**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

# PENGAMANAN PESAN TEKS MENGGUNAKAN KRIPTOFRAFI ALGORITMA VIGENERE CHIPER DARI SERANGAN EAVESDROPPING

**Benyamin Sihombing[1)], Dina Patresia Samuana Manrung [2)], Eko Ahadi[3)], Indra Gunawan[4)]**

*Program Studi Teknik Informatika*
*STIKOM Tunas Bangsa Pematangsiantar*
*Jl. Jend. Sudirman Blok A No.1, 2, dan 3, Pematang Siantar, Sumatera Utara (21143)*
*E-mail: benyaminssihombing@gmail.com[1], dinamanurung729@gmail.com[2], eko.ahady123@gmail.com[3], indra@amiktunasbangsa.ac.id[4]*

***ABSTRACT***

*The development of information technology is increasing rapidly, increasingly in communication and information. People often travel data or information with the help of technology, one of which is by using text messages. Security is very necessary so that threats such as piracy or eavesdropping on a message can prevent and not involve the parties concerned. Many attacks occur such as eavesdropping attacks that leak messages or information, but this can be overcome by using the vigenere cipher algorithm. This vigenere cipher cryptographic algorithm uses encryption and description processes to permit confidentiality of messages.*

***Keywords: eavesdropping, messages, cryptography, vigenere cipher, encryption, decryption.***

**ABSTRAK**

Perkembangan teknologi informasi semakin meningkat dengan pesat, terutama pada komunikasi dan informasi. Masyarakat sering melakukan pertukaran data atau informasi dengan bantuan teknologi, salah satunya adalah dengan menggunakan pesan teks. Keamanan sangat dibutuhkan agar ancaman seperti pembajakan atau penyadapan pada suatu pesan dapat dicegah dan tidak merugikan pihak-pihak yang berkepentingan. Banyak serangan-serangan terjadi seperti serangan eavesdropping yang mengakibatkan kebocoran pesan atau informasi, namun hal itu dapat diatasi dengan menggunakan algoritma kriptografi vigenere chiper. Algoritma kriptografi vigenere chiper ini menggunakan proses enkripsi dan deskripsi untuk menjaga kerahasiaan pesan.

**Kata Kunci : eavesdropping, pesan, kriptografi, vigenere cipher, enkripsi , dekripsi.**

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

## 1.PENDAHULUAN

Pada era teknologi komunikasi dan informasi saat ini, sebagian masyarakat tidak lagi melakukan komunikasi dengan pertemuan secara langsung atau bertatap muka. Salah satu alat komunikasi yang digunakan adalah teknologi, sehingga penggunaan pesan teks dapat sampai dari sisi pengirim ke sisi penerima dengan memudahkan kita terutama lebih efektif dan efisien. Pesan teks yang kita miliki dikirim dengan bebas melalui jaringan dengan tingkat kemanan yang relatif rendah. Dibutuhkan pengamanan yang dapat menjaga kerahasiaan pesan teks agar sampai kepada si penerima dengan aman dan tidak ada kebocoran atau serangan- serangan yang terjadi, seperti serangan eavesdropping. Perlu adanya pengamanan data pada pesan teks dengan menyandikan (mengenkripsikan) pesan yang akan dikirim. Teknik kriptografi yang dapat digunakan untuk menjaga kerahasiaan pesan teks yaitu algoritma vigenere chiper dengan proses enkripsi dan deskripsi.

### 1.1 Eavesdropping

Eavesdropping adalah penangkapan komunikasi antara dua titik oleh pihak yang tidak berwenang. Passive eavesdropping adalah ketika seseorang hanya menangkap dan mendengarkan pesan di dalam komunikasi jaringan secara diam-diam. Sedangkan active eavesdropping adalah ketika penyerang tidak hanya mendengarkan pesan, tetapi juga menyusupkan pesan ke dalam sistem komunikasi[1]. Hal ini dapat menyebabkan pesan menjadi kacau dan informasi yang sensitif dapat dicuri Tindakan ini dilakukan untuk mencuri data yang dikirim melalui jaringan tanpa dienkripsi terlebih dahulu.

## 2. METODE PENELITIAN

### 2.1 Kriptografi

Cryptography berasal dari dua kata Yunani, yaitu crypto yang berarti rahasia dan grapho yang berarti menulis. Secara umum cryptography dapat diartikan sebagai ilmu dan seni penyandian yang bertujuan untuk menjaga keamanan dan kerahasiaan suatu pesan. Cryptography pada dasarnya sudah dikenal sejak lama. Menurut catatan sejarah, cryptography sudah digunakan oleh bangsa mesir sejak 4000 tahun yang lalu oleh raja-raja Mesir pada saat perang untuk mengirimkan pesan rahasia kepada panglima perangnya melalui kurir-kurirnya [2].

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Teknik untuk mengacak-mengacak suatu pesan agar tidak dapat diketahui maknanya disebut enkripsi, dan membentuk suatu bidang keilmuan yang disebut Kriptografi. Prinsip dasarnya adalah menyembunyikan informasi sedemikian rupa agar orang yang berhak saja yang dapat mengetahui isi dari informasi yang tersembunyi tersebut [3].

Prinsip-prinsip yang mendasari kriptografi yakni:

1. *Confidelity* (kerahasiaan) yaitu layanan agar isi pesan yang dikirimkan tetap rahasia dan tidak diketahui oleh pihak

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

lain (kecuali pihak pengirim, pihak penerima / pihak-pihak memiliki ijin). Umumnya hal ini dilakukan dengan cara membuat suatu algoritma matematis yang mampu mengubah data hingga menjadi sulit untuk dibaca dan dipahami.

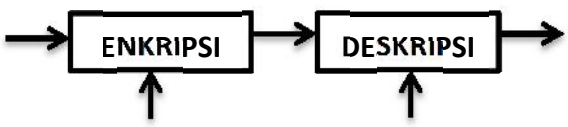
2. Data *integrity* (keutuhan data) yaitu layanan yang mampu mengenali/mendeteksi adanya manipulasi (penghapusan, pengubahan atau penambahan) data yang tidak sah (oleh pihak lain)
3. *Authentication*yaitu layanan yang berhubungan dengan identifikasi.
4. *Non-repudiation* (anti-penyangkalan) yaitu layanan yang dapat mencegah suatu pihak untuk menyangkal aksi yang dilakukan sebelumnya (menyangkal bahwa pesan tersebut berasal dirinya).

Berbeda dengan kriptografi klasik yang menitikberatkan kekuatan pada kerahasiaan algoritma yang digunakan (yang artinya apabila algoritma yang digunakan telah diketahui maka pesan sudah jelas "bocor" dan dapat diketahui isinya oleh siapa saja yang mengetahui algoritma tersebut), kriptografi modern lebih menitikberatkan pada kerahasiaan kunci yang digunakan pada algoritma tersebut (oleh pemakainya) sehingga algoritma tersebut dapat saja disebarkan ke kalangan masyarakat tanpa takut kehilangan kerahasiaan bagi para pemakainya.

Berikut adalah istilah-istilah yang digunakan dalam bidang kriptografi:

a. *Plaintext* (M) adalah pesan yang hendak dikirimkan (berisi data asli).
b. *Ciphertext*(C) adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi.
c. Enkripsi (fungsi E) adalah proses pengubahan plaintext menjadi *ciphertext*.
d. Dekripsi (fungsi D) adalah kebalikan dari enkripsi yakni mengubah ciphertext menjadi plaintext, sehingga berupa data awal/asli.
e. Kunci adalah suatu bilangan yang dirahasiakan yang digunakan dalam proses enkripsi dan dekripsi.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Enkripsi adalah suatu proses yang melakukan perubahan dari suatu kode yang bisa dimengerti menjadi tidak bisa dimengerti (tidak terbaca). Dekripsi adalah suatu proses dengan algoritma yang sama untuk mengembalikan informasi yang tidak bias dimengerti tadi menjadi bentuk aslinya [4]. Pada gambar 2.1. dijelaskan diagram proses enkripsi dan dekripsi




Gambar 1. Diagram Proses Enkripsi dan Deskripsi

Peranan kunci sangatlah penting dalam proses enkripsi dan dekripsi (disamping pula algoritma yang digunakan)

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

sehingga kerahasiaannya sangatlah penting, apabila kerahasiaannya terbongkar, maka isi dari pesan dapat diketahui.

### 2.2 Vigenere Cipher

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu Blaise de Vigenère, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553[5].

Vigenere cipher merupakan teknik kriptografi sederhana yang lebih aman. Dikembangkan dari metode caesar cipher, metode ini menggunakan karakter huruf sebagai kunci enkripsi. Vigenere cipher juga merupakan polyalphabetic substition cipher[6]. Karakter huruf yang digunakan pada vigenere cipher yaitu A, B, C, ..., Z dan disamakan dengan angka 0, 1, 2, ..., 25. Proses enkripsi dilakukan dengan menulis kunci secara berulang. Penulisan kunci secara berulang dilakukan hingga setiap karakter pada pesan memiliki pasangan sebuah karakter dari kunci. Selanjutnya karakter pada pesan dienkripsi menggunakan metode caesar cipher dengan nilai kunci yang telah dipasangkan dengan angka [7].

| | | |
|---|---|---|
| Plaintext | = | T U N A S B A N G S A |
| Key | = | S T I K O M V A M I K |
| Ciphertext K | = | L N V K G N V N S A |

Gambar 2. Contoh Enkripsi Menggunakan Vigenere Cipher

Contoh enkripsi pada Gambar 2, karakter pesan “T” dienkripsi dengan kunci “S” dan menghasilkan cipher text “L”. Hasil enkripsi didapatkan dari karakter pesan “T” bernilai 19 dan karakter kunci “S” yang bernilai 18 . Masing-masing nilai karakter ditambahkan 19 + 18 = 37. Karena 37 lebih besar dari pada 26 yang merupakan jumlah karakter yang digunakan, maka 37 dibagi dengan 26. Sisa pembagian tersebut adalah 11 yang merupakan nilai karakter “L”. Proses enkripsi dapat dihitung dengan persamaan berikut[8] :

$$Ei = (Pi + Ki)\ mod\ 26 \quad (2.3)$$

dimana $Ei$, $Pi$ dan $Ki$ merupakan karakter hasil enkripsi, karakter pesan dan karakter kunci. Sedangkan proses dekripsi dapat menggunakan persamaan berikut :

$$Di = (Ci - Ki)\ mod\ 26 \quad (2.4)$$

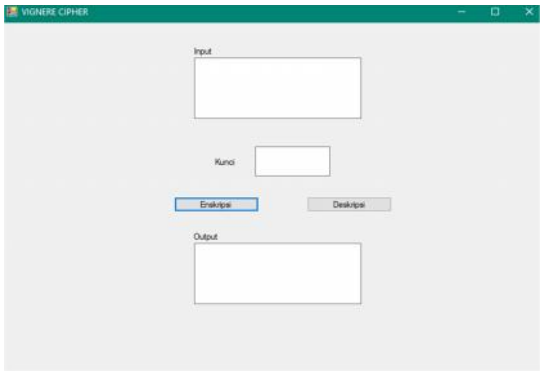
dengan $Di$ adalah karakter hasil dekripsi, $Ci$ adalah karakter cipher text atau sandi, $Ki$ adalah karakter kunci.

## 3.HASIL DAN PEMBAHASAN

Pada perancangan aplikasi enkripsi dan deskripsi data dengan menggunakan metode Vigenere Cipher terdapat tampilan form yang di desain dari Microsoft Visual Basic 2010 untuk memudahkan pemakai atau user dalam menggunakan aplikasi ini. Pada saat aplikasi Vigenere Cipher dijalankan, tampilan form akan muncul. Terdapat dua button yang disediakan pada

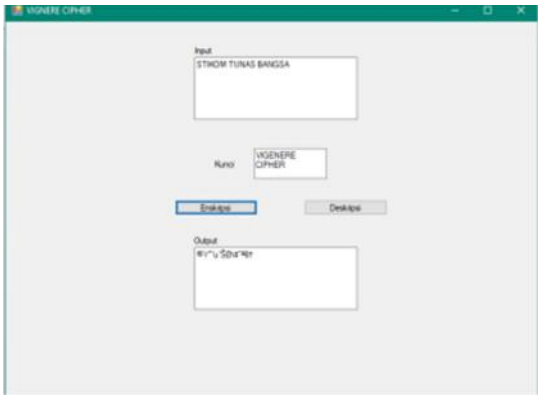
P-ISSN: 2548-9704
E-ISSN: 2686-0880

tampilan awal form, yaitu button enkripsi dan button deskirpsi.



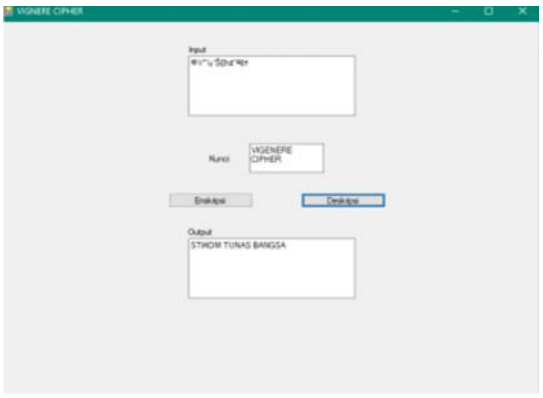

Gambar 3. Tampilan Form Vigenere Chiper

Gambar 3 input yang disediakan diisi dengan teks dan menghasilkan output dari hasil enkripsi dan deskripsi sesuai dengan kunci yang sudah ditentukan.




Gambar 4. Tampilan Form dari Hasil Enkripsi Data Text

Gambar 4 merupakan penginputan data teks berupa "STIKOM TUNAS BANGSA" dengan kunci yang sudah ditentukan, yaitu "VIGENERE CIPHER" sehingga output yang dihasilkan dari proses enkripsi adalah "© 'r™u'‰œp‡"¤ š†". Hasil dari ouput pengenkripsian merupakan sebuah ciphertext yang dienkripsikan dan untuk mengubah ciphertext menjadi plaintext dapat dilakukan dengan proses dekripsi.




Gambar 5. Tampilan Form dari Hasil Deskripsi Data Text

Gambar 5 Untuk proses pendeskripsian, hasil dari enskripsi pada output sebelumnya yang merupakan ciphertext, disalin pada input untuk dideskripsi dan menghasilkan output yang merupakan bagian plainteks pada saat proses enskripsi sebelumnya.

## 4. KESIMPULAN

Dalam Perancangan dan implementasi aplikasi ini, dapat disimpulkan bahwa:

1. Pengamanan data teks dengan menggunakan metode vigenere cipher sangat berguna dalam menjaga keamanan pesan teks dari serangan-serangan yang lain, seperti serangan eavesdropping.
2. Proses enkripsi dan deskripsi dirancang dalam aplikasi ini agar lebih menjaga kerahasiaan data dengan mengubah pesan asli (plaintext) menjadi pesan tersandi (ciphertext).

**P-ISSN: 2548-9704**
**E-ISSN: 2686-0880**

## 5.SARAN

1. Dalam pembuatan aplikasi ini dapat dikembangkan serta diharapkan dapat lebih berguna untuk menjaga dan menjamin kerahasiaan data
2. Membuat design lebih menarik agar user lebih minat menggunakan aplikasi ini
3. Menambahkan fitur-fitur penting pada aplikasi ini agar membuat user lebih tertarik

## DAFTAR PUSTAKA

[1]. Rajra M.B.B, J Deepa ME., 2015. A Survey on Network Security Attacks and Prevention Mechanism. Nagercoil. Departement of Computer Science Ponjesly College of Engineering Nagercoil.

[2]. Ariyus, Dony. 2006. *Kriptografi Keamanan Data dan Komunikasi. Yogyakarta: Graha Ilmu*

[3]. Wibowo, Ivan dkk. 2008. *Penerapan Algoritma Kriptografi Asimetris RSA untuk Keamanan Data di Oracle*. Fakultas Teknik, Universitas Kristen Duta Wacana.

[4]. WAHANAKomputer Semarang. 2003. *Memahami Model Enkripsi dan Security Data.* Yogyakarta: ANDI.

[5]. *Hallim, Abd, 2010, Pembuatan Perangkat Lunak Media Pembelajaran Kriptografi Klasik. Surabaya.Politeknik Eletronika Negeri.11 Hal*

[6]. Salomon, D. 2003. *Data Privacy and Security*. Springer-Verlag New York Inc.New York.

[7]. Katz, J. and Y. Lindell. 2015. *Introduction to Modern Cryptography.* 2nd ed. CRC Press. Boca Raton.

[8]. Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*. 5th ed. Pearson Education Inc. New York.