



INNOVATIVE: Journal Of Social Science Research

Volume 3 Nomor 5 Tahun 2023 Page 9107-9116

E-ISSN 2807-4238 and P-ISSN 2807-4246

Website: <https://j-innovative.org/index.php/Innovative>

Analisis Vigenere Chipter Dalam Tulisan Nama Mahasiswa Di Hasil Ujian akhir Semester Ganjil T.A 2023/2024

Peniel Sam Putra Sitorus^{1✉}

Program Studi Ilmu Komputer, Universitas HKBP Nommensen Pematangsiantar, Pematang
Siantar, Indonesia

Email: peniel.sitorus@uhnp.ac.id^{1✉}

Abstrak

Teknologi informasi yang modern merupakan suatu informasi yang banyak di akses masyarakat sekarang ini. Dengan kemajuan teknologi maka akses untuk mencari data sangatlah mudah di lihat banyak orang. Data yang kita ketahui saat ini ada 2 jenis yaitu umum dan rahasia. Data yang di bilang dengan rahasia maka data itu tidak bisa di akses oleh masyarakat. Dimana perkembangan ilmu pengetahuan sekarang data yang rahasia bisa lihat oleh masyarakat.

Oleh karena itu data yang berisi dengan tulisan teks bisa kita buat dengan rahasia yang tidak di mengerti banyak orang. Maksudnya teks yang berisi tulisan, bisa kita buat tulisannya acak sehingga maksud tulisan tersebut tidak di mengerti oleh orang lain. Dengan mengacak tulisan itu dibutuhkan suatu metode yang diberikan namanya Vigenere Cipher. Metode ini sangat besar pengaruhnya pada titik kuncinya. Dengan upaya menciptakan hal keamanan sebuah data yang berisi teks metode ini mampu mengamankan sebuah data yang berisi sebuah teks tulisan.

Kata Kunci: *kriptografi algoritma kunci teks*

Abstract

Modern information technology is information that is widely accessed by society today. With advances in technology, access to search for data is very easy for many people to see. There are currently 2 types of data that we know, namely general and confidential. If data is disclosed confidentially, the data cannot be accessed by the public. Where the development of science is now confidential data can be seen by the public. Therefore, we can create data containing written text with secrets that many people do not understand. This means that the text contains writing, we can make the writing random so that the meaning of the writing is not understood by other people. To randomize the writing, a method is needed called the Vigenere Cipher. This method has a huge impact on the key point. By trying to create security for data containing text, this method is able to secure data containing written text.

Keywords: *kriptografi Algoritma KunciTeks*

PENDAHULUAN

Data merupakan suatu kumpulan informasi dengan keterangan yang banyak tulisan, kalimatnya, ini berasal dari narasumber. Data yang dimiliki oleh banyak orang bisa saja dapat diakses oleh banyak masyarakat melalui akses sebuah internet ataupun offline. Data dimiliki biasanya memiliki dua jenis seperti data pribadi, dan data publik[1]. Data yang buat sebagai tenaga kerja merupakan suatu konsep yang mendudukan data dari pengguna internet menjadi hak milik tersendiri. Keterangan tentang sesuatu hal, bisa dapat mempunyai makna didalamnya. Jadi sejumlah informasi yang telah didapat memberikan suatu gambaran di dalam suatu keadaan, atau permasalahan seperti berbentuk angka maupun huruf[2].

Di generasi 4.0 sekarang ini tidak ada yang mencari informasi dengan tidak cepat, semua sudah dikelilingi oleh teknologi informasi digital. Sesuatu data sekarang ini bisa saja didapatkan dengan kumpulan informasi-informasi yang dapat diakses dari teknologi sistem informasi digital[3][4]. Dengan data yang bersifat rahasia dengan akses dimiliki banyak orang, harus dimiliki yang namanya keamanan data. Bukan data yang bersifat rahasia saja, data yang boleh diakses banyak orang bisa di buat keamanan data tersebut[5][6].

Keamanan data merupakan proses praktik yang telah dilakukan dalam melindungi data dari akses tidak bertanggung jawab. Adapun tujuan dari keamanan data untuk mendapat kerahasiaan atau integritas sehingga cuma orang yang berwenangan yang bisa dapat akses data tersebut. Keamanan data tersebut ada namanya yang dikenal dengan kriptografi[7].

Kriptografi yang sudah ada sekarang merupakan suatu ilmu keamanan untuk mengubah teks asli menjadi teks acak yang tidak dapat diketahui atau dimengerti oleh

banyak orang. Kriptografi juga menjaga kerahasiaan pesan dengan menggunakan metode klasik dan modern[8][9]. Metode klasik ini menjadi awal dalam perkembangan kriptografi, yang sulit terbaca oleh banyak orang dengan penalaran logika tinggi. Kriptografi memiliki banyak jenis algoritma yang ditemukan oleh para pakar atau ahli peneliti. Kriptografi menjadi sumber atau bagian dari algoritmanya yang dibuatnya[10].

Algoritma merupakan suatu kumpulan instruksi dalam penyelesaian suatu masalah. Algoritma ini tidak hanya berkaitan dengan ilmu komputer, tetapi juga berlaku dalam kehidupan sehari-hari. Dalam bidang ilmu komputer, algoritma sangat dipergunakan untuk menyelesaikan permasalahan-permasalahan dalam berkomputasi numerik[11][12].

Penelitian ini, dalam algoritma yang digunakan adalah algoritma *vigenere chipher*, juga dikenal sebagai algoritma yang klasik, didalam teknologi sistem informasi akademik di sebuah kampus. Adanya kekurangan dalam teknologi sistem informasi akademik muncul dalam perkembangan teknologi sekarang ini. Telah terjadi tersebar informasi yang belum dapat diketahui oleh banyak orang, yang datanya belum resmi diberitakan dengan publik. Oleh karena itu diperlukan metode keamanan data dalam sebuah teknologi informasi yang berisi data-data yang dapat diakses banyak orang.

METODE PENELITIAN

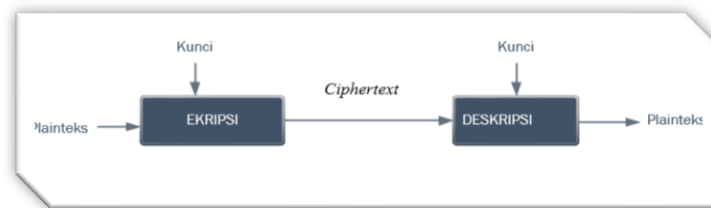
Tahapan-tahapan dalam keamanan sebuah data bentuknya seperti teks abjad maupun abservasi diterapkan dialgoritma *vigenere chipher* memiliki tahapan metode penelitian yang harus dilakukan sebagai berikut :

Kriptografi

Kriptografi banyak dikatakan dengan makna yang disembunyikan atau mempunyai sebuah rahasia tulisan yang bermakna. Kriptografi ini awalnya berasal dari Yunani dengan kata lain *cryptos* yang berhubungan dengan bidang matematika. Karena ada proses pengolahan angka dan huruf maka kriptografi diartikan bidang yang mempunyai seni dalam menjaga kerahasiaan sebuah teks. Hal ini kriptografi menulis sebuah pesan kerahasiaan bertujuan untuk menyembunyikan makna pesan tersebut[13]. Ada pula kata lain di dalam kriptografi tersebut yaitu :

- a) *Plaintext*
- b) *Key*
- c) *Chiptertext*
- d) *Enkripsi*
- e) *Deskripsi*

Proses untuk mengubah *chiptertext* menjadi plainteks memerlukan namanya kunci atau *key*. Begitu juga prosesnya pada *cipherteks* memerlukan namanya kunci untuk mengubah kembali teks yang sudah teracak menjadi teks yang aslinya. Berikut ini gambar alur dalam menginkripsikan dan deskripsi dalam sebuah teks, sebagai berikut :



Gambar 1. Proses Kriptografi

Kriptografi ini memiliki tujuannya yaitu menjaga kerahasiaan data, integritas pada data, autentifikasi, non-repudasi. Dimana untuk menjaga sebuah informasi dari pihak yang tidak hak memiliki otoritas merupakan definisi dari kerahasiaan. Integritas merupakan tentu informasi yang menerima tidak berubah dengan yang aslinya. Identifikasi dalam kebenaran suatu informasi sangat berhubungan dengan pengenalan sama pengguna, itu dinamakan autentifikasi [14]. Penerima serta pengirim suatu informasi tidak dapat memberikan sangkalan terhadap informasi yang diterimanya.

Vigenere Chipher

Metode perhitungan ini termasuk suatu metode keamanan yang mempunyai standarnya. Metode *vigenere Cipher* suatu bagian dari *polialfabetik* yang eranya pada 1586an ditemukan oleh Blaise de Vigenere dari diplomatnya perancis. Di *vigenere Cipher* ada namanya tabel standart huruf yang kita ketahui secara umum yaitu mulai dari huruf A sampai Z. Dimana kunci pada metode ini telah dipakai dengan berulang-ulang sebanyak kalimat yang mau di enkripsi. Huruf alfabetik semakin beragam dipergunakan dengan kunci, maka akan semakin kuatlah keamanan metode *vigenere Cipher*[15].

Metode *vigenere Cipher* terdapat banyak variasai yang terdapat perbedaan pada kunci tersebut, antara lain yaitu *full vigenere cipher*, *auto key vigenere cipher*, *running key vigenere chipher*. Berikut ini perumusan enkripsi dan deskripsi :

$$\text{Enkripsi : } C_i = P_i + K_i \text{ mod } 26$$

$$\text{Deskripsi : } P_i = C_i - K_i \text{ mod } 26$$

HASIL DAN PEMBAHASAN

Penelitian didalam ini data yang digunakan dalam pengujian adalah data ilmu komputer uhkbpnp tahun ajaran 2023 sampai 2024 matakuliah aljabar linier fundamental. Data yang dimiliki berjumlah 16 dan data yang mau diujikan dalam algoritma tersebut yaitu 1. Berikut ini data mahasiswa/mahasiswi tahun ajaran 2022-2023, sebagai berikut :

Tabel 1. Tabel Data Mahasiswa/Mahasiswi Matkul Aljabar Linier Fundamental T.A 2023-2024

NO	NIM	NAMA MAHASISWA
1	2202050001	THEO KRISTIAN GULTOM
3	2202050003	RONI INDRAWAN SIAHAAN
5	2202050005	DINDA ZEFANYA SIMANJUNTAK
6	2202050006	NAUFHAL FACHREZA
7	2202050007	RIDO WINHAT PANJAITAN
9	2202050009	ANDIKA SOPIAN SAMOSIR
10	2202050010	POLDEN HERMANSYAH SIDABUTAR
11	2202050011	SENIOR ALFIAN SILITONGA
13	2202050013	LOLI SEPTRY YANIGERS SIAHAAN
14	2202050014	JESSE CRISTIAN SAMOSIR
15	2202050015	SAMUEL MANURUNG
16	2202050016	MARIA KRISTINA RONDANG SITORUS

a. Enkripsi

Plainteks : MARIA KRISTINA RONDANG SITORUS

Kunci : ROSIA BAHTERNA MARSIH PULAUTE

$$M = R \text{ mod } 26$$

$$= D$$

$$A = O \text{ mod } 26$$

$$= O$$

$$R = S \text{ mod } 26$$

$$= J$$

$$I = I \text{ mod } 26$$

$$= Q$$

$$A=A \text{ mod } 26$$

= A
KB mod 26
= L
RA mod 26
= R
I = H mod 26
= P
S = T mod 26
= L
T = E mod 26
= X
I = R mod 26
= Z
N = N mod 26
= A
A = A mod 26
= A
R = M mod 26
= D
O = A mod 26
= O
N = R mod 26
= E
D = S mod 26
= V
A = I mod 26
= I
N = H mod 26
= U
G = I mod 26
= O
S = P mod 26
= H
I = U mod 26
= C

$T = L \text{ mod } 26$
= E
 $O = A \text{ mod } 26$
= O
 $R = U \text{ mod } 26$
= L
 $U = T \text{ mod } 26$
= N
 $S = E \text{ mod } 26$
W

b. Deskripsi

Chiptertext : DOJQA LRPLXZAA DOEVIUO HCEOLNW

Kunci : ROSIABAHTERNAMARSIHIPULAUTE

$D = R \text{ mod } 26$
= M
 $O = O \text{ mod } 26$
= A
 $J = S \text{ mod } 26$
= R
 $Q = I \text{ mod } 26$
= I
 $A = A \text{ mod } 26$
= A
 $L = B \text{ mod } 26$
= K
 $R = A \text{ mod } 26$
= R
 $P = H \text{ mod } 26$
= I
 $L = T \text{ mod } 26$
= S
 $X = E \text{ mod } 26$
= T
 $Z = R \text{ mod } 26$

= I
A = N mod 26
= N
A = A mod 26
= A
D = M mod 26
= R
O = A mod 26
= O
E = R mod 26
= N
V = S mod 26
= D
I = I mod 26
= A
U = H mod 26
= N
O = I mod 26
= G
H = P mod 26
= S
C = U mod 26
= I
E = L mod 26
= T
O = A mod 26
= O
L = U mod 26
= R
N = T mod 26
= U
W = E mod 26
= S

SIMPULAN

Di dalam menerapkan metode *vigenere Cipher* pengenkripsian pada tulisan teks nama di dalam data, dapat menghasilkan kode tulisan yang acak atau tidak dapat di mengerti oleh banyak orang. Di dalam pengujian ini satu nama diatas seperti MARIA KRISTINA RAMONDANG SITORUS telah diujikan dengan metode *vigenere Cipher* dapat dienkrispikan dengan hasil DOJQALRPLXZAA DOEVIUO HCEOLNW. Sebaliknya untuk dapat mengembalikan tulisan nama teks tersebut maka kunci yang terdapat pada kita, dapat digunakan sesuai dengan kunci awal dienkrripsi dan apabila kunci tersebut tidak sesuai dengan yang dipergunakan pada enkripsi maka tulisan teks didalam nama tersebut tidak dapat muncul dengan tulisan teks nama pada awalnya. oleh karena itu metode *vigenere Cipher* ini dapat menjaga data yang didalamnya tulisan atau bentuk teks.

DAFTAR PUSTAKA

- Wulan Permata Sari and Tata Sutabri, "Analisa Cluster Dengan K-Mean Clustering Untuk Pengelompokan Data Cybercrime," *J. Inform. Teknol. dan Sains*, vol. 5, no. 1, pp. 49–53, 2023, doi: 10.51401/jinteks.v5i1.2209.
- W. A. Triani, S. Nawari, and I. Abbas, "Efektivitas Layanan Elektronik Menurut Permen Agraria No. 1 Tahun 2021 Dalam Pemeliharaan Data Pendaftaran Tanah Di Kantor Pertanahan Kabupaten Gowa," *J. Lex Gen.*, vol. 4, no. 2, pp. 590–606, 2023.
- E. Novianto, E. I. Heri Ujianto, and R. Rianto, "Keamanan Informasi (Information Security) Pada Aplikasi Sistem Informasi Manajemen Kepegawaian Dengan Defense in Depth," *J. Komput. dan Inform.*, vol. 11, no. 1, pp. 1–6, 2023, doi: 10.35508/jicon.v11i1.9139.
- E. Susanto, H. Moses, R. Ramadan, and S. Dhenova, "ANALISIS KEAMANAN SISTEM INFORMASI MANAJEMEN DALAM PEMANFAATAN TEKNOLOGI INFORMASI TERHADAP PT BANK CENTRAL ASIA Tbk . (BCA)," vol. 1, no. 4, pp. 207–217, 2023.
- E. Susanto, Lady Antira, K. Kevin, E. Stanzah, and A. A. Majid, "Manajemen Keamanan Cyber Di Era Digital," *J. Bus. Entrep.*, vol. 11, no. 1, p. 23, 2023, doi: 10.46273/jobbe.v11i1.365.
- P. A. R. L. L. Indra Rambu Kandokang, Arini Aha Pekuwali, "Perancangan Sistem Pengamanan Data Pasien Menggunakan Metode Kriptografi Vigenère Cipher," *SATI Sustain. Agric. Technol. Innov.*, pp. 27–28, 2023.
- Wahyu Hidayat M *et al.*, "Analisa Clustering Phising Untuk Meningkatkan Kesadaran Mahasiswa Terhadap Keamanan Data Pribadi Mahasiswa Universitas Negeri Makassar," *Vokatek J. Pengabd. Masy.*, vol. 1, no. 1, pp. 28–33, 2023, doi: 10.61255/vokatekjmp.v1i1.29.
- K. Andrea, A. Wardana, B. S. Wanandi, and A. Ikhwan, "Penerapan Kriptografi Caesar Cipher

- Pada Fitur Aplikasi Chatting Whatsapp," *Januari*, vol. 2, no. 1, p. 6, 2023, [Online]. Available: <https://doi.org/10.47233/jppie.v2i1.660>.
- N. B. Samantha, S. Destya, and W. M. Ashari, "Perancangan Keamanan Pengguna Cardless dari Ancaman Cyber Crime Menggunakan Kriptografi Curva Elliptic," vol. 7, pp. 1706–1715, 2023, doi: 10.30865/mib.v7i4.6827.
- Z. Arif, A. Nurokhman, P. Studi, T. Informatika, and K. Data, "Analisis Perbandingan Algoritma Kriptografi Simetris Dan Asimetris Dalam Meningkatkan Keamanan Sistem Informasi," vol. 4, no. 2, pp. 394–405, 2023.
- R. Amalia, S. Assani', and M. A. Effindi, "Rancang Bangun Media Pembelajaran Algoritma Perograman Berbasis Android," *J. Ilm. Edutic Pendidik. dan Inform.*, vol. 9, no. 2, pp. 188–200, 2023, doi: 10.21107/edutic.v9i2.20215.
- R. Wandri, Suandi Daulay, Yudhi Arta, Anggi Hanafiah, and Jerika Mardafora, "Pengenalan Dan Pelatihan Algoritma Pemrograman Menggunakan Aplikasi Scratch Untuk Siswa SMK YKWI Pekanbaru," *J. Pengabd. Masy. dan Penerapan Ilmu Pengetah.*, vol. 4, no. 1, pp. 14–18, 2023, doi: 10.25299/jpmpip.2023.11966.
- S. S. Mukrimaa *et al.*, "Pengantar algoritma dan pemograman," *J. Penelit. Pendidik. Guru Sekol. Dasar*, vol. 6, no. August, p. 128, 2016.
- A. R. Ningtyas, A. M. Elhanafi, M. Khairani, R. Ningtyas, A. M. Elhanafi, and M. Khairani, "Paper Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi TTVC Dan OTP Berbasis Android Studio Perancangan Aplikasi Pengamanan Pesan Teks Menggunakan Algoritma Kombinasi TTVC Dan OTP."
- I. Introduction, "Implementasi Sandi Vigenere Cipher Dalam," vol. 1, no. 1, pp. 42–50, 2023.