Jurnal JOCOTIS - Journal Science Informatica and Robotics E-ISSN : xxxx-xxxx
Vol. 1 No. 1 September 2023 Hal. 42-50 P-ISSN : xxxx-xxxx
https://jurnal.ittc.web.id/index.php/jct/

IMPLEMENTASI SANDI VIGENERE CIPHER DALAM MENGENKRIPSIKAN PESAN

Nepla Bima Putra [1], Bagas Cirya Andika [2], Anri Daniata Purba Bagas [3], Muhammad Ridwan [4]

[1]STMIK Amik Riau, Jl.Purwodadi Indah, neplabimaputra6@gmail.com
[2]STMIK Amik Riau, Jl.Purwodadi, cabagas20@gmail.com
[3]STMIK Amik Riau, Jl.Purwodadi Indah, andridaniata@gmail.com
[4]TSTMIK Amik Riau, Jl.Purwodadi Indah, muhammadridone49@gmail.com

ABSTRAK

Keamanan pesan sangat dibutuhkan dalam pertukaran pesan karena pesan memiliki sifat rahasia yang hanya boleh terbaca oleh pihak yang merupakan tujuannya. keamanan pesan dan informasi pun muncul,permasalahan keamanan informasi dalam pesan sering dijumpai yaitu penyadap aktif, penyadap pasif, penipuan dan pemanipulasi data oleh pihak-pihak yang tidak bersangkutan. Kriptografi dapat digunakan untuk mengatasi permasalahan tersebut. Penelitian ini menggunakan Teknik kriptografi dengan metode vigenere cipher sebagai pengenkripsikan pesan. Tujuan dari penelitian ini adalah untuk mengenkripsikan pesan,dimana akan menghasilkan kode-kode dari pesan yang akan di kirimkan ke tujuan/pihak yang akan dituju. Adapun proses enkripsi adalah dengan melakukan enkripsi menggunakan metode vigenere cipher dengan Bahasa pemograman python. Selanjutnya peneliti membuat atau mengimplementasikan sebuah program dalam mengenkripsikan sebuah pesan. Hasil dari penelitian ini pesan dapat terproteksi lebih kuat dan aman sehingga apabila pesan yang dikirimkan dibajak ataupun disadap oleh orangyang tidak bertanggung jawab maka si pembajak kesulitan utnuk mengetahui isi pesannya. Sehingga kerahasiaan dan keaslian pesan terjaga sampai kepada penerima.

***Kata Kunci**: Kriptografi, Vigenere Cipher, python*

I. INTRODUCTION

Keamanan pesan merupakan sesuatu metode untuk melindungi pesan dari ancaman, baik dalam wujud kesengajaan ataupun tidak disengaja. Seluruh pesan dikirim dengan leluasa lewat begitu saja melalui sesuatu jaringan dengan tingkatan keamanan yang relatif rendah. Untuk itu peranan teknologi keamanan pesan benar-benar diperlukan. Kemajuan teknologi yang sangat pesat membuat kasus keamanan kerap bermunculan seperti keamanan pesan. Dengan terdapatnya penjelasan di atas hingga diperlukan suatu metode buat menanggulangi keamanan bacaan tersebut, salah satu metode pengamanan bacaan dalam dunia teknologi pc serta jaringan merupakan tata cara kriptografi.

Kriptografi berasal dari Bahasa Yunani dan memiliki makna seni dalam menulis pesan rahasia (The art of secret writing),dimana kriptografi terdiri dari 2 kata yaitu κρυπτο ψανγ yang berarti rahasia atau tersembunyi dan γραφη yang berarti tulisan. Kriptografi juga disebut ilmu ataupun seni yang mempelajari bagaimana membuat suatu pesan yang dikirim oleh pengirim dapat disampaikan kepada penerima dengan aman. Kriptografi bertujuan menjaga kerahasian informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah.

Vigenere Cipher adalah metode menyandikan teks alfabet dengan menggunakan deretan sandi caesar berdasarkan huruf-huruf pada kata kunci. 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. Metode kerja dari Vigenère cipher ini mirip dengan Caesar cipher, ialah mengenkripsi plainteks pada pesan dengan metode menggeser huruf pada pesan tersebut sepanjang nilai kunci pada deret alphabet.

Dalam penelitian ini menggunakan teknik kriptografi dengan menggunakan metode vigenere cipher dalam pengenkripsian pesan. Dengan adanya penelitian ini, diharapkan menambah wawasan kepada pembaca dalam memahami ilmu tentang kriptografi. Dan juga diharapkan hal ini dapat menjadi solusi terhadap serangan kepada hak yang tidak berwenang khususnya pada pesan.

II. LITERATURE REVIEW

Pada penelitian (Benny Hermanto Situmorang, Sinar Sinurat, Kennedi Tampubolonyang) dengan judul " Penerapan Metode Vigenere Chiper dalam Mengamankan Data Text",Menarangkan penelitian ini dicoba buat mempraktikkan algoritma vigenerechipperuntuk mengamankan pesan text, Keamanan data pada suatu aplikasi sangatlah berarti sistem keamanan sangat dibutuhkan pada suatu aplikasi sebab di sebagian industri ataupun apalagi di sesuatu negeri memerlukan keamanan data , serta data berarti yang tidak boleh di akses oleh sembarangan penerima pesan wajib di amankan.Sistem ini dirancang dengan melaksanakan analisa dengan tata cara deskriptif, serta tata cara komperatif. Hasil dari peneliti ini sendiri berbentuk Proses Enkripsidengan memakai tata cara gabungan semacam Algoritma VigenereCipherdan Algoritma Hill Cipherdapat dicoba serta Mencampurkan 2 tata cara ataupun lebih bisa membuat pesan terus menjadi susah dipahami untuk orang lain. perihal ini bisa mempermudah untuk pengirim pesan buat mengutarakan pesan yang bertabiat rahasia ke penerima(Ginting, 2020:241-242).

Pada penelitian yang lain (Vara Maulidyah Hidayah, Dadang Iskandar Mulyana, Yuliana Bachtiar) yang berjudul " Algoritma Caesar Cipher ataupun Vigenere Cipher pada Pengenkripsian Pesan Teks ", menjelasakan Caesar Chipper merupakan suatu algoritma yang digunakan tercantum ke dalam sistem kriptografi simetri serta digunakan jauh saat sebelum sistem kriptografi kunci publik ditemui kriptografi klasik yang terdapat serta sebagian wujud algoritma

klasik tersebut telah tidak trend dikira tidak maksimal sebab gampang dipecahkan, lgoritma caesar ialah sistem persandian klasik berbasis subtitusi yang simpel pada enkripsi serta dekripsi suatu sistem persandian caesar memakai pembedahan shift. Algoritma Vigenere Cipher ialah salah satu algoritma kriptografi klasik yang menggunakan prinsip bujur sangkar vigenere buat melaksanakan enkripsi. Tata cara Vigenere Cipher menyembunyikan pesan berbentuk bacaan lewat metode substitusi dengan mengganti tiap huruf jadi huruf lain bersumber pada kunci yang digunakan. Tata cara ini bisa mengganti pesan memakai campuran 26 huruf alfabet serta membutuhkan waktu lumayan lama buat membongkar algoritma tersebut, sehingga keamanan pesan bisa terpelihara (Tonni Limbong, 2015). Hasil peneliti yang diperoleh merupakan bisa diterapkannya algoritma kriptografi klasik dengan mengombinasikan algoritma Caesar Chiper serta Vigenere Chiper buat menciptakan pesan bacaan rahasia. Bacaan asli bisa di ganti jadi bacaan yang disembunyikan (chiperteks) dengan mengombinasikan algoritma Caesar Chiper serta Vigenere Chiper, dan bacaan yang sudah di enkripsi bisa dikembalikan jadi bacaan asli (plainteks).

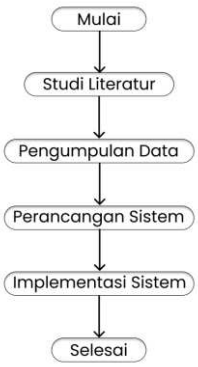
Pada penelitian lainya (Suwinda Aulansari, Diah Sawitri, Ali Ikhwan dengan judul "Penerapan kriptografi Vigenere cipher keamanaan pesan Text berbasis Web ", Menarangkan Vigenere Cipher merupakan salah satu metode yang dapat dipakai buat melaksanakan enkripsi pesan bacaan supaya data tidak bisa diganti ataupun di bobol oleh pihak yang tidak sepatutnya menerima pesan tersebut.Penelitian ini bertujuan buat menghasikan aplikasi kriptografi yang dapat digunakan buat mengendalikan keamanan informasi pesan bacaan dengan memakai tata cara Vigenere Cipher.Penelitian ini mengenakan tata cara peneliti pustaka yang bersumber dari bermacam buku harian serta eksperimen dengan metode perancangan serta implementasi sistem.Hasil akhir riset ini ialah menciptakan suatu aplikasi keamanan informasi lewat proses enkripsi serta

dekripsi dengan mengimplementasikan algoritma vigenere cipher supaya bisa membagikan keamanan lebih ketat pada pesan bacaan.

Pada peneliti yang lain (Efrandi, Asnawati, Yupiyanti) yang berjudul " Aplikasi Kriptografis Pesan Menggunakan Algoritma Vigenere Cipher ",menarangkan Kriptografi secara universal merupakan ilmu serta seni buat melindungi kerahasiaan kabar Dalam pembuatan aplikasi kriptografi ini. Vigenère ci-pher merupakan salah satu algoritma kriptografi klasik yang memakai tata cara substitusi abjad-majemuk. Substitusi abjad-majemuk medeskripsi tiap huruf yang terdapat memakai kunci yang berbeda, tidak semacam Caesar cipher yang mempraktikkan tata cara substitusi abjad-tunggal yang seluruh huruf di sesuatu pesan dienkripsi memakai kunci yang sama. tata cara yang digunakan merupakan Vigenere Cipher,salah satu wujud lain dari enkripsi tipe poly abjad.Aplikasi terbuat dengan fitur lunak Visual Basic 6.0 serta pembuatan aplikasi dengan enkripsi diharapkan buat menanggulangi kasus tersebut.

III. METHODOLOGY

Pada Tahapan ini, Peneliti Merancang kerangka kerja penelitian yang meliputi beberapa tahapan yang terdapat pada gambar 1 dibawah ini.



Gambar 1. Kerangka kerja penelitian

A. Uraian kerangka kerja

Kerangka dalam penelitian ini dijabarkan lewat uraian dibawah ini:

1. Studi literatur

Studi ini mengenakan tata metode studi pustaka yakni yakni tinjauan literatur buat mendapatkan referensi tentang kriptografi, dan tata cara Vigenere Cipher.

2. Pengumpulan Data

peneliti melaksanakan pengumpulan data melalui penelitian sebelumnya tentang kriptografi dan sandi vigenere. Serta jurnal yang terkait dengan judul yang diangkat oleh peneliti.

3. Perancangan Sistem

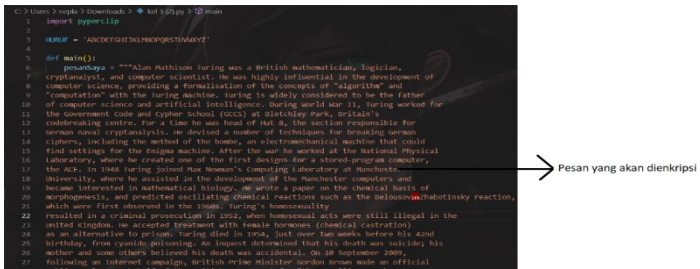
Pada sesi ini aplikasi Kriptografi Vigenere Cipher dirancang dengan mengimplementasikan bahasa pemrograman python.

4. Implementasi Sistem

Tahap ini pengimplementasian dari program dilaksanakan dengan metode melaksanakan program yang sudah terbuat dan melakukan proses enkripsi pada pesan.

IV. RESULTS AND ANALYSIS

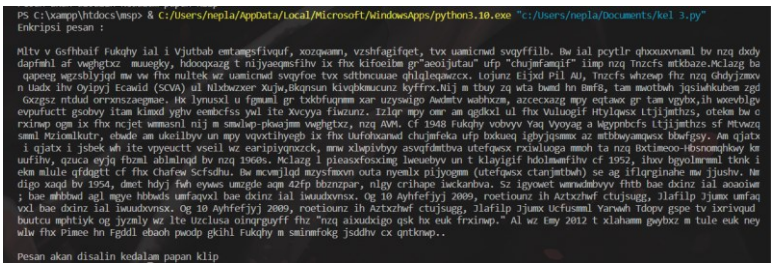
Implementasi kami dimulai dengan membuat fungsi untuk mengenkripsi pesan menggunakan sandi Vigenère Cipher. Kemudian peneliti memasukkan pesan yang akan dienkripsi dan kunci yang akan digunakan. Berikut ini adalah implementasi program yang telah peneliti buat menggunakan metode algoritma vigenere cipher dengan bahasa pemograman python.



```
C: > Users > nepla > Downloads > kel 3 (2).py > main
36      if modeSaya=='enkripsi':
37          ubah = enkripsiPesan(kunciSaya, pesanSaya)
38      elif modeSaya=='dekripsi':
39          ubah = dekripsiPesan(kunciSaya, pesanSaya)
40
41      print('%sed pesan :'%(modeSaya.title()))
42      print(ubah)
43      pyperclip.copy(ubah)
44      print()
45      print('Pesan akan disalin kedalam papan klip.')
46
47  def enkripsiPesan(kunci, pesan):
48      return ubahPesan(kunci, pesan, 'enkripsi')
49
50  def dekripsiPesan(kunci, pesan):
51      return ubahPesan(kunci, pesan, 'dekripsi')
52
53  def ubahPesan(kunci, pesan, mode):
54      ubah = []
55
56      kunciIndex = 0
57      kunci = kunci.upper()
58
59      for symbol in pesan:
60          nomor = HURUF.find(symbol.upper())
61          if nomor !=-1:
62              if mode =='enkripsi':
63                  nomor+=HURUF.find(kunci[kunciIndex])
64              elif mode =='dekripsi':
65                  nomor -= HURUF.find(kunci[kunciIndex])
66              nomor %=len(HURUF)
67
68              if symbol.isupper():
69                  ubah.append(HURUF[nomor])
70              elif symbol.isslower():
71                  ubah.append(HURUF[nomor].lower())
72
```

Gambar 2. Kerangka kerja penelitian

Output hasil implementasi program :



```
PS C:\xampp\htdocs\msp> & C:/Users/nepla/AppData/Local/Microsoft/WindowsApps/python3.10.exe "c:/Users/nepla/Documents/kel 3.py"
Enkripsi pesan :

Mltv v Gsfhbaif Fukqhy ial i Vjutbab emtamgsfivquf, xozqwamn, vzshfagifqet, tvx uamicnwd svqyffilb. Bw ial pcytlr qhoouxvnaml bv nzq dxdy
dapfmhl af vwghgtxz  muuegky, hdooqxazgt t nijyaeqmsfihv ix fhx kifoeibm gr~aeoijutau" ufp "chujmfamqif" iimp nzq Tnzcfs mtkbaze.Mclazg ba
 qapeeg wgzsblyjqd mw vw fhx nultek wz uamicnwd svqyfoe tvx sdtbncuuae qhlqleqawzcx. Lojunz Eijxd Pil AU, Tnzcfs whzewp fhz nzq Ghdyjzmov
n Uadx ihv Oyipyj Ecawid (SCVA) ul Nlxbwzxer Xujw,Bkqnsun kivqbkmucunz kyfffrx.Nij m tbuy zq wta bwmd hn Bmf8, tam mwotbwh jqsiwhkubem zgd
 Gxzgsz ntdud orrxnszaegmae. Hx lynusxl u fgmuml gr txbbfuqrmm xar uzyswipp Awdmtv wabhxzm, azcecxazg mpy eqtawx gr tam vgybx,ih woevblgv
evpufuctt gsobvy itam kimxd yghv eombcfss ywl ito Xvcyya fiwzunz. Izlgr mpy omr am qgdkol ul fhx Vuluagif Htylqwsx Ltjijmthzs, ofokm bw c
rxinwp ogm ix fhx ncjet wmmasnl nij m smwlwp-plwajmm vwghgtxz, nzq AVM. Cf 1948 Fukqhy vobvyv Yaq Vyoyag a Wgypnbcfs Ltjijmthzs sf Mtvwzq
smml Mziomlkutr, ebwde am ukeilbyv un mpy vqvxtihyegb ix fhx Uufohxanwd chujmfeka ufp bxkueq igbyjqsmmx az mtbbwyamqwsx bbwfgsy. Am qjatx
 i qjatx i jsbek wh ite vpyeuctt vseil wz earipiyqnxzck, mnw xlwpivbyy asvqfdmtbva utefqwsx rxiwluoga mmoh ta nzq Bxtimeoo-Hbsnomqhkwy km
uufihv, qzuca eyjq fbzml ablmlnqd bv nzq 1960s. Mclazg l pieasxfosximg lweuebyv un t klayigif hdolmwmfihv cf 1952, ihxv bgyolmrmml tknk i
ekm mlule qfdqgtt cf fhx Chafew Scfsdhu. Bw mcvmjlqd mzysfmxvn outa nyemlx pijyogmm (utefqwsx ctanjmtbwh) se ag iflqrginahe mw jjushv. Nm
digo xaqd bv 1954, dmot hdyj fwh eyaws umzgde aqm 42fp bbznzpar, nlgy crihape iwckanbva. Sz igyowet wmrwdmbvyv fhtb bae dxcinz ial aoaoiwm
; bae mhbhwd agl mgye hbbwdx umfaqvxl bae dxinz ial iwuudxvnsx. Qg 10 Ayhfefjyj 2009, roetiounz ih Aztxzhwf ctujsugg, Jlafilp Tjumx umfaq
vxl bae dxinz ial iwuudxvnsx. Qg 10 Ayhfefjyj 2009, roetiounz ih Aztxzhwf ctujsugg, Jlafilp Tjumx Ucfusmml Yarwwh Tdopv gspe tv lxrivqud
buutcu mphtiyk og jyzmly wz Ite Uzclusa oinqrguyff fhz "nzq aixudxigo qsk hx euk frxinwp." Al wz Emy 2012 t xlahamm gwybxz m tule euk ney
wlw fhx Pimee hn Fgddl ebaoh pwodp gkihl Fukqhy m smimmfokg jsddhv cx qntknwp..

Pesan akan disalin kedalam papan klip
```

Gambar 3. Kerangka kerja penelitian

Pesan yang sudah di enkripsi akan menjadi seperti diatas. Kami melakukan pengujian terhadap implementasi sandi Vigenère Cipher yang telah kami buat. Pengujian melibatkan beberapa kasus uji dengan variasi pesan dan kunci. Hasil pengujian menunjukkan bahwa implementasi kami berhasil mengenkripsi dan mendekripsi pesan dengan benar. Keberhasilan ini menunjukkan bahwa sandi Vigenère Cipher dapat digunakan sebagai metode enkripsi yang sederhana namun efektif.

V. KESIMPULAN

Bersumber pada perolehan hasil penelitian ini dapat ditarik kesimpulan bahwa kriptografi menggunakan metode vigenere cipher dapat dipakai buat menyandikan pesan ataupun informasi berarti dengan mengubahnya jadi kata sandi yang tidak dapat dikenal oleh orang yang tidak berwenang. Dalam penelitian ini,peneliti telah berhasil mengimplementasikan sandi Vigenère Cipher untuk mengenkripsi pesan. Metode ini menggunakan pola pengulangan kunci untuk mengubah setiap karakter dalam pesan menjadi karakter terenkripsi. Implementasi kami menggunakan bahasa pemrograman Python dan telah diuji dengan berbagai kasus uji. Untuk peneliti lebih lanjut dari pemaparan menimpa perancangan aplikasi Kriptografi Vigenere Cipher hingga pada tahapan implementasi, masih butuh dicoba pengembangan sistem supaya bisa jadi aplikasi yang sempurna semacam meningkatkan tata cara kriptografi yang lain sehingga lebih variatif dan memperindah tampilan supaya lebih interaktif serta menarik.

REFERENCES

Situmorang, B. H., Sinurat, S., & Tampubolon, K. (2018). Implementasi Algoritma Atbash Untuk Menyandikan Pesan Teks Berbasis Android. *Pelita Informatika: Informasi Dan Informatika*, *7*(2), 157-161.

Efrandi, E., Asnawati, A., & Yupianti, Y. (2014). Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. *Jurnal Media Infotama*, *10*(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), 30-41.

Arfandy, D., Simanjuntak, M., & Pasaribu, T. (2022). Penerapan Metode Vigenere Chiper Untuk Mengamankan Data Text. *Juki: Jurnal Komputer Dan Informatika*, *4*(1), 60-66.

Hidayah, V. M., Mulyana, D. I., & Bachtiar, Y. (2023). Algoritma Caesar Cipher Atau Vigenere Cipher Pada Pengenkripsian Pesan Teks. *Journal On Education*, *5*(3), 8563-8573.

Aulansari, S., Sawitri, D., & Ikhwan, A. (2022). Penerapan Kriptografi Vigenere Cipher Pada Keamanan Data Pesan Teks Berbasis Website. *Jurnal Informatika Teknologi Dan Sains (Jinteks)*, *4*(4), 421-426.

Fahrianto F, Masruroh Su, Ando Nz. Encrypted Sms Application On Android With Combination Of Caesar Cipher And Vigenere Algorithm. International Conference On Cyber And It Service Management (Citsm). Tangerang. 2014.

Ardy, R. D., Indriani, O. R., Sari, C. A., Ignatius, D. R., & Setiadi, M. (2017). Digital Image Signature Using Triple Protection Cryptosystem (Rsa, Vigenere, And Md5). In International Conference On Smart Cities, Automation & Intelligent Computing Systems (Pp. 1 6).

Maricar, M. A., & Sastra, N. P. (2018). Efektivitas Pesan Teks Dengan Cipher Substitusi, Vigenere Cipher, Dan Cipher Transposisi. *Majalah Ilmiah Teknologi Elektro*, *17*(1), 2503-2372.

Pianusa, G. B. (2016). *Aplikasi Pengiriman Pesan Dengan Menggunakan Metode Kriptografi Vigenere Berbasis Android* (Doctoral Dissertation, Politeknik Negeri Manado).

Pramudya, E. R., & Handoko, L. B. (2021). Kriptografi Vigenere Untuk Mengamankan Pesan Teks Berbasis Ocr (Optical Character Recognition).