vigenere Cipher ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya.

Konsep Dasar Vigenere Cipher

Vigenere Cipher merupakan cipher substitusi abjad majemuk. Tujuan utama dari Vigenere Cipher ini adalah menyembunyikan keterhubungan antara plainteks dan cipherteks dengan menggunakan kata kunci sebagai penentu pergeseran karakternya dengan syarat plaintext tidak boleh lebih pendek dari pada kunci. Secara matematis perhitungan Vigenere Cipher sebagai berikut:

$$c = (p + K) \text{ mod } n \dots\dots\dots(1)$$

Keterangan:

Ci (c1,c2,...ct) = rangkaian cipherteks

Pi (p1,p2,...pt) = rangkaian plainteks

K (k1,k2,...km) = rangkaian kunci

n = jumlah susunan alphabet

Dalam proses enkripsi dan dekripsi menggunakan Vigenere Cipher, dibutuhkan kunci untuk dapat mengubah plainteks menjadi cipherteks. Apabila kunci yang digunakan lebih pendek daripada plainteks, maka huruf dalam kunci akan diulang sebanyak plainteks yang akan di enkripsi. Dibawah ini adalah tabel bujur sangkar Vigenere yang digunakan untuk enkripsi dan dekripsi suatu teks.

Tabel 1. Bujur Sangkar Vigenere Chiper

| | PLAINTEXT | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|-----------|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| a | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z |
| b | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| c | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| d | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| e | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| f | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| g | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| h | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| i | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| j | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| k | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| l | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| m | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| n | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| o | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| p | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| q | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| r | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| s | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R |
| t | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| u | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| v | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| w | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| x | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| y | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X |
| z | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

3. Metode Penelitian

Analisis Modifikasi Vigenere Cipher

Pada penelitian ini, penulis melakukan modifikasi algoritma Vigenere Cipher untuk mengamankan pesan rahasia berupa teks. Modifikasi dilakukan pada penambahan karakter pada tabel Vigenere dan penggunaan 3 buah kunci. Pada

pengembangan penambahan karakter yaitu penambahan angka dan simbol, dengan demikian ukuran tabel yang digunakan untuk melakukan enkripsi dan dekripsi menjadi lebih besar menjadi 46 karakter.

Pada modifikasi algoritma Vigenere Cipher ini dilakukan penambahan karakter angka dan simbol, sehingga Plaintext yang dapat dienkripsi tidak hanya terbatas pada alfabet, tetapi juga angka dan simbol. Tabel modifikasi Vigenere Cipher dapat dilihat seperti pada Tabel 2.

Tabel 2. Modifikasi Tabel Vigenere Cipher

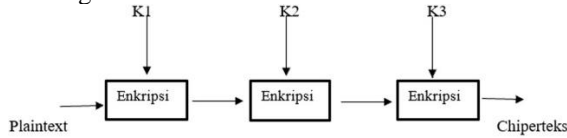
| P K | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? |
|--------|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|----|---|---|---|---|---|---|
| A | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? |
| B | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | |
| C | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | |
| D | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | |
| E | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | |
| F | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | |
| G | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | |
| H | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | |
| I | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | |
| J | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | |
| K | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | |
| L | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | |
| M | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | |
| N | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | |
| O | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | |
| P | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | |
| Q | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | |
| R | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | |
| S | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | |
| T | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | |
| U | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | |
| V | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | |
| W | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | |
| X | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | |
| Y | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | |
| Z | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | |
| 0 | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 1 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 2 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 3 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 4 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 5 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 6 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 7 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 8 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| 9 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ! | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| @ | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| # | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| \$ | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| % | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| * | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| (| (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|) |) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| \ | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
| ? | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Berdasarkan tabel 2 di atas, nilai-nilai karakter dapat dilihat pada tabel 3 di bawah ini.

Tabel 3. Nilai Karakter

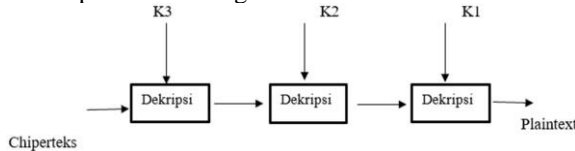
| | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|----|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|----|---|---|---|---|---|---|
| A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? |
| 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | ! | @ | # | \$ | % | * | (|) | \ | ? | | | | | | | | | | | | | | | | | | | | | | | | | | | |

Dengan dibuatnya 3 buah kunci, maka kelemahan penggunaan kunci pada algoritma Vigenere Cipher dapat diatasi. Pada penelitian ini, penulis mencoba membuat 3 lapis kunci yang dapat dilihat pada Gambar 1 dan 2. Penggunaan kunci dalam proses enkripsi adalah sebagai berikut:



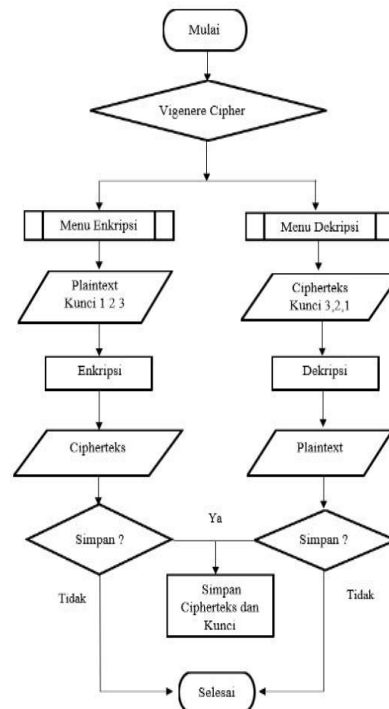
Gambar 1. Proses Enkripsi dengan 3 Lapis Kunci

Penggunaan kunci dalam proses dekripsi adalah sebagai berikut:



Gambar 2. Proses Dekripsi dengan 3 Lapis Kunci

Adapun diagram alir proses enkripsi dan dekripsi pesan teks dengan algoritma Vigenere Cipher dapat dilihat pada Gambar 3.



Gambar 3. Proses Enkripsi dan Dekripsi File Teks

Enkripsi dan Dekripsi Algoritma Vigenere Cipher Menggunakan 3 Kunci

Proses pengamanan pesan pada Vigenere Cipher juga dapat diselesaikan dengan rumus matematis algoritma Caesar Chiper, dengan mensubsitusikan nilai A - ? adalah 0 - 46 dengan nilai sesuai dengan Tabel 1.

Rumus Algoritma Vigenere Chiper adalah sebagai berikut:

Untuk Enkripsi:

$$C_i = Ek (P_i) = (P_i + K_i) \text{ mod } 46 \dots\dots\dots(2)$$

Untuk Dekripsi:

$$P_i = Dk (C_i) = (C_i - K_i) \text{ mod } 46 \dots\dots\dots(3)$$

Keterangan :

- C = Ciphertext
- P = Plaintext
- E = Enkripsi
- D = Dekripsi
- K = Kunci

Penerapan Vigenere dengan kunci 3 lapis adalah sebagai berikut:

Plaintext : MERDEKA 1945

- K1 : SEMOGA
- K2 : BERHASIL
- K3 : SYUKUR

Proses Enkripsi menggunakan persamaan (2):

- Plaintext : MERDEKA 1945
- K1 : SEMOGASEMOG
- Ciphertext 1 : 4I3RKK5B \@
- K2 : BERHASILBER
- Ciphertext 2 : 5MAYK20(CCI
- K3 : SYUKURSYUKU
- Ciphertext 3 : D!U84?\UWM2

Untuk mengembalikan ke Plaintext melalui proses dekripsi, pada kasus ini kita menggunakan rumus matematika yang telah dibahas sebelumnya dengan melihat perpotongan antara pergeseran ciphertext dengan kunci dapat diselesaikan, namun secara matematis rumus digunakan pada persamaan (2) maka proses dekripsinya sebagai berikut:

Chipertext : D ! U 8 4 ? \ U W M 2
 K3 : SYUKUR
 K2 : BERHASIL
 K1 : SEMOGA

Proses Dekripsi menggunakan persamaan (3):

Chipertext 3 : D ! U 8 4 ? \ U W M 2
 K3 : S Y U K U R S Y U K U
 Chipertext 2 : 5 M A Y K 2 0 (C C I
 K2 : B E R H A S I L B E R
 Chipertext 1 : 4 I 3 R K K S 5 B \ @
 K1 : S E M O G A S E M O G
 Plaintext : M E R D E K A 1 9 4 5

4. Hasil Penelitian

Rancangan Form Modifikasi Vigenere Cipher

Rancangan Form Modifikasi Vigenere Cipher untuk melakukan enkripsi dan dekripsi dengan algoritma Vigenere Cipher dilihat seperti pada Gambar 4.

Gambar 4. Rancangan Form Modifikasi Vigenere Cipher

Keterangan:

1. Kotak Teks: fungsi untuk entri teks biasa
2. TextBox: berfungsi untuk entri kunci 1
3. TextBox: berfungsi untuk menampilkan ciphertext 1
4. TextBox: berfungsi untuk masukan kunci 2
5. TextBox: berfungsi untuk menampilkan ciphertext 2
6. TextBox: berfungsi untuk memasukkan kunci 3.
7. TextBox: berfungsi untuk menampilkan ciphertext hasil enkripsi.
8. TextBox: berfungsi untuk memasukkan Plaintext dari file yang dimuat
9. TextBox: berfungsi untuk memasukkan kunci 1
10. TextBox: berfungsi untuk menampilkan ciphertext 1
11. TextBox: berfungsi untuk masukan kunci 2.
12. TextBox: berfungsi untuk menampilkan ciphertext 2
13. TextBox: berfungsi untuk input kunci 3.
14. TextBox: berfungsi untuk menampilkan ciphertext hasil enkripsi.
15. Tombol: berfungsi untuk melakukan enkripsi
16. Button: berfungsi untuk melakukan dekripsi
17. Tombol: berfungsi untuk melakukan pembersihan layer

18. Tombol: berfungsi untuk melakukan enkripsi
19. Tombol: berfungsi untuk melakukan dekripsi
20. Tombol: berfungsi untuk memanggil file teks
21. Tombol: berfungsi untuk menyimpan hasil enkripsi
22. Tombol: berfungsi untuk menutup tampilan form

Hasil

Setelah melakukan perancangan Modifikasi Algoritma Vigenere Cipher maka tahap selanjutnya adalah penulisan kode program (coding) dan pembuatan aplikasi. Tampilan Modifikasi Algoritma Vigenere Cipher untuk melakukan enkripsi dan dekripsi dapat dilihat seperti pada Gambar 5.



Gambar 5. Tampilan Modifikasi Vigenere Cipher

Pada Gambar 5 di atas terdiri dari 2 bagian, yaitu bagian Input Plaintext, yaitu proses enkripsi dan dekripsi dengan cara memasukkan plaintext melalui keyboard dan bagian Load Plaintext, yaitu proses enkripsi dan dekripsi dengan cara memasukkan plaintext melalui file plaintext yang sudah tersedia.

Pembahasan

Enkripsi dilakukan dengan memasukkan plaintext melalui keyboard dengan jumlah huruf 13, 24, dan 53 dengan key1= a, key2 = b dan key3 = c. Hasil enkripsi Algoritma Vigenere Cipher dengan input teks dapat dilihat pada Tabel 4.

Tabel 4. Hasil Test Enkripsi Modifikasi Vigenere Cipher

| No | Plaintext | Jumlah Karakter | Ciphertext |
|----|---|-----------------|--|
| 1 | STMIK NEUMANN | 13 | VWPLNQHXPDQQ |
| 2 | STMIK NEUMANN MEDAN 2018 | 24 | VWPLNQHXPDQQPHGDQ534@ |
| 3 | STMIK NEUMANN MEDAN 2018 PERANGKAT LUNAK KRIPTOGRAFI | 53 | VWPLNQHXPDQQPHGDQ534@SHUDQJND WOXQDNNULSWRJUDIL |

Hasil dekripsi dari Modifikasi Algoritma Vigenere Cipher dengan input teks dapat dilihat pada Tabel 5.

Tabel 5. Hasil Test Dekripsi Modifikasi Vigenere Cipher

| No | Ciphertext | Plaintext | Hasil |
|----|--|--|---------|
| 1 | VWPLNQHXPDQQ | STMIK NEUMANN | SUCCESS |
| 2 | VWPLNQHXPDQQPHGDQ534@ | STMIK NEUMANN MEDAN 2018 | SUCCESS |
| 3 | VWPLNQHXPDQQPHGDQ534@SHUDQJND JNDWO XQDNNULSWRJUDIL | STMIK NEUMANN MEDAN 2018 PERANGKAT LUNAK KRIPTOGRAFI | SUCCESS |

5. Kesimpulan

Adapun kesimpulan dari penelitian ini adalah sebagai berikut: Vigenere cipher dapat dimodifikasi dengan menambahkan jumlah karakter. Untuk meningkatkan keamanan vigenere cipher, maka dapat dilakukan dengan

manambahkan jumlah karakter lebih banyak lagi. Selain dengan menambahkan jumlah karakter, keamanan vigenere cipher dapat ditingkatkan dengan menambahkan jumlah kunci.

6. Daftar Pustaka

- [1] Aditya Permana, A. (2018). Penerapan Kriptografi Pada Teks Pesan dengan Menggunakan Metode Vigenere Cipher Berbasis Android. *Jurnal AL-AZHAR INDONESIA SERI SAINS DAN TEKNOLOGI*, 4(3), 110–115.
- [2] Afandi, M. I., & Nurhayati, N. (2021). Implementasi Algoritma Vigenere Cipher Dan Atbash Cipher Untuk Keamanan Teks Pada Aplikasi Catatan Berbasis Android. *It (Informatic Technique) Journal*, 8(1).
- [3] Astuti, D., & Sundari, C. (2022). IMPLEMENTASI ALGORITMA VIGENERE CIPHER UNTUK ENKRIPSI DAN DEKRIPSI PADA PERESEPAN DATA OBAT DI PUSKESMAS MERTOYUDAN 1 KABUPATEN MAGELANG. *Jurnal Teknik Informasi Dan Komputer (Tekinkom)*, 5(2), 341–350.
- [4] Riski, A., Kamsyakawuni, A., & Arif, M. Z. (2018). IMPLEMENTASI VIGENERE CIPHER PADA PENGAMANAN DATA MEDIS. *Jurnal Riset Dan Aplikasi Matematika*, 02(01), 23–30.
- [5] Riadi, I., Fadlil, A., & Tsani, F. A. (2022). Pengamanan Citra Digital Berbasis Kriptografi Menggunakan Algoritma Vigenere Cipher. *JISKA (Jurnal Informatika Sunan Kalijaga)*, 7(1), 33–45.