Terbit *online* pada laman web jurnal : http://ejournal.upbatam.ac.id/index.php/comasiejournal

Jurnal Comasie

ISSN (Online) 2715-6265

PERANGKAT LUNAK KEAMANAN BERBASIS FILE MENGGUNAKAN ALGORITMA KRIPTOGRAFI VIGENERE CIPHER

Edi Susanto[1], Sestri Novia Rizki[2]

[1] Mahasiswa Program Studi Teknik Informatika, Universitas Putera Batam
[2] Dosen Program studi Teknik Informatika, Universitas Putera Batam
e-mail: pb140210196@upbatam.ac.id

ABSTRACT

Security is an important aspect of an information system. Many people do not know how to secure files that are created or received or do not know how to protect files that are created or received so that there is no theft of files that cause information from those files to leak. Every organization, industry, or infrastructure, needs a level of network security solution to protect against the growing hacker threats in today's world. Text files that contain information in text form. Data originating from word processing documents, numbers used in calculations, names and addresses in the database are examples of text data input consisting of characters, numbers and punctuation marks. Input and output text data is represented as a character set or code system recognized by the computer system. Cryptography is a science that studies how to keep data safe when sent, from sender to receiver without experiencing interference from third parties. Vigenere Cipher is method of encrypting alphabetic text using letter and numbers. This table is usually referred to as the Vigenere Table. The concept of cryptography itself has long been used by humans, for example in the Egyptian and Roman civilizations, although it is still very simple.

Keywords: Cryptography; Files; Security; Vigenere Cipher.

PENDAHULUAN

Keamanan jaringan menjadi lebih penting bagi pengguna komputer pribadi, organisasi, dan militer. Dengan munculnya internet, keamanan menjadi perhatian utama dan memungkinkan keamanan menjadi lebih baik dengan pemahaman tentang munculnya teknologi keamanan. (Funmilola dan Oluwafemi, 2015). Keamanan merupakan salah satu aspek yang penting dalam sebuah sistem informasi. Banyak orang yang tidak tahu bagaimana cara mengamankan berkas yang dibuat atau diterimanya atau tidak tahu bagaimana cara melindungi berkas yang dibuat atau diterimanya agar tidak terjadi pencurian berkas yang menyebabkan bocornya informasi dari berkas tersebut. Kriptografi adalah ilmu yang mempelajari bagaimana menjaga keamananan suatu pesan (*plaintext*). Tugas utama kriptografi adalah untuk menjaga agar baik pesan atau kunci ataupun keduanya tetap terjaga kerahasiaannya dari penyadap (*attacker*).

Vigenere Cipher adalah *cipher* blok polialfabetik, tetapi jika dilihat dengan cara lain, ini adalah *stream cipher* yang merupakan generalisasi alami dari sandi

geser (Smart, 2013). *Vigenere Cipher* merupakan bentuk pengembangan dari *caesar cipher*. Kelebihan sandi ini dibanding *Caesar Cipher* dan *cipher* polialfabetik lainnya adalah *cipher* ini tidak begitu rentan terhadap metode pemecahan *cipher* yang disebut analisis frekuensi. *Cipher* ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. Pada penelitian ini penulis menemukan adanya permasalahan di PT. Pioneer Offshore Indo Raya. Penulis menemukan adanya masalah keamanan pada *file* penting perusahaan yang tidak diamankan dengan baik. *File* penting yang harus dijaga kerahasiannya, seperti dokumen perusahaan, dokumen pribadi dan lainnya. Sehingga mengharuskan karyawan untuk lebih waspada ketika *file* tersebut diambil oleh orang yang tidak bertanggung jawab. *File* ini bisa saja dicuri dan diubah oleh orang yang ingin mengetahui rahasia perusahaan melalui jaringan atau wifii yang sama. Sehingga diperlukan perangkat lunak yang bisa menjaga kerahasiaan dan keamanan dokumen tersebut. khususnya untuk pekerja kantor agar dapat diterima dengan aman dari pengirim dan penerima tanpa gangguan dari pihak yang tidak bertanggung jawab.

KAJIAN TEORI

2.1 Teori Dasar

Jaringan komputer adalah sebuah kumpulan dari komputer, *printer*, dan peralatan lainnya yang terhubung dalam satu kesatuan dan membentuk suatu sistem tertentu. (Maslan,Andi dan Wangdra,Tonny, 2012). Jaringan komputer dibangun dengan mengkombinasikan antara *hardware* dan *software*. Dua buah komputer yang masing-masing memiliki sebuah kartu jaringan, kemudian dikoneksikan melalui kabel maupun tanpa kabel (*nirkabel*) sebagai media transmisi data, dan terdapat *software* sistem operasi jaringan akan membentuk sebuah jaringan yang sederhana. Tidak semua jaringan komputer sama. Jaringan yang penulis gunakan untuk menghubungkan laptop ini ke router nirkabel, printer, dan peralatan lain adalah yang terkecil yang bisa dibayangkan. Jika bekerja di kantor, jaringan tersebut menggunakan *LAN (Local Area Network)*, biasanya merupakan beberapa komputer terpisah yang terhubung ke satu atau dua *printer, scaner*, dan satu koneksi ke Internet. Jaringan bisa lebih besar dari ini. Di sisi lain ada juga *MAN (Metropolitan Area Network),* yang mencakup seluruh kota, dan *WAN (Wide Area Network)*, yang dapat mencakup area geografis mana pun. Internet adalah *WAN* yang mencakup seluruh dunia.

2.2 Teori Khusus

Keamanan jaringan

Keamanan jaringan menjadi lebih penting bagi pengguna komputer pribadi, organisasi, dan militer. Dengan munculnya internet, keamanan menjadi perhatian utama dan memungkinkan keamanan menjadi lebih baik dengan pemahaman tentang munculnya teknologi keamanan. (Funmilola & Oluwafemi, 2015). Setiap organisasi, terlepas dari ukuran, industri, atau infrastruktur, membutuhkan tingkat solusi keamanan jaringan untuk melindungi dari ancaman *hacker* yang terus tumbuh di dunia saat ini. Arsitektur jaringan saat ini sangat kompleks dan dihadapkan dengan lingkungan ancaman yang selalu berubah dan penyerang yang selalu berusaha menemukan dan mengeksploitasi kerentanan. Kerentanan ini terdapat di sejumlah area, termasuk perangkat, data, aplikasi, pengguna, dan lokasi. Jenis-jenis Umum dari Serangan Keamanan Jaringan

1. Serangan *Phishing*

Definisi *phising* yaitu aktivitas seseorang untuk mendapatkan informasi rahasia pengguna dengan cara menggunakan *email* dan situs palsu yang tampilannya menyerupai tampilan asli atau resmi situs sebenarnya. (Rachmawati, 2014). Itu terjadi ketika seorang penyerang menyamar sebagai individu terpercaya, menipu korban untuk membuka pesan teks, email, atau pesan instan. Korban kemudian ditipu untuk membuka tautan jahat yang dapat menyebabkan pembekuan sistem sebagai bagian dari serangan *ransomware*, mengungkapkan informasi sensitif, atau pemasangan *malware*. Bagi seorang individu, ini

termasuk pencurian identitas, pencurian uang, atau pembelian tanpa izin. Phishing sering digunakan untuk mendapatkan celah di jaringan pemerintah atau perusahaan sebagai bagian dari plot yang lebih signifikan seperti *advanced persistent threat (APT).* Dalam kasus seperti itu, karyawan dikompromikan untuk mendapatkan akses istimewa ke data aman, mendistribusikan *malware* di lingkungan tertutup, dan memintas parameter keamanan.

2. Serangan *Spear Phishing*

Spear phishing adalah *email* yang ditargetkan pada individu atau grup tertentu, bukan mengirim spam ke pengguna acak. *Spear phishing* biasanya diawali dengan perencanaan yang matang ke calon korbannya. Penyerang kemudian dapat mengirim pesan yang tampak seperti asli dari sumber yang terpercaya. (Sagar, Shivani, & Chakravarty, 2019). Peretasan ini tidak dilakukan oleh penyerang acak tetapi kemungkinan besar dilakukan oleh orang-orang yang keluar karena rahasia dagang, keuntungan finansial, atau intelijen militer. *Email spear phishing* tampaknya berasal dari seseorang di dalam organisasi penerima sendiri atau seseorang yang dikenal secara pribadi oleh target. Cukup sering peretas yang disponsori pemerintah melakukan kegiatan ini. Penjahat dunia maya juga melakukan serangan ini dengan tujuan menjual kembali data rahasia ke perusahaan swasta dan pemerintah. Penyerang ini menggunakan rekayasa sosial dan pendekatan yang dirancang secara individual untuk mempersonalisasi situs web dan pesan secara efektif.

3. Serangan *Malware*

Malware adalah istilah umum yang digunakan untuk mewakili berbagai bentuk perangkat lunak berbahaya, Perangkat lunak apa pun sengaja didesain untuk niat buruk bisa dikategorikan sebagai *malware*. (D, Vijayanand C S, dan Arunlal K, 2019). Definisi luas ini mencakup banyak jenis perangkat lunak jahat *(malware)* tertentu seperti *spyware*, *ransomware*, perintah, dan kontrol. Banyak pelaku bisnis dan pelaku kriminal yang terkenal telah terlibat dan menemukan penyebaran *malware*. *Malware* berbeda dari perangkat lunak lain karena dapat menyebar ke seluruh jaringan, menyebabkan perubahan dan kerusakan, tetap tidak terdeteksi, dan gigih dalam sistem yang terinfeksi. Itu dapat menghancurkan jaringan dan membuat kinerja mesin bertekuk lutut. Dalam sebuah bisnis, administrator keamanan sistem dapat mengurangi efektivitas peretasan seperti itu dengan mendorong staf manajemen perusahaan untuk menghadiri pelatihan kesadaran keamanan.

4. Trojan Horse

Trojan horse adalah program berbahaya yang dapat merepresentasikan dirinya dengan menyamar sebagai program biasa, program ini digunakan untuk mengelabui korbannya. (Okereke & Chukwunonso, 2018). *Trojan horse* biasanya membawa fungsi tersembunyi yang diaktifkan saat aplikasi dimulai. . Mereka menyebar dengan terlihat seperti perangkat lunak rutin dan membujuk korban untuk menginstal. *trojan horse* dianggap sebagai salah satu jenis *malware* yang paling berbahaya, karena sering dirancang untuk mencuri informasi keuangan.

5. Serangan *Distributed Denial-of-Service (DDoS)*

Distributed Denial-of-service (DDoS) adalah upaya untuk menghabiskan *bandwidth* korban atau mengganggu akses pengguna ke layanan internet. (Prasad, Reddy, & Rao, 2014). Serangan ini mempunyai misi yaitu dengan membanjiri target dengan *bandwidth* atau membanjirinya dengan informasi yang memicu kerusakan. Dalam kedua situasi tersebut, serangan *DDoS* menyangkal pengguna yang sah seperti karyawan, pemegang akun, dan anggota sumber daya atau layanan yang mereka harapkan.

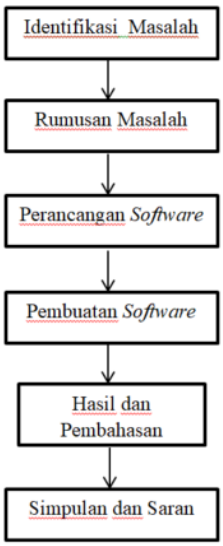
Vigenere Cipher adalah *cipher* blok polialfabetik, tetapi jika dilihat dengan cara lain, ini adalah *stream cipher* yang merupakan generalisasi alami dari sandi geser (Smart, 2013). *Vigenere Cipher* merupakan bentuk pengembangan dari

caesar cipher. Kelebihan sandi ini dibanding *caesar cipher* dan *cipher* polialfabetik lainnya adalah *cipher* ini tidak begitu rentan terhadap metode pemecahan *cipher* yang disebut analisis frekuensi. *Cipher* ini dikenal luas karena cara kerjanya mudah dimengerti dan dijalankan, dan bagi para pemula sulit dipecahkan. *Vigenere Cipher* adalah metode mengenkripsi teks alfabet dengan menggunakan huruf/ tabel dan angka. Tabel ini biasanya disebut sebagai *vigenere table*, *vigenere table* atau *vigenere square*. Penulis akan menggunakan Tabel *vigenere*. Baris pertama tabel ini memiliki 26 huruf alfabet. Dimulai dengan baris kedua, setiap baris memiliki huruf bergeser ke posisi satu kiri. Misalnya, ketika B digeser ke posisi pertama di baris kedua, huruf A bergerak ke akhir.

METODE PENELITIAN

3.1 Desain penelitian

Penelitian adalah suatu penyelidikan terorganisasi, atau penyelidikan yang hati-hati dan kritis dalam mencari fakta untuk menentukan sesuatu. (Siyoto, 2015) Penelitian dilakukan melalui tahapan-tahapan kegiatan dengan mengikuti kerangka berpikir. Berikut ini adalah alur desain penelitian :



Gambar 1. Desain Penelitian
(Sumber : Data penelitian 2021)

1. Identifikasi Masalah

Pada identifikasi masalah penulis ingin melakukan identifikasi terlebih dahulu dengan permasalahan yang ada di lapangan. Sangat jarang sekali pengguna mengamankan *file* nya. Banyak pengguna tidak mengetahui pentingnya menjaga sebuah data.

2. Rumusan Masalah

Pada rumusan masalah penulis ingin melakukan gambaran terhadap masalah yang dialami di lapangan. Cara mengamankan file berformat *(*.txt, *.pdf, *.xls dan *.doc)* menggunakan algoritma kriptografi *vigenere ci*pher. Cara merancang perangkat lunak sistem enkripsi dan dekripsi agar *file* pengguna aman.

3. Perancangan *Software*

Perancangan *software* digunakan untuk menciptakan tampilan yang mudah digunakan dan dipahami oleh pengguna. Pada perancangan ini yang digunakan terdapat dua tampilan yaitu tampilan awal *software* dan tampilan untuk enkripsi dan dekripsi *file*.

Bahasa pemrograman yang digunakan pada penelitian ini menggunakan bahasa pemrograman java dan dibangun menggunakan perangkat lunak IntelijIdea. Hasil dari bahasa program dapat dilihat pada halaman lampiran.

4. Hasil dan Pembahasan

Pada hasil dan pembahasan akan berisi hasil dari penelitian meliputi hasil perancangan *software* yang dibuat dan juga pembahasan mengenai kriptografi *Vigenere Cipher* dapat mengamankan *file* berformat **.txt, *.doc, *.xls, *.pdf*.

5. Simpulan dan Saran

Pada simpulan dan saran akan berisi simpulan mengenai program yang dibuat menggunakan algoritma krptografi *Vigenere Cipher*, dan kelebihan serta kekurangan *software* yang dibuat oleh penulis.

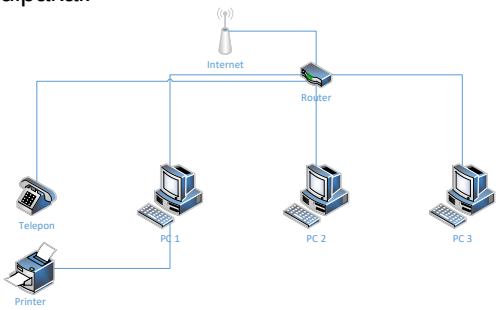
3.2 Analisis Jaringan Lama/ yang Sedang Berjalan

Pada analisis jaringan lama/ yang sedang berlangsung penulis akan menjelaskan tentang jaringan yang dipakai, *OS* yang sedang dipakai dalam

menjalankan sebuah *file* atau menyimpan *file* di PT. Pioneer Offshore Indo Raya.

Jaringan yang dipakai

Jaringan yang dipakai adalah internet yang dihubungkan dengan router, router yang menghubungkan ke beberapa komputer dalam sebuah perusahaan. Berikut adalah gambar dari jaringan yang dipakai.



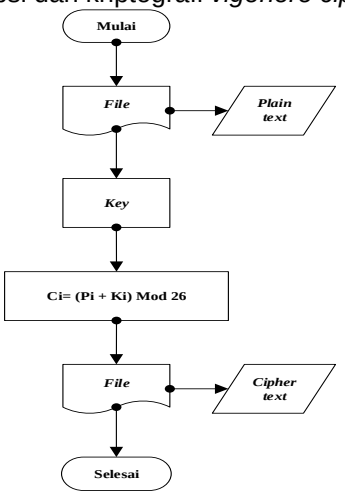
Gambar 2 Jaringan perusahaan
(Sumber : Data penelitian 2021)

3.3 Rancangan Jaringan yang Dibangun/ Diusulkan

Pada rancangan jaringan yang sedang dibangun/ diusulkan penulis akan menjelaskan tentang *flowchart* kriptografi *vigenere cipher,*diagram *usecase* diagram *activity*, *software* yang dipakai dalam menjalankan sebuah *file* atau menyimpan *file* di PT. Pioneer Offshore Indo Raya.

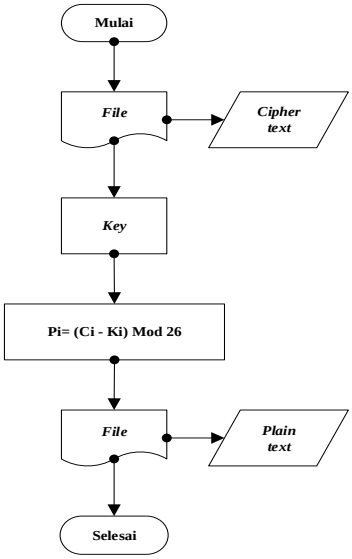
1. *Flowchart* Kriptografi *Vigenere Cipher*

Berikut ini adalah *flowchart* enkripsi dan dekripsi dari kriptografi *vigenere cipher*.



Gambar 3 Proses Enkripsi Kriptografi *Vigenere Cipher*
(Sumber : Data penelitian 2021)

Pada awal proses enkripsi mulanya kita memasukkan *file* berformat (**,pdf, *.xls, *.doc, dan *.txt*) ke program yang sudah dijalankan *file* ini dibsebut *plaintext.* Selanjutnya program akan mengeksekusi p*laintext* ke *ciphertext* dengan kunci. Setelah dieksekusi dengan kriptografi *vigenere cipher, file* yang keluar berupa *ciphertext* yang tidak bisa dibuka.



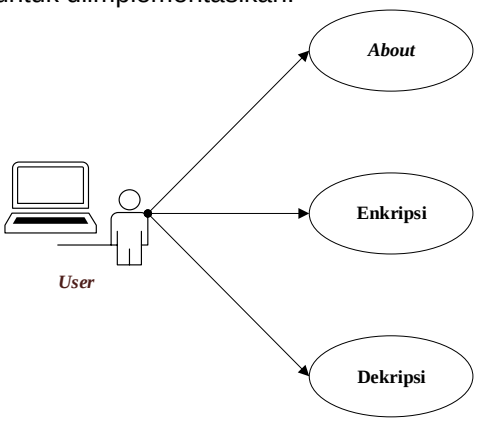
Gambar 4 Proses Dekripsi Krptografi *Vigenere Cipher*
(Sumber : Data penelitian 2021)

Ketika pengguna ingin membuka *file* yang terenkripsi, proses awal yang dilakukan adalah memasukkan *file* yang terenkripsi terlebih dahulu. Selanjutnya isi kunci yang sama pada proses enkripsi, maka *file* akan didekripsi dengan kriptografi *vigenere cipher*. Setelah didekripsi *file* akan berubah ke asalnya atau disebut juga dengan *plaintext*.

2. Diagram *Use Case*

Use case merupakan sebuah konstruksi untuk menggambarkan hubungan yang terjadi antara aktor dan kegiatan yang terkandung dalam sistem. Kasus penggunaan pemodelan target adalah untuk menentukan kebutuhan fungsional dan operasional sistem dengan menentukan skenario penggunaan sistem yang akan dibangun. Dari output analisis perangkat lunak yang ada

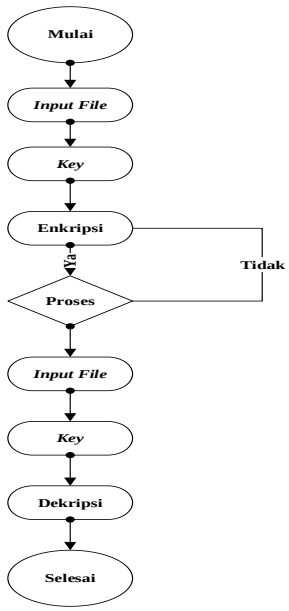
kemudian menggunakan diagram kasus untuk diimplementasikan.



Gambar 5 Diagram *Use case*
(Sumber : Data penelitian 2021)

3. Diagram *Activity*

Pada *activity* diagram dimulai dengan memasukkan *file* yang ingin di enkripsi ke perangkat lunak, masukkan *key* dan klik enkripsi. *File* yang terenkripsi kemudian menjadi sebuah *file* tidak dapat dibaca. Selanjutnya jika ingin mengembalikan seperti semula *file* enkripsi harus dimasukkan terlebih dahulu beserta *key*. Klik dekripsi maka *file* akan kembali seperti semula.



Gambar 6 Diagram *Activity*
Sumber : (Data penelitian 2021)

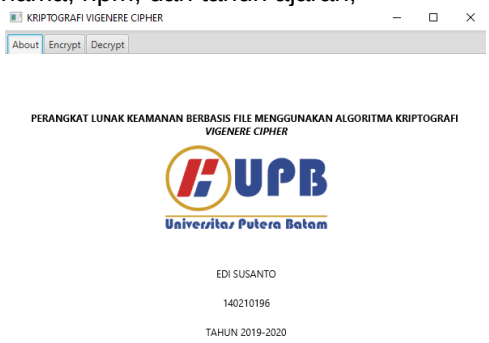
HASIL DAN PEMBAHASAN

4.1 Hasil

Hasil penelitian yang dibahas adalah hasil dari enkripsi *file* perusahaan dan dekripsi *file* perusahaan menggunakan perangkat lunak dengan algoritma kriptografi *vigenere cipher.*

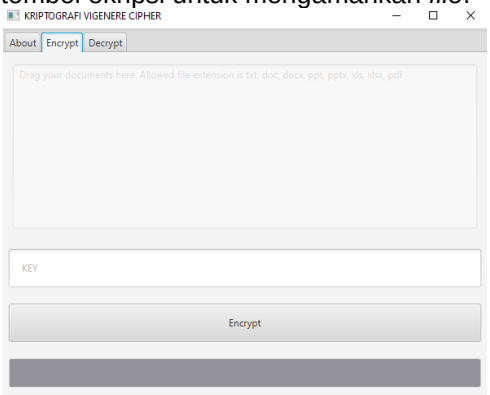
1. Tampilan Perangkat Lunak

Tampilan pada menu *about* berisi tentang informasi penulis berupa judul skripsi, foto universitas putera batam, nama, npm, dan tahun ajaran,



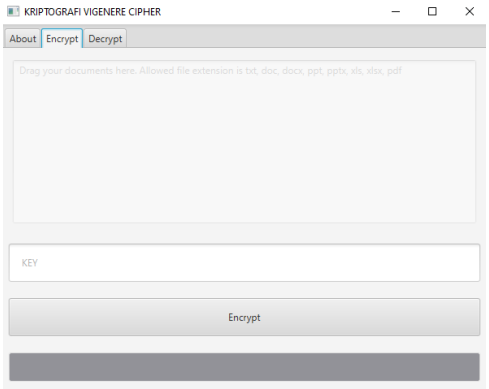
Gambar 7 Tampilan *about*
(Sumber : Data penelitian 2021)

Tampilan menu enkripsi berupa *file* yang akan dimasukkan ke perangkat lunak, *key* yang akan dimasukkan dan juga tombol ekripsi untuk mengamankan *file*.



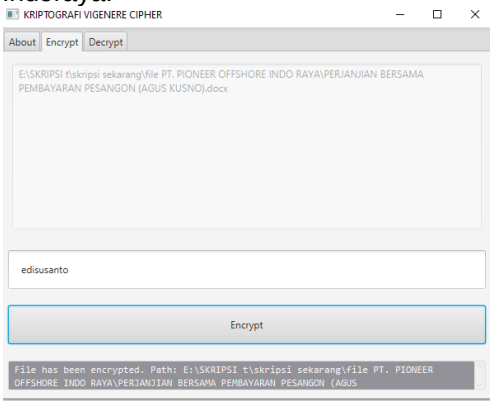
Gambar 8 Tampilan Enkripsi
(Sumber : Data penelitian 2021)

Tampilan menu dekripsi berupa *file* yang akan dimasukkan ke perangkat lunak, *key* yang akan dimasukkan dan juga tombol dekripsi untuk mengamankan *file*.



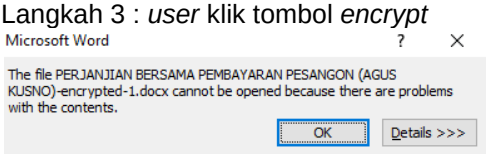
Gambar 9 Tampilan Dekripsi
(Sumber : Data penelitian 2021)

2. Pengujian Perangkat Lunak
Pada pengujian perangkat lunak berisi tentang hasil enkripsi dan dekripsi *file* yang ingin diamankan.
Pengujian 1
Pada penjgujian pertama, penulis memasukkan *file* berformat **.doc. File* ini didapatkan dari PT. Pioneer Offshore Indoraya.



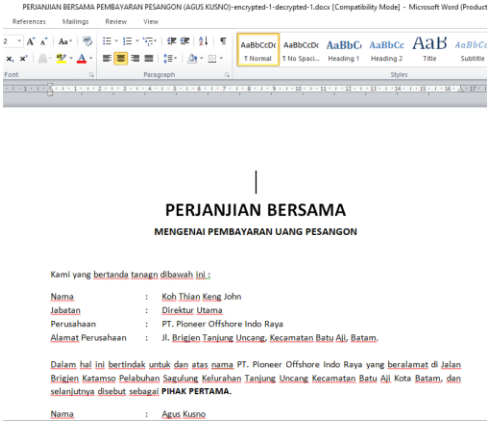
Gambar 10 Enkripsi *File* berformat **doc*
(Sumber : Data penelitian 2021)

Proses enkripsi pada *file *doc* menggunakan algoritma kriptografi *vigenere cipher*. *File* didapat dari PT. Pioneer Offshore Indoraya :
Langkah 1 : *user* memilih *file *doc* yang ingin dienkripsi
Langkah 2 : *user* memasukkan *key* terlebih dahulu
Langkah 3 : *user* klik tombol *encrypt*
Langkah 3 : *user* klik tombol *encrypt*



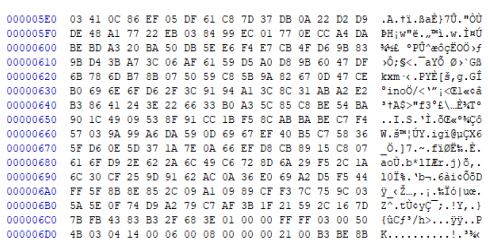
Gambar 11 Hasil Enkripsi *File* berformat **doc*
(Sumber : Data penelitian 2021)

Hasil dari enkripsi *file *doc* tidak bisa dibuka pada microsoft word karena *file* telah diamankan dengan kriptografi *vigenere cipher.*
Pada proses dekripsi pada *file* berformat **.doc* langkah-langkah yang digunakan sama saja dendan proses enkripsi, akan tetapi jika memasukkan kunci yang berbeda maka hasil dari *file* dekripsi tidak akan bisa dibuka. Kunci yang dimasukkan pada proses dekripsi harus sama dengan kunci yang dimasukkan pada proses enkripsi agar *file* yang didekripsi bisa kembali ke *file* asli.

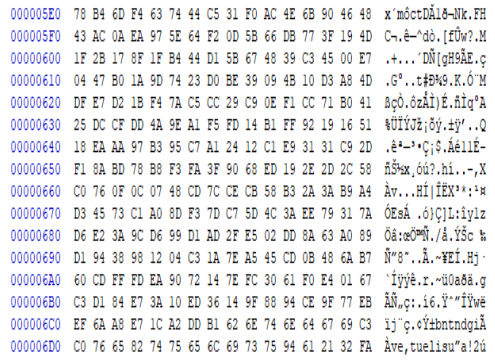


Gambar 12 Hasil Dekripsi *File* berformat **doc*
(Sumber : Data penelitian 2021)

Hasil dari dekripsi *file *doc* bisa dibuka kembali pada microsoft word seperti *file* asli.
Berikut ini adalah hasil perbandingan struktur *file* asli dan *file* yang telah dienkripsi dengan menggunakan algoritma kriptografi *vigenere cipher* dalam bentuk hexadecimal.



Gambar 13. Stuktur *File* asli berformat **doc*
(Sumber : Data penelitian 2021)



Gambar 14. Stuktur *File* enkripsi berformat **doc*
(Sumber : Data penelitian 2021)

File pada format **doc* dapat terlihat jelas perbedaannya, sehingga pada saat file terenkripsi tidak dapat dibuka.

4.2. Pembahasan

Pada pembahasan kali ini berisi tentang pembahasan hasil peneliatian dari perangkat lunak dalam melakukan proses enkripsi dan dekripsi pada setiap format.

1. Hasil enkripsi dan dekripsi *file* format **doc, *pdf, dan *xls*

Enkripsi pada *file* berformat **doc* sangat aman dan tidak bisa dibuka pada *microsoft word*, sehingga untuk pelaku pencurian *file* atau penyusup yang ingin mengambil file ini dia tidak akan bisa membaca isi dari *file* tersebut. Pada enkripsi *file* berformat **pdf* juga tidak bisa dibuka pada *adobe reader*, pelaku pencurian *file* atau penyusup tidak akan bisa membaca *file* yang sudah terenkripsi itu. Pada *file* berformat **xls*, *file* dienkripsi dengan perangkat lunak algoritma kriptografi *vigenere cipher*. Hasil dari enkripsi *file* berformat **xls* tidak akan bisa dibaca oleh pelaku pencurian *file* atau penyusup yang ingin mencuri *file* tersebut. Pada *file* berformat **.txt, file* yang sudah terenkripsi bisa di buka pada notepad namun hasilnya berupa huruf yang sudah terenkripsi. Penyusup tidak akan bisa membaca *file* itu. Terlihat juga bahwa struktur *file* pada masing-masing format dalam hexadesimal sangat berbeda dan struktur *file* yang sudah terenkripsi tidak bisa dibuka.

SIMPULAN

Berdasarkan hasil penelitian dan pembahasan dapat disimpulkan melalui kajian ini , antara lain :

1. *User* dapat mengamankan *file* menggunakan algoritma kriptografi *Vigenere Cipher*.
2. *User* dapat mengetahui pentingnya keamanan sebuah data.
3. User dapat mengetahui tentang kriptografi *vigenere cipher*.

DAFTAR PUSTAKA

Maslan, A., dan Wangdra, T. (2012). *Belajar Cepat Teori, Praktek dan Simulasi Jaringan Komputer dan Internet*. Baduose Media.

D, V. C., & S, A. K. (2019). Impact of Malware in Modern Society. *International Journal of Scientific Research and Engineering Development*, 2(3), 593–600. Retrieved from www.ijsred.com

Funmilola, A., & Oluwafemi, A. (2015). Review of Computer Network Security System. *Network and Complex Systems*, 5(5), 40–47. Retrieved from www.iiste.org

Okereke, A. O., & Chukwunonso, C. E. (2018). Malware Analysis and Mitigation in Information Preservation. *Journal of Computer Engineering*, 20(4), 53–62. Retrieved from https://doi.org/10.9790/0661-2004015362

Prasad, K. M., Reddy, A. R. M., & Rao, K. V. (2014). DoS and DDoS Attacks: Defense, Detection and TracebackMechanisms -A Survey. *Global Journal of Computer Science and Technology*, 14(7), 19.

Rachmawati, D. (2014). Phising Sebagai Salah Satu Bentuk Ancaman Dalam Dunia Cyber. *Jurnal Ilmiah Saintikom, Universitas Sumatera Utara, Medan*, 1978–6603, 209–216.

Sagar, S., Shivani, & Chakravarty, V. D. (2019). Phishing attacks and defences. *International Journal of Recent Technology and Engineering*, 8(1), 894–897.

Siyoto. (2015). Dasar Metodologi Penelitian Dr. Sandu Siyoto, SKM,

M.Kes M. Ali Sodik, M.A. 1. *Dasar Metodologi Penelitian*, 1–109.

Smart, N. (2013). *Cryptography: An Introduction (3rd Edition) Nigel Smart*. Mcgraw-Hill College (December 30, 2004); eBook (3rd Edtion, 2013).