PENINGKATAN KEAMANAN VIGENERE CIPHER MELALUI INTEGRASI CAESAR CIPHER DAN SUBSTITUSI KARAKTER ACAK DENGAN PERLUASAN SET KARAKTER

SKRIPSI

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

KHANSA INTANI

20.83.0547

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

PENINGKATAN KEAMANAN VIGENERE CIPHER MELALUI INTEGRASI CAESAR CIPHER DAN SUBSTITUSI KARAKTER ACAK DENGAN PERLUASAN SET KARAKTER

SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana

Program Studi Teknik Komputer

disusun oleh

KHANSA INTANI

20.83.0547

Kepada

FAKULTAS ILMU KOMPUTER

UNIVERSITAS AMIKOM YOGYAKARTA

YOGYAKARTA

2024

HALAMAN PERSETUJUAN

SKRIPSI

PENINGKATAN KEAMANAN VIGENERE CIPHER MELALUI INTEGRASI CAESAR CIPHER DAN SUBSTITUSI KARAKTER ACAK DENGAN PERLUASAN SET KARAKTER

yang disusun dan diajukan oleh

Khansa Intani
20.83.0547

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 22 Januari 2024

Dosen Pembimbing,

Dony Ariyus, M.Kom
NIK. 190302128

HALAMAN PENGESAHAN

SKRIPSI

PENINGKATAN KEAMANAN VIGENERE CIPHER MELALUI INTEGRASI CAESAR CIPHER DAN SUBSTITUSI KARAKTER ACAK DENGAN PERLUASAN SET KARAKTER

yang disusun dan diajukan oleh

Khansa Intani

20.83.0547

Telah dipertahankan di depan Dewan Penguji
pada tanggal 22 Januari 2024

Susunan Dewan Penguji

Nama Penguji	Tanda Tangan
Jeki Kuswanto, M.Kom **NIK. 190302456**	
Joko Dwi Santoso, M.Kom **NIK. 190302181**	
Dony Ariyus, M.Kom **NIK. 190302128**	

Skripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 22 Januari 2024

DEKAN FAKULTAS ILMU KOMPUTER

Hanif Al Fatta, S.Kom., M.Kom., Ph.D
NIK. 190302096

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Khansa Intani
NIM : 20.83.0547

Menyatakan bahwa Skripsi dengan judul berikut:

Peningkatan Keamanan Vigenere Cipher melalui Integrasi Caesar Cipher dan Substitusi Karakter Acak dengan Perluasan Set Karakter

Dosen Pembimbing : Dony Ariyus, M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 22 Januari 2024

Yang Menyatakan,

Khansa Intani

HALAMAN PERSEMBAHAN

Skripsi ini dengan tulus dipersembahkan untuk:

1. Orangtua tercinta yang senantiasa memberikan doa, dukungan, dan kasih sayang.
2. Bapak Dony Ariyus, M.Kom., sebagai Kepala Prodi Teknik Komputer dan pembimbing yang memberikan bimbingan, arahan, dan motivasi.
3. Teman-teman yang selalu memberikan semangat dan dukungan.
4. Diri saya sendiri yang sudah melakukan penelitian dan penyusunan skripsi.

Semua persembahan ini adalah ungkapan terima kasih atas dedikasi dan dukungan yang tak terhingga selama penulisan skripsi ini.

Yogyakarta, 03 Januari 2024

Penulis

KATA PENGANTAR

Puji syukur penulis panjatkan kehadirat Allah SWT, yang telah melimpahkan rahmat, petunjuk, dan karunia-Nya sehingga penulis dapat menyelesaikan skripsi berjudul "Peningkatan Keamanan Vigenere Cipher Melalui Integrasi Caesar Cipher dan Substitusi Karakter Acak dengan Perluasan Set Karakter." Skripsi ini disusun sebagai salah satu syarat untuk memperoleh gelar Sarjana Komputer (S.Kom) dari Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas Amikom Yogyakarta.

Penelitian ini bertujuan untuk meningkatkan tingkat keamanan Vigenere Cipher dengan mengintegrasikan metode Caesar Cipher dan substitusi karakter acak, sekaligus memperluas set karakter yang digunakan. Pengembangan keamanan pada teknik enkripsi klasik ini diharapkan dapat memberikan kontribusi positif terhadap keamanan informasi dalam komunikasi digital.

Penulis ingin menyampaikan penghargaan dan terima kasih kepada:

1. Bapak Dony Ariyus, M.Kom., dosen pembimbing, atas bimbingan, arahan, dan motivasi dalam penyusunan skripsi.
2. Seluruh dosen dan staf Fakultas Ilmu Komputer Universitas Amikom Yogyakarta atas ilmu dan dukungannya.
3. Keluarga tercinta yang senantiasa memberikan doa, dukungan, dan semangat.
4. Teman-teman sejawat dan semua pihak yang membantu dalam berbagai aspek selama penulisan skripsi.

Semoga skripsi ini dapat memberikan kontribusi positif dalam pengembangan ilmu pengetahuan, khususnya di bidang keamanan informasi. Akhir kata, penulis berharap semoga hasil penelitian ini dapat memberikan manfaat dan inspirasi bagi pembaca.

Yogyakarta, 03 Januari 2024

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

DAFTAR LAMPIRAN

DAFTAR LAMBANG DAN SINGKATAN

C_i	Karakter *ciphertext* ke-i
K_i	Karakter kunci/*key* ke-i
K	Nilai pergeseran yang digunakan dalam Caesar
m	Panjang dari alfabet
T_i	Karakter ke-i dari *plaintext*
n	Jumlah karakter yang digunakan
F_i	Jumlah karakter muncul dalam teks
N	Jumlah karakter dalam teks

DAFTAR ISTILAH

Kriptografi	Ilmu dan praktik penyandian pesan untuk menjaga keamanan komunikasi.
Plaintext	Pesan asli sebelum dienkripsi.
Ciphertext	Pesan setelah dienkripsi, tidak dapat dibaca tanpa dekripsi.
Key	Parameter yang digunakan dalam algoritma kriptografi untuk enkripsi dan dekripsi.
Enkripsi	Proses mengubah pesan asli menjadi bentuk yang tidak dapat dibaca tanpa kunci.
Dekripsi	Proses mengubah pesan yang telah dienkripsi menjadi pesan asli menggunakan kunci yang sesuai.
Kriptografi Simetris	Sistem kriptografi di mana kunci enkripsi dan dekripsi sama.
Kriptografi Asimetris	Sistem kriptografi di mana kunci enkripsi dan dekripsi berbeda.
Algoritma Kriptografi	Serangkaian langkah matematis yang digunakan untuk enkripsi dan dekripsi.

INTISARI

Enkripsi merupakan salah satu cara untuk mengubah suatu pesan menjadi sulit dibaca dan membutuhkan cara tertentu dalam memahami pesan tersebut dan Vigenere Cipher adalah salah satu dari metode tersebut. Dalam penggunaan nya panjang key yang pendek menyebabkan adanya perulangan karakter untuk menyamakan panjang pesan, menyebabkan adanya perulangan karakter pada text hasil enkripsi sehingga Vigenere Cipher dapat dipecahkan dengan menggunakan salah satu metode yaitu Kasiski Test. Dengan Substitution Cipher dan Shuffled Key serta perluasan karakter dari 26 menjadi 95 karakter yang digunakan, Vigenere Cipher menghasilkan ciphertext yang memiliki nilai index of coincidence menurun mengikuti jumlah karakter yang digunakan pada key. Index of coincidence digunakan untuk menunjukkan besaran nilai peluang dari suatu karakter muncul dalam suatu teks. Hal ini menujukkan bahwa selain menggunakan algoritma Substitution Cipher, pengacakan karakter key dan perluasan karakter yang digunakan, panjang kunci atau key juga memengaruhi hasil enkripsi dari algoritma Vigenere Cipher sehingga perulangan karakter pada kunci dapat diminimalisirkan dan karakter yang repetitif pada teks hasil enkripsi juga berkurang.

Kata kunci: Enkripsi, Vigenere Cipher, Substitution Cipher, Index of Coincidence, key.

ABSTRACT

Encryption is one way to transform a message into something difficult to read and requires a specific method to understand the message. The Vigenere Cipher is one of these methods. In its use, a short key length causes character repetition to match the message's length, resulting in repeated characters in the encrypted text. This makes the Vigenere Cipher vulnerable to decryption using methods like the Kasiski Test. By using Substitution Cipher and a shuffled key, along with an expanded character set from 26 to 95 characters, the Vigenere Cipher produces ciphertext with a decreased index of coincidence following the number of characters used in the key. The index of coincidence is used to indicate the probability of a character appearing in a text. This demonstrates that besides using the Substitution Cipher algorithm, character shuffling in the key, and expanding the character set, the length of the key also affects the encryption result of the Vigenere Cipher, allowing for the minimization of character repetition in the key and reducing repetitive characters in the encrypted text.

Keyword**:** *Encryption, Vigenere Cipher, Substitution Cipher, Index of Coincidence, key.*