



**IMPLEMENTASI ALGORITMA *VIGENERE* DAN
COLUMNAR UNTUK MENGAMANKAN DATA TEKS
YANG DISIMPAN DI *DATABASE MYSQL***

Skripsi

**diajukan sebagai salah satu persyaratan untuk memperoleh gelar
Sarjana Pendidikan Program Studi Teknik Informatika dan Komputer**

Oleh

Mahya Azka

NIM. 5302414061

**PENDIDIKAN TEKNIK INFORMATIKA DAN KOMPUTER
JURUSAN TEKNIK ELEKTRO
FAKULTAS TEKNIK
UNIVERSITAS NEGERI SEMARANG**

2019

PERSETUJUAN PEMBIMBING

Nama : Mahya Azka.
NIM : 5302414061.
Program Studi : S-1 Pendidikan Teknik Informatika dan Komputer.
Judul Skripsi : IMPLEMENTASI ALGORITMA VIGENERE
DAN COLUMNAR UNTUK MENGAMANKAN
DATA TEKS YANG DISIMPAN DI DATABASE
MYSQL.

Skripsi ini telah disetujui oleh pembimbing untuk diajukan ke sidang panitia ujian skripsi Program Studi S-1 Pendidikan Teknik Informatika dan Komputer FT. UNNES.

Semarang, 10 Januari 2019

Pembimbing,



Arief Arfriandi, S.T., M.Eng.

NIP. 198208242014041001

PENGESAHAN

Skripsi dengan judul “Implementasi Algoritma *Vigenere* dan *Columnar* untuk Mengamankan Data Teks yang Disimpan di *Database MySQL*” ini telah dipertahankan dihadapan sidang Panitia Ujian Skripsi Fakultas Teknik, UNNES pada tanggal 14 Januari 2019.

Oleh

Nama : Mahya Azka
NIM : 5302414061
Program Studi : Pendidikan Teknik Informatika dan Komputer

Panitia;

Ketua Panitia



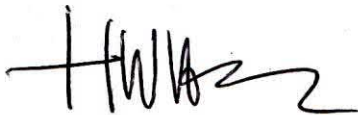
Dr-Ing. Dhidik Prastiyanto, S.T.,M.T.
NIP. 197805312005011002

Sekretaris



Ir. Ulfah Mediaty Arief, M.T.
NIP. 196605051998022001

Penguji I



Dr. Hari Wibawanto, M.T.
NIP. 196501071991021001

Penguji II



Alfa Faridh Suni, ST, MT
NIP. 198210192014041001

Penguji III/Pembimbing



Arief Arfriandi, S.T., M.Eng
NIP. 198208242014041001

Mengetahui;



Dekan Fakultas Teknik UNNES

Dr. Nur Qudus, M.T.

NIP. 196911301994031001

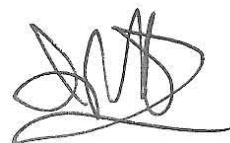
PERNYATAAN KEASLIAN

Dengan ini saya menyatakan bahwa:

1. Skripsi ini adalah asli dan belum pernah diajukan untuk mendapatkan gelar akademik (sarjana, magister, dan/atau doktor), baik di Universitas Negeri Semarang (UNNES) maupun perguruan tinggi lain.
2. Karya tulis ini adalah murni gagasan, rumusan dan penelitian saya sendiri, tanpa bantuan pihak lain, kecuali arahan Pembimbing dan masukan Penguji.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat yang telah ditulis atau dipublikasikan orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan dicantumkan dalam daftar pustaka.
4. Pernyataan ini saya buat dengan sesungguhnya dan apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka saya bersedia menerima sanksi akademik berupa pencabutan gelar yang telah diperoleh karena karya ini, serta sanksi lainnya sesuai dengan norma yang berlaku di perguruan tinggi ini.

Semarang, 14 Januari 2019

Yang membuat pernyataan



Mahya Azka

NIM. 5302414061

MOTTO DAN PERSEMBAHAN

Motto:

- Allah tidak membebani seseorang itu melainkan sesuai dengan kesanggupannya (Q.S. Al-Baqarah: 286).
- Tetap tegakan sholat walaupun sedang menjalani tugas seberat apapun.
- Tak ada orang hebat yang tak punya mimpi dahsyat, dan semua prosesnya dibentuk dari kesukaran,, tantangan dan air mata.

Persembahan:

Skripsi ini saya persembahkan untuk:

1. Bapak saya Muhlisin, S.Ag., M.M. dan Ibu saya Asih Sulasih yang selalu mendukung, mendoakan dan percaya pada anaknya bahwa anaknya mampu untuk menyelesaikan kuliah dengan baik.
2. Seluruh teman-teman PTIK UNNES angkatan 2014, terkhusus untuk Rombel 2 yang telah dan tengah berjuang berama-sama menyelesaikan studi S-1nya.
3. Rekan-rekan Taruna Siaga Bencana Kabupaten Kendal, Saka Wira Kartika Kodim 0715/Kendal dari TNI dan anggota yang telah memberi semangat, motivasi dan do'a kepada saya.
4. Almamater Universitas Negeri Semarang yang telah memberikan kesempatan, ilmu dan pengalaman.

Abstract

Evolution of information and technology make data in our lives slowly changed into digital data. Along the improvement there was an increased case of criminal theft of data so it is necessary accompanied by the development of better security systems to maintain security and data integrity. This research was aimed to implement vigenere and columnar algorithm to secure text from txt files which will be stored in MySQL database. This research will test the used algorithm in the encryption process.

This research make encryption text system that obtained text from the result of reading files with txt extension with vigenere and columnar algorithm. This program was developed with waterfall method and made with PHP, HTML, CSS, Javascript and MySQL programming language. The testing technique in this research uses the whitebox method to test the accuracy of the algorithm used.

The result of this research indicate the algorithm runs accord the planning and the program can do the encryption and decryption process properly.

Keywords : encryption, vigenere, columnar, white-box testing

Abstrak

Mahya Azka. 2018. Implementasi Algoritma *Vigenere* dan *Columnar* untuk Mengamankan Data Teks yang Disimpan di *Database MySQL*. Pembimbing : Arief Afriandi, S.T., M.Eng. Pendidikan Teknik Informatika dan Komputer.

Perkembangan teknologi informasi membuat data pada kehidupan kita secara perlahan beralih menjadi data digital. Seiring perkembangan tersebut terjadi peningkatan kasus kejahatan pencurian data sehingga perlu diiringi dengan pengembangan sistem keamanan yang lebih baik untuk menjaga keamanan dan integritas data. Penelitian ini bertujuan untuk mengimplementasikan algoritma *vigenere* dan *columnar* untuk mengamankan teks dari *file txt* yang disimpan di *database MySQL*. Penelitian ini juga akan menguji algoritma yang digunakan dalam proses enkripsi.

Penelitian ini membuat sistem enkripsi teks yang didapat dari hasil pembacaan *file* berekstensi *txt* menggunakan algoritma *vigenere* dan *columnar*. Program ini dikembangkan menggunakan metode *waterfall* dan dibuat menggunakan bahasa pemrograman *PHP*, *HTML*, *CSS*, *Javascript* dan *MySQL*. Teknik pengujian pada penelitian ini menggunakan metode *white-box* untuk menguji keakuratan algoritma yang digunakan.

Hasil dari penelitian ini menunjukkan bahwa algoritma berjalan sesuai rencana dan program dapat melakukan proses enkripsi dan dekripsi dengan baik.

Kata Kunci : enkripsi, *vigenere*, *columnar*, uji *white-box*

KATA PENGANTAR

Puji syukur penulis ucapkan atas kehadiran Allah SWT yang telah memberikan rahmat-Nya sehingga penulis dapat menyelesaikan penyusunan skripsi yang berjudul “Implementasi Algoritma *Vigenere* dan *Columnar* untuk Mengamankan Data Teks yang Disimpan di *Database MySQL*”. Skripsi ini disusun sebagai salah satu persyaratan meraih gelar Sarjana Pendidikan pada Program Studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang.

Dalam penyusunan skripsi ini tidak bisa lepas dari dukungan berbagai pihak. Oleh sebab itu pada kesempatan ini ingin diberikan rasa hormat dan ucapan terima kasih kepada,

1. Bapak Prof. Dr. Fathur Rokhman, M.Hum., Rektor Universitas Negeri Semarang yang telah memberikan kesempatan kepada saya untuk belajar di Universitas Negeri Semarang.
2. Bapak Dr. Nur Qudus, M.T., Dekan Fakultas Teknik Universitas Negeri Semarang yang telah memberikan izin untuk melaksanakan penelitian.
3. Bapak Dr.-Ing. Dhidik Prastiyanto, S.T., M.T., Ketua Jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang yang telah memberikan kesempatan untuk memaparkan gagasan dalam bentuk skripsi ini.
4. Ibu Ir. Ulfah Mediaty Arief, M.T., Ketua Prodi Pendidikan Teknik Informatika dan Komputer Fakultas Teknik Universitas Negeri Semarang yang telah membantu dalam administrasi penelitian, serta memberikan dorongan sehingga dapat selesainya skripsi ini.

5. Bapak Arief Arfriandi, S.T., M.Eng. Dosen pembimbing yang telah memberikan bimbingan, pengarahan, saran, dan motivasi kepada saya dalam penyusunan skripsi ini.
6. Segenap dosen jurusan Teknik Elektro Fakultas Teknik Universitas Negeri Semarang yang telah banyak membekali ilmu pengetahuan.
7. Staf Tata Usaha jurusan dan fakultas yang membantu administrasi selama penyusunan skripsi ini.
8. Teman-teman mahasiswa PTIK UNNES angkatan 2014 yang saling memberikan semangat, perhatian dan penguatan.
9. Semua pihak yang telah membantu dalam penyusunan skripsi ini.

Penulis hanya bisa memanjatkan doa semoga semua pihak yang telah membantu penulis dalam penyusunan skripsi ini mendapatkan pahala dari Allah SWT. Penulis berharap semoga skripsi ini bermanfaat bagi semua pihak khususnya bagi penulis sendiri dan masyarakat serta pembaca pada umumnya.

Semarang, 12 Januari 2019

Penulis

DAFTAR ISI

JUDUL	i
PERSETUJUAN PEMBIMBING.....	ii
PENGESAHAN	iii
PERNYATAAN KEASLIAN.....	iv
MOTTO DAN PERSEMBAHAN	v
ABSTRAK	vi
KATA PENGANTAR	viii
DAFTAR ISI.....	x
DAFTAR TABEL.....	xii
DAFTAR GAMBAR	xiii
DAFTAR LAMPIRAN.....	xiv
BAB I.....	1
1.1. Latar Belakang	1
1.2. Identifikasi Masalah	3
1.3. Pembatasan Masalah	4
1.4. Rumusan Masalah	4
1.5. Tujuan Penelitian.....	5
1.6. Manfaat Penelitian.....	5
1.6.1. Manfaat Teoritis	5
1.6.2. Manfaat Praktis	6
BAB II.....	7
2.1. Kajian Pustaka	7
2.2. Landasan Teori	9
2.2.1. Kriptografi.....	9
2.2.2. Algoritma <i>Vigenere</i>	12
2.2.3. Algoritma <i>Columnar</i>	14
2.2.4. <i>Unicode</i>	15

2.2.5.	ASCII	16
2.2.6.	<i>Bubble Sort</i>	19
BAB III	20
3.1.	Tempat dan Waktu Penelitian	20
3.2.	Desain Penelitian	20
3.2.1.	Tahap 1	21
3.2.2.	Tahap 2.....	21
3.3.	Teknik Pengumpulan Data	24
3.4.	Teknik Analisis Data	24
3.4.1.	<i>Basic path testing</i>	24
3.4.2.	<i>Test case</i>	27
BAB IV	28
4.1.	Hasil Enkripsi dan Dekripsi	28
4.2.	Hasil Uji Coba <i>White-box</i>	30
4.2.1.	<i>Basic path testing</i>	31
4.2.2.	<i>Cyclomatic Complexity</i>	41
4.2.3.	<i>Test case</i>	44
4.3.	Hasil Pengujian File txt pada Beberapa Sistem Operasi	64
4.4.	Hasil Pengujian pada File txt.....	67
4.5.	Pembahasan	74
BAB V	76
5.1.	Kesimpulan.....	76
5.2.	Saran.....	76
DAFTAR PUSTAKA	77
LAMPIRAN	78

DAFTAR TABEL

Tabel 2.1. Tabel ASCII	16
Tabel 3.1. Kebutuhan Perangkat Lunak	22
Tabel 3.2. Nilai Kompleksitas dan Artinya.....	26
Tabel 4.1. Hasil <i>Test Case</i> pada Proses Enkripsi	48
Tabel 4.2. Hasil <i>Test Case</i> pada Proses Dekripsi.....	57
Tabel 4.3. File txt di beberapa sistem operasi	64
Tabel 4.4. Hasil Pengujian pada File txt	67

DAFTAR GAMBAR

Gambar 2.1. <i>Symmetric Key Cryptography</i>	11
Gambar 2.2. <i>Asymmetric-Key Cryptography</i>	11
Gambar 2.3. Enkripsi dengan Algoritma <i>Columnar</i>	15
Gambar 3.1. Metode Penelitian yang Digunakan pada Penelitian Ini	20
Gambar 3.2. <i>Mock Up</i> Tampilan Sistem Enkripsi	23
Gambar 3.3. Aturan <i>Flowgraph</i>	25
Gambar 3.4. Contoh merubah <i>flowchart</i> (a) menjadi <i>Flowgraph</i> (b)	25
Gambar 4.1. Tampilan Halaman <i>Upload File</i>	28
Gambar 4.2. Tampilan Halaman <i>Download File</i>	30
Gambar 4.3. Baris Kode Enkripsi	32
Gambar 4.4. <i>Flowgraf</i> Enkripsi	36
Gambar 4.5. Baris Kode Dekripsi	37
Gambar 4.6. <i>Flowgraf</i> Dekripsi	40

DAFTAR LAMPIRAN

Lampiran 1. Formulir Usulan Topik Skripsi	79
Lampiran 2. Surat Keputusan Pembimbing Skripsi	80
Lampiran 3. <i>Source Code</i> Enkripsi	81
Lampiran 4. <i>Source Code</i> Dekripsi	85

BAB I PENDAHULUAN

1.1. Latar Belakang

Teknologi digital berkembang sangat pesat pada dasawarsa terakhir. Dengan perkembangan yang sedemikian pesat tersebut, dokumen dalam kehidupan kita juga perlahan beralih menjadi data digital. Data digital tersebut sebagian tersimpan pada *database*. Dengan semakin besarnya data yang disimpan di *database* maka rentan keamanan data merupakan permasalahan yang harus ditanggulangi, terutama terkait dengan kerahasiaan ketersediaan dan integritas data.

Menurut Indonesia (2018) dalam webnya berjudul *Kasus Pencurian Data Terbesar yang Terjadi di Tahun 2017*, kasus pencurian data semakin meningkat, dimana setiap harinya tercatat ada kasus pencurian dan kehilangan data sensitif sekitar 5 juta akun, dan di tahun 2017 terdapat 1,9 milyar kasus pencurian dan kehilangan data sensitif melalui 918 insiden. Menurut Soewito (2017), seiring meningkatnya pengguna dan aplikasi pada internet, maka meningkat pula kasus kejahatan menggunakan internet yang berupa *injection, Broken Authentication and Session Management, Cross-site Scripting, Insecure Direct Object References, Security Misconfiguration, Sensitive Data Exposure, Missing Function Level Access Control, Cross-site Request Forgery (CSRF), Using Components with Known Vulnerabilities, dan Unvalidated Redirects and Forwards*. Menurut Acunetix dalam Soewito (2017), website dan jaringan berpotensi diserang atau di eksploitasi oleh *hacker* sebesar 70%.

Menurut Pabokory, et al., (2015), menyatakan, “Kriptografi merupakan seni dan ilmu untuk memberi proteksi pengiriman data dengan mengubahnya menjadi kode tertentu dan hanya ditujukan untuk orang yang memiliki sebuah kunci untuk mengubah kode itu kembali yang berfungsi dalam menjaga kerahasiaan data atau pesan”. Dalam teknik kriptografi terdapat dua konsep yaitu enkripsi dan dekripsi data, enkripsi merupakan proses dimana informasi atau data yang hendak dikirim diubah menjadi data yang sulit untuk dikenali, sedangkan dekripsi merupakan proses untuk mengembalikan data ke bentuk data yang asli sebelum dienkripsi. Menurut Imran (2014) Enkripsi pada data ditujukan agar data tidak terbaca menggunakan komputer biasa, sehingga diperlukan komputer atau *server* yang mampu membaca data yang terenkripsi tersebut.

Untuk mengatasi permasalahan tersebut, metode kriptografi dapat digunakan untuk menanggulangi masalah keamanan dan privasi tersebut. Akan tetapi hasil proses enkripsi yang dilakukan dengan menggunakan satu algoritma enkripsi mempunyai kelemahan yaitu dapat dipecahkan menggunakan metode *brute force* atau percobaan berulang.

Terdapat beragam algoritma dalam kriptografi. Menurut Pramanik (2014) algoritma yang menggunakan metode enkripsi *substitusi* dan transposisi akan menghasilkan *ciphertext* yang aman dan kuat sehingga susah untuk dipecahkan. Salah satu algoritma yang menggunakan enkripsi *substitusi* adalah algoritma *vigenere*, dan algoritma yang menggunakan metode transposisi adalah algoritma *columnar*.

Isnaeni (2017) telah melakukan penelitian dengan menggabungkan antara algoritma *vigenere* dan *columnar* dalam simulasi pengamanan data transaksi pengambilan uang pada ATM. Dari beberapa penelitian tentang enkripsi dengan algoritma *vigenere* dan *columnar*, belum ada pengembangan lebih lanjut tentang pengamanan data teks ASCII dari *file txt* yang disimpan di database dengan algoritma *Vigenere* dan *Columnar*. *File* teks biasa atau *.txt* adalah format sederhana dan efektif. File txt memiliki keunggulan tidak memerlukan software khusus untuk membukanya dan teks dapat bersifat fleksibel contohnya mudah menyalin dan menempelkan isi file teks biasa ke dokumen atau aplikasi apa pun, dan tidak memiliki opsi pemformatan yang rumit.

Oleh karena itu pada penelitian ini akan di implementasikan algoritma *vigenere* dan algoritma *columnar* pada data teks ASCII dari *file* dengan format *txt* yang akan disimpan dalam *database*, dimana algoritma *vigenere* yang melakukan proses *subtitusi* atau penggantian karakter dikombinasikan dengan proses pengacakan karakter oleh algoritma *columnar*.

1.2. Identifikasi Masalah

Sesuai dengan latar belakang di atas, permasalahan tersebut dapat diidentifikasi sebagai berikut :

1. Perlu dikembangkan teknik pengamanan data menggunakan algoritma kriptografi *vigenere* dan *columnar* pada data teks ASCII dari *file txt*.

2. Perlu dikembangkan aplikasi untuk mengamankan data teks ASCII dari *file txt* yang akan disimpan pada *database* berdasarkan teknik pengamanan data dengan algoritma *vigenere* dan algoritma *columnar*.
3. Perlu dilakukan pengujian *white-box* untuk menguji implementasi algoritma kriptografi pada aplikasi yang telah dibuat.

1.3. Pembatasan Masalah

Dalam penelitian ini perlu adanya batasan masalah agar mudah, terarah dan terhindar dari penyimpangan masalah yang sedang diteliti. Pembatasan masalah dalam penelitian ini sebagai berikut.

1. Aplikasi dikembangkan menggunakan bahasa pemrograman HTML, PHP, CSS dan Javascript.
2. Data teks yang di enkripsi merupakan isi dari *file txt* berupa teks ASCII.
3. Pembuatan *database* untuk penyimpanan menggunakan MySQL dan pengimplementasian algoritma *vigenere* dan *columnar* menggunakan Java Script.
4. Implementasi algoritma pada proses enkripsi menggunakan algoritma *vigenere* terlebih dahulu kemudian dienkripsi lagi menggunakan algoritma *columnar*.
5. Implementasi algoritma pada proses dekripsi menggunakan algoritma *columnar* terlebih dahulu kemudian di dekripsi lagi menggunakan algoritma *vigenere*.

1.4. Rumusan Masalah

Berdasarkan identifikasi masalah diatas, maka rumusan masalah dalam

penelitian ini adalah sebagai berikut:

1. Bagaimana mengembangkan teknik pengamanan data teks dari file txt menggunakan algoritma kriptografi *vigenere* dan *columnar* ?
2. Bagaimana membuat aplikasi yang dapat mengamankan data teks dari *file txt* di *database* berdasarkan teknik pengamanan data yang telah dikembangkan?
3. Bagaimana hasil pengujian *white-box* untuk menguji implementasi algoritma kriptografi pada aplikasi yang telah dibuat?

1.5.Tujuan Penelitian

Berdasarkan permasalahan diatas dapat dirumuskan bahwa tujuan dari penelitian ini adalah untuk :

1. Mengembangkan teknik pengamanan data teks ASCII dari *file txt* menggunakan algoritma kriptografi *vigenere* dan *columnar* sehingga dapat menanggulangi berbagai ancaman dan kelemahan terkait keamanan data digital pada *database*.
2. Membuat aplikasi yang dapat mengamankan data teks ASCII dari *file txt* yang disimpan di *database* berdasarkan teknik pengamanan data yang telah dikembangkan.
3. Melakukan pengujian *white-box* untuk menguji implementasi algoritma kriptografi pada aplikasi yang telah dibuat.

1.6. Manfaat Penelitian

1.6.1.Manfaat Teoritis

Hasil dari penelitian ini dapat memberikan kontribusi ilmiah terkait pengembangan materi teknik pengamanan data.

1.6.2. Manfaat Praktis

1. Bagi Penulis

Menambah wawasan pengetahuan penulis khususnya dalam pengembangan sistem keamanan data.

2. Bagi Pengguna

Penelitian ini membantu pengguna dalam mengamankan data teks dari *file txt* yang disimpan di *database*, sehingga dapat mengurangi resiko ancaman keamanan yang dapat terjadi.

3. Bagi Pemerintah

Teknik pengamanan ini juga dapat digunakan untuk mengamankan data yang sedang dikirim, sehingga mengurangi resiko penyadapan.

BAB II

KAJIAN PUSTAKA DAN LANDASAN TEORI

2.1. Kajian Pustaka

Menurut Cohen (1995), keamanan data merupakan suatu hal yang vital jika kita membahas mengenai komunikasi yang melibatkan pertukaran data. Ilmu yang mempelajari bagaimana mengamankan data salah satunya adalah ilmu kriptografi yang dalam awal perkembangannya masih dalam bentuk *kriptosistem*. Terdapat 3 *kriptosistem* yang rumit untuk dipecahkan, ketiga *kriptosistem* ini dinamakan oleh peneliti sebagai *random-key cipher* karena bentuknya susah untuk dikenali dan dipecahkan.

Penelitian mengenai pengembangan aplikasi dengan penambahan algoritma untuk keamanan data telah banyak dilakukan, salah satunya adalah penelitian implementasi enkripsi data dengan algoritma *vigenere* yang dilakukan oleh Arjana et al (2012). Penelitian ini dilakukan dengan menerapkan algoritma *vigenere* untuk mengamankan data pelanggan sebuah toko dengan melakukan enkripsi data yang ada di *database* aplikasi. Namun dari penelitian yang dilakukan Wilson (2006) algoritma *vigenere* dapat dipecahkan menggunakan metode *kasiski* dan *kerckhoff*.

Penelitian lainnya dilakukan oleh Ananto (2015). Penelitian ini melakukan *Kriptanalisis* pada algoritma *columnar*, dimana tujuan dari penelitian ini adalah menguji keamanan data dengan menggunakan algoritma *columnar* dengan melakukan pengujian metode *bruce force attack* dan metode *kasiski* untuk mencari kunci dan panjang kunci. Hasilnya, algoritma *columnar* sulit di tebak dengan

metode brute force attack ketika di enkripsi menggunakan kunci yang panjang dan acak. Sedangkan metode kasiski tidak dapat bekerja untuk melakukan dekripsi algoritma columnar yang merupakan kelemahan pada algoritma vigenere.

Isnaeni (2017) telah melakukan penelitian dengan menggabungkan antara algoritma *vigenere* dan *columnar* untuk mengamankan data transaksi pengambilan uang pada ATM. Hasilnya, proses enkripsi yang dilakukan dengan menggunakan dua algoritma menghasilkan data enkripsi yang lebih acak karakternya dibandingkan jika hanya menggunakan satu algoritma saja. Namun, pada penelitian tersebut masih memiliki kekurangan belum dikembangkan untuk mengamankan *file* dalam bentuk dokumen.

Penelitian ini akan menerapkan algoritma *vigenere* dan algoritma *columnar* untuk mengamankan *file txt* yang nantinya di simpan pada *database*, sehingga data dalam *database* tersebut relatif lebih aman dan susah untuk diretas oleh pihak yang tidak bertanggung jawab.

Berdasarkan penelitian-penelitian sebelumnya penggabungan algoritma menghasilkan keamanan data yang relatif lebih aman dan sulit untuk dipecahkan. Sehingga pada penelitian ini akan digunakan penggabungan dua algoritma kriptografi yaitu algoritma *vigenere* dan algoritma *columnar* untuk mengamankan *file txt*.

2.2. Landasan Teori

2.2.1. Kriptografi

Menurut Delfs dan Knebl (2007) “Kriptografi merupakan suatu ilmu pengetahuan yang berhubungan dengan kerahasiaan. Konteks dari arti kata kerahasiaan ini adalah ketika seseorang ingin mengirim suatu pesan kepada seseorang yang dituju, dan pesan tersebut merupakan suatu pesan yang bersifat pribadi maka diperlukan pengamanan data agar tidak ada pihak yang tidak bertanggung jawab meretas atau memodifikasi data tersebut. Oleh karena itu salah satu tujuan dari kriptografi adalah menyediakan metode-metode untuk mencegah serangan-serangan pada data tersebut”.

Prinsip dasar dari kriptografi adalah merahasiakan data menggunakan teknik enkripsi dan dekripsi. Pesan yang akan dikirimkan oleh pengirim pesan (*sender*) biasa disebut dengan *plaintext*, kemudian *plaintext* tersebut akan dienkripsi menjadi sebuah pesan baru, untuk mengenkripsi pesan membutuhkan *key* (kunci) untuk mengubah menjadi pesan baru. Pesan hasil enkripsi ini biasa disebut dengan *ciphertext*, kemudian *ciphertext* inilah yang akan diterima oleh pihak yang dituju (*receiver*). Ketika penerima pesan ingin mengetahui isi pesan tersebut, ia harus mengubah *ciphertext* tersebut menjadi *plaintext* kembali, dimana proses ini biasa disebut dengan dekripsi. Untuk mengubahnya penerima pesan harus memiliki informasi tambahan untuk mengubah menjadi *plaintext* kembali. (Delfs & Knebl, 2007).

Menurut Arjana (2012) dalam bidang kriptografi sering dijumpai istilah-istilah kriptografi yang mengandung arti sebagai berikut.

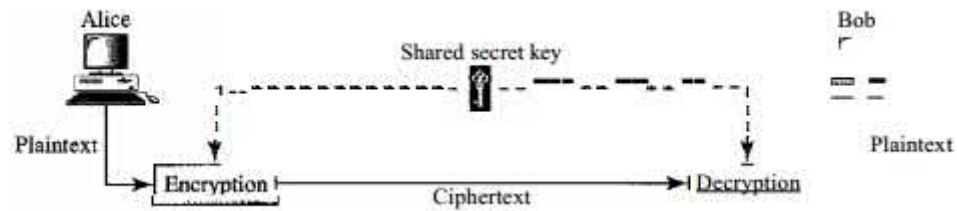
1. *Plaintext*, merupakan pesan yang hendak dikirim (berisi data asli)
2. *Ciphertext*, adalah pesan terenkripsi (tersandi) yang merupakan hasil enkripsi.
3. Enkripsi, adalah proses perubahan *plaintext* menjadi *ciphertext*.
4. Dekripsi, adalah kebalikan dari *enkripsi* yaitu mengubah *ciphertext* menjadi *plaintext*.
5. Kunci, adalah bilangan atau angka yang dirahasiakan untuk digunakan dalam proses enkripsi dan dekripsi.

Menurut Forouzan (2007) metode kriptografi merupakan suatu ilmu yang sudah berkembang cukup lama bahkan terus berkembang sampai sekarang. Jadi tidak heran jika banyak tercipta algoritma-algoritma yang telah berkembang dan digunakan sejak dulu hingga sekarang. Secara umum metode kriptografi terbagi menjadi dua kategori yaitu *Symmetric Key Cryptography* dan *Asymmetric-Key Cryptography*.

1. *Symmetric Key Cryptography*

Symmetric Key Cryptography ini telah berkembang lama, dan pernah digunakan saat akan mengirimkan pesan rahasia ketika perang. Sampai saat ini *symmetric key cryptography* masih digunakan dalam keamanan jaringan, bahkan sekarang telah berkembang menjadi lebih kompleks lagi.

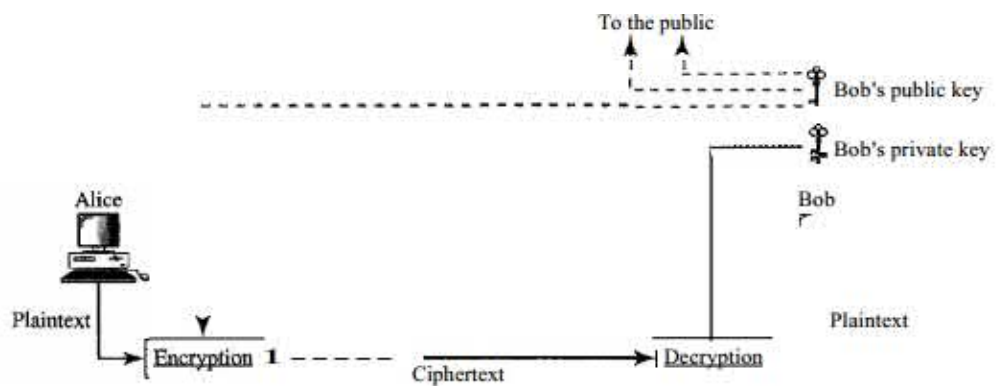
Pada algoritma *symmetric key* ini, kunci yang digunakan pada proses enkripsi digunakan kembali pada saat proses dekripsi, seperti yang bisa dilihat pada gambar 2.1.



Gambar 2.1. *Symmetric Key Cryptography* (Faraouzan, 2007)

2. *Asymmetric-Key Cryptography*

Pada algoritma *asymmetric-key* ini, terdapat dua kunci yang digunakan dalam proses enkripsi dan dekripsi, *private key* digunakan oleh penerima untuk mendekripsikan pesan, sedangkan *public key* digunakan oleh pengirim pesan untuk mengenkripsi pesan. Proses *asymmetric-key* ini bisa dilihat pada gambar 2.2.



Gambar 2.2. *Asymmetric-Key Cryptography* (Faraouzan, 2007)

Pada proses *asymmetric key cryptography* ini kedua kunci yang digunakan yaitu *private key* dan *public key*, merupakan kedua kunci yang berbeda, *public key* bisa diketahui oleh orang banyak akan tetapi *private key* hanya dimiliki oleh satu orang.

2.2.2. Algoritma Vigenere

Menurut McDonald (2009) perkembangan kriptografi pertama kali dilakukan oleh pasukan mesir pada tahun 1900 sebelum masehi dimana perkembangan dalam bentuk gambaran kehidupan raja mesir atau biasa disebut dengan *hieroglyphics*. *Hieroglyphics* yang digambarkan berisi kombinasi nomor dan simbol yang digunakan untuk menggambarkan kehidupan saat itu. Metode yang digunakan dalam penggambaran ini menjadi contoh enkripsi dengan metode *subtitusi*, dimana metode ini berjalan dengan *mensubtitusikan* antara satu simbol atau karakter dengan simbol atau karakter yang lainnya. Sekitar 500 tahun sebelum masehi, bangsa Sparta menciptakan alat yang disebut dengan *Scytale*. Alat ini merupakan contoh dari alat yang menggunakan metode *transposition cipher*, dimana dalam proses pengenkripsannya mengubah urutan karakter berdasarkan kunci yang ditetapkan. Pada tahun 1500 Blaise De *Vigenere* mengembangkan suatu konsep algoritma yang berdasarkan pada penemuan sebelumnya milik Alberti, konsep ini biasa disebut dengan algoritma *vigenere*. Konsep algoritma *vigenere* ini hampir mirip dengan *caesar cipher* namun perbedaanya terletak pada penambahan kunci pada saat proses enkripsi. Efrandi et al (2014) mengatakan bahwa kunci yang digunakan algoritma *vigenere* berbentuk deretan huruf yang memungkinkan setiap huruf *plaintext* untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci

yang digunakan lebih pendek dari panjang *plaintext* maka kunci akan diulang sampai panjang kunci sama dengan panjang *plaintext*.

Arjana et al (2012) mendeskripsikan rumus enkripsi dan dekripsi algoritma *vigenere* sebagai berikut.

Enkripsi:

$$C_i = (P_i + K_i) \bmod 26$$

Dekripsi:

$$P_i = (C_i - K_i) \bmod 26; \text{ untuk } C_i \geq K_i$$

$$P_i = (C_i + 26 - K_i) \bmod 26; \text{ untuk } C_i < K_i$$

Keterangan:

C = *Chiphertext*

P = *Plaintext*

K = Kunci

Mod 26 = karakter yang akan dienkripsi ada pada cakupan 26 karakter

Menurut penelitian yang dilakukan Wilson (2006) algoritma *vigenere* menjadi algoritma yang sukar untuk dipecahkan, namun pada akhirnya terdapat metode yang dapat memecahkannya yaitu metode *kasiski* dan *kerckhoff*. Semenjak ditemukannya metode tersebut dan dengan semakin berkembangnya zaman algoritma *vigenere* semakin mudah dipecahkan. Akan tetapi banyak peneliti yang mengembangkan kembali algoritma *vigenere* dengan menggabungkannya dengan algoritma lainnya seperti algoritma *transposition*, algoritma *OTP (One Time Pad)* atau algoritma lainnya yang membuat semakin sulit dipecahkan karena

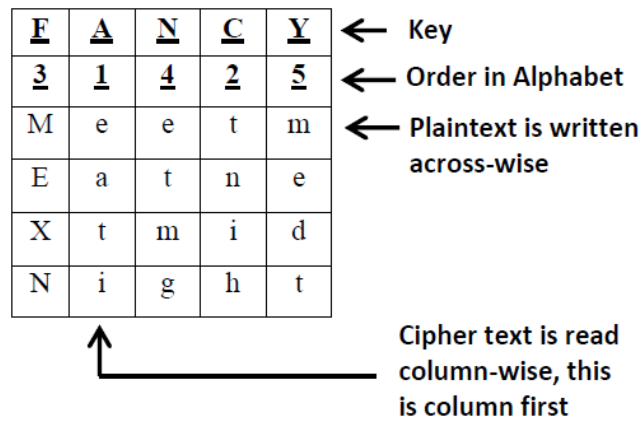
menambahkan metode pengacakan karakter sesuai dengan fungsinya masing-masing.

2.2.3. Algoritma *Columnar*

Menurut penelitian yang dilakukan oleh Stallings (2011), algoritma *columnar* merupakan salah satu teknik dari algoritma *transposition*, prinsip dari algoritma ini adalah *mensubstitusikan* karakter dengan berdasarkan urutan karakter yang ditentukan ataupun berdasarkan hasil permutasi yang telah ditentukan. Bentuk asli dari algoritma *transposition* sangat mudah untuk dipecahkan karena karakter yang terenkripsi memiliki kesamaan huruf dengan bentuk aslinya, akan tetapi algoritma *columnar transposition* menjadi salah satu teknik algoritma *transposition* yang sukar untuk dipecahkan karena untuk memecahkan *ciphertext* harus memecahkan bagaimana suatu *matrix* yang dipakai dan mengetahui posisi kolom yang ditentukan. Menurut Fidelis (2015), algoritma *columnar* menghasilkan *ciphertext* yang relatif susah untuk dipecahkan dan tidak dapat dipecahkan menggunakan metode kasiski yang merupakan metode yang dapat memecahkan algoritma *vigenere*. Teknik algoritma *transposition* ini akan lebih aman jika dilakukan lebih dari satu tahapan atau dikombinasikan dengan algoritma yang lainnya, maka akan menghasilkan permutasi yang lebih kompleks lagi dan sukar untuk dipecahkan.

Menurut Pramanik (2014) dalam algoritma *columnar* pesan ditulis dalam baris yang panjangnya ditentukan sesuai jumlah huruf pada kunci, kemudian karakter pada kolom disusun lagi (permutasi) dengan urutan alfabet pada kata kunci. Contohnya jika kuncinya kata *ZEBRAS* maka panjang kolom adalah 6, dan permutasi ditentukan oleh urutan abjad huruf dalam kata kunci yaitu "6 3 2 4 1 5".

Contoh lainnya adalah enkripsi dengan algoritma *columnar* kata “*Meet me at next midnight*” dengan kunci *FANCY* adalah sebagai berikut :



Gambar 2.3. Enkripsi dengan Algoritma *Columnar*

Hasil enkripsi dari teks diatas adalah : eatitnihMEXNetmgmedt

2.2.4. Unicode

Menurut situs resmi dari *Unicode* dijelaskan bahwa *Unicode* merupakan karakter-karakter yang sekarang digunakan untuk menyusun sebuah sistem komputer. Sebelum ada *Unicode*, komputer menggunakan pengkodean karakter yang berbeda-beda karna pada dasarnya komputer hanya berurusan dengan angka, dimana susunan dari kalimat dan karakter tertentu ditetapkan pada masing-masing angka. Pengkodean tersebut terbatas dan tidak dapat memuat banyak karakter yang terdapat pada semua bahasa di seluruh dunia, termasuk simbol dan tanda baca yang tidak umum digunakan.

Dengan adanya Standar *Unicode*, setiap karakter memiliki kode unik masing-masing yang dapat digunakan di berbagai platform. Dukungan *Unicode* juga dapat digunakan dalam representasi simbol dan bahasa di semua sistem operasi, platform, *browser*, dan lain-lain. Munculnya Standar *Unicode* dan ketersediaan alat

pendukungnya adalah salah satu tren teknologi perangkat lunak global terbaru yang paling signifikan.

2.2.5. ASCII

ASCII adalah singkatan dari *American standard Code for Information Interchange*. Karna komputer hanya dapat mengerti angka, maka kode ASCII sebagai representasi numerik karakter seperti “a” atau “@” atau perintah yang lain. Berikut adalah tabel ASCII dari nomor 32 sampai 126 dan 32 karakter *non-printing* dari kode 0 sampai 31.

Tabel 2.1. Tabel ASCII

Nilai ANSI ASCII (Desimal)	Nilai <i>Unicode</i> (Heksa Desimal)	Karakter	Keterangan
0	0000	NUL	Null (tidak terlihat)
1	0001	SOH	<i>Start of heading</i> (tidak terlihat)
2	0002	STX	<i>Start of text</i> (tidak terlihat)
3	0003	ETX	<i>End of text</i> (tidak terlihat)
4	0004	EOT	<i>End of transmission</i> (tidak terlihat)
5	0005	ENQ	<i>Enquiry</i> (tidak terlihat)
6	0006	ACK	<i>Acknowledge</i> (tidak terlihat)
7	0007	BEL	<i>Bell</i> (tidak terlihat)
8	0008	BS	<i>Backspace</i>
9	0009	HT	<i>Horizontal tabulation</i>
10	000A	LF	Pergantian baris (Line feed)
11	000B	VT	Tabulasi vertikal
12	000C	FF	Pergantian baris (Form feed)
13	000D	CR	Pergantian baris (carriage return)
14	000E	SO	<i>Shift out</i> (tidak terlihat)
15	000F	SI	<i>Shift in</i> (tidak terlihat)
16	0010	DLE	<i>Data link escape</i> (tidak terlihat)
17	0011	DC1	<i>Device control 1</i> (tidak terlihat)
18	0012	DC2	<i>Device control 2</i> (tidak terlihat)
19	0013	DC3	<i>Device control 3</i> (tidak terlihat)

Nilai ANSI ASCII (Desimal)	Nilai Unicode (Heksa Desimal)	Karakter	Keterangan
20	0014	DC4	<i>Device control 4</i> (tidak terlihat)
21	0015	NAK	<i>Negative acknowledge</i> (tidak terlihat)
22	0016	SYN	<i>Synchronous idle</i> (tidak terlihat)
23	0017	ETB	<i>End of transmission block</i> (tidak terlihat)
24	0018	CAN	<i>Cancel</i> (tidak terlihat)
25	0019	EM	<i>End of medium</i> (tidak terlihat)
26	001A	SUB	<i>Substitute</i> (tidak terlihat)
27	001B	ESC	<i>Escape</i> (tidak terlihat)
28	001C	FS	<i>File separator</i>
29	001D	GS	<i>Group separator</i>
30	001E	RS	<i>Record separator</i>
31	001F	US	<i>Unit separator</i>
32	0020	spasi	Spasi
33	0021	!	Tanda seru (exclamation)
34	0022	“	Tanda kuti dua
35	0023	#	Tanda pagar (kres)
36	0024	\$	Tanda mata uang dolar
37	0025	%	Tanda persen
38	0026	&	Karakter <i>ampersand</i> (&)
39	0027	‘	Karakter Apostrof
40	0028	(Tanda kurung buka
41	0029)	Tanda kurung tutup
42	002A	*	Karakter <i>asterisk</i> (bintang)
43	002B	+	Tambah
44	002C	,	Koma
45	002D	-	Strip
46	002E	.	Tanda titik
47	002F	/	Garis miring
48	0030	0	Angka nol
49	0031	1	Angka satu
50	0032	2	Angka dua
51	0033	3	Angka tiga
52	0034	4	Angka empat
53	0035	5	Angka lima
54	0036	6	Angka enam
55	0037	7	Angka tujuh
56	0038	8	Angka delapan
57	0039	9	Angka sembilan
58	003A	:	Tanda titik dua

Nilai ANSI ASCII (Desimal)	Nilai <i>Unicode</i> (Heksa Desimal)	Karakter	Keterangan
59	003B	;	Tanda titik koma
60	003C	<	Tanda lebih kecil
61	003D	=	Tanda sama dengan
62	003E	>	Tanda lebih besar
63	003F	?	Tanda tanya
64	0040	@	At (@)
65	0041	A	Huruf latin A kapital
66	0042	B	Huruf latin B kapital
67	0043	C	Huruf latin C kapital
68	0044	D	Huruf latin D kapital
69	0045	E	Huruf latin E kapital
70	0046	F	Huruf latin F kapital
71	0047	G	Huruf latin G kapital
72	0048	H	Huruf latin H kapital
73	0049	I	Huruf latin I kapital
74	004A	J	Huruf latin J kapital
75	004B	K	Huruf latin K kapital
76	004C	L	Huruf latin L kapital
77	004D	M	Huruf latin M kapital
78	004E	N	Huruf latin N kapital
79	004F	O	Huruf latin O kapital
80	0050	P	Huruf latin P kapital
81	0051	Q	Huruf latin Q kapital
82	0052	R	Huruf latin R kapital
83	0053	S	Huruf latin S kapital
84	0054	T	Huruf latin T kapital
85	0055	U	Huruf latin U kapital
86	0056	V	Huruf latin V kapital
87	0057	W	Huruf latin W kapital
88	0058	X	Huruf latin X kapital
89	0059	Y	Huruf latin Y kapital
90	005A	Z	Huruf latin Z kapital
91	005B	[Kurung siku kiri
92	005C	/	Garis miring terbalik
93	005D]	Kurung siku kanan
94	005E	^	Tanda pangkat
95	005F	_	Garis bawah
96	0060	`	Tanda petik satu
97	0061	a	Huruf latin a kecil
98	0062	b	Huruf latin b kecil
99	0063	c	Huruf latin c kecil

Nilai ANSI ASCII (Desimal)	Nilai <i>Unicode</i> (Heksa Desimal)	Karakter	Keterangan
100	0064	d	Huruf latin d kecil
101	0065	e	Huruf latin e kecil
102	0066	f	Huruf latin f kecil
103	0067	g	Huruf latin g kecil
104	0068	h	Huruf latin h kecil
105	0069	i	Huruf latin i kecil
106	006A	j	Huruf latin j kecil
107	006B	k	Huruf latin k kecil
108	006C	l	Huruf latin l kecil
109	006D	m	Huruf latin m kecil
110	006E	n	Huruf latin n kecil
111	006F	o	Huruf latin o kecil
112	0070	p	Huruf latin p kecil
113	0071	q	Huruf latin q kecil
114	0072	r	Huruf latin r kecil
115	0073	s	Huruf latin s kecil
116	0074	t	Huruf latin t kecil
117	0075	u	Huruf latin u kecil
118	0076	v	Huruf latin v kecil
119	0077	w	Huruf latin w kecil
120	0078	x	Huruf latin x kecil
121	0079	y	Huruf latin y kecil
122	007A	z	Huruf latin z kecil
123	007B	{	Kurung kurawal buka
124	007C		Garis vertikal
125	007D	}	Kurung kurawal tutup
126	007E	~	Karakter gelombang

2.2.6. *Bubble Sort*

Appiah et al (2015) mengatakan bahwa *bubble sort* adalah algoritma pengurutan sederhana yang berulang kali mengurutkan daftar yang diurutkan, membandingkannya dengan sepasang konten yang berdekatan dan menukarnya jika tidak sesuai dengan pengurutan. Pengulangan terus dilakukan hingga tidak ada konten yang ditukar yang menandakan bahwa daftar telah diurutkan.

BAB V

KESIMPULAN DAN SARAN

5.1. Kesimpulan

Berdasarkan penelitian yang dilakukan, telah dikembangkan teknik pengamanan data dengan algoritma *vigenere* dan *columnar* untuk mengamankan *file txt*. Aplikasi simulasi penyimpanan *file txt* telah dibangun dalam platform web dengan bahasa pemrograman HTML, CSS, PHP, dan *Javascript*. Dalam proses penyimpanan ke database digunakan MySQL.

Berdasarkan hasil pengujian *white-box*, algoritma ini berjalan dengan baik dalam mengamankan *file txt*. Algoritma dan proses yang digunakan memiliki baris kode yang kompleks, tingkat pengujian sedang dan penggunaan biaya dan upaya yang sedang juga dalam proses pengujiannya. Hasil dari enkripsi menghasilkan *ciphertext* yang baik dan dapat terbentuk lagi ke dalam bentuk *file txt*.

5.2. Saran

Penelitian ini memiliki keterbatasan hanya dapat mengamankan data *file txt*, karena aplikasi ini dibuat menggunakan pemrograman javascript dan *file* dokumen seperti PDF dan DOCX memiliki struktur file yang berbeda-beda ketika akan dibaca isinya sehingga diperlukan penelitian lebih lanjut untuk melakukan enkripsi pada tipe dokumen tersebut.

Saran dari penulis, supaya dapat dikembangkan penelitian yang dapat melakukan enkripsi pada *file* dokumen dengan format dokumen yang lain.

Daftar Pustaka

- Ananto, F.E. 2015. Kriptanalisis Algoritma Transposisi Columnar. *Skripsi*. Program Studi Teknik Informatika Universitas Sanata Dharma. Yogyakarta.
- Appiah, Obed dan Ezekiel M. M. 2015. Magnetic Bubble Sort Algorithm. *International Journal of Computer Applications* 122 (21):24-28.
- Arjana,P.H, T.P.Rahayu, dan Y.Hariyanto. 2012 *.Implementasi Enkripsi Data dengan Algoritma Algoritma vigenere*. Artikel disajikan pada Seminar Nasional Teknologi Informasi dan Komunikasi 2012. Yogyakarta. 10 Maret 2012.
- ASCII Table. 2010. *ASCII Table and Description*. <http://www.asciitable.com/>. 21 Mei 2018 (10.38).
- Cohen, F. 1995. *Short History of Cryptography*. 1st ed United States : Fred Cohen & Associates.
- Constantianus, Frederick & Bernard Renaldy Suteja. (2005). Analisa dan Desain Sistem Bimbingan Tugas Akhir Berbasis Web dengan Studi Kasus Fakultas Teknologi Informas. *Jurnal Informatika UKM* Vol. I (2) : 93-105.
- Delfs, H., Knebl, H. 2007. *Introduction to Cryptography, Principles and Applications. Second Edition* . Springer.
- Efrandi, Asnawati dan Yupiyanti. 2014. Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher. *Jurnal Media Infotama* Vol. 10 (2):120-128.
- Elergic. 2018 . *About JavaScript* . https://developer.mozilla.org/en-US/docs/Web/JavaScript/About_JavaScript . 1 Agustus 2018 (21.10).
- Forouzan,B.A. dan S.C. Fegan. 2007. *Data Communication and Networking*. 4th ed McGraw-Hill Companies, Inc. New York.
- Imran, Syaiful.2014. *Sistem Keamanan pada Penyimpanan File Online Untuk Menjaga Keamanan dan Kerahasiaan File dan Data Pengguna*. <http://ipankint.com/internet/sistem-keamanan-penyimpanan-file-online/>. 14 Juni 2018 (11.15).
- Indonesia, C.L.2017.*Kasus Pencurian Data Terbesar yang Terjadi di Tahun 2017*. <http://jakartaurbanhosting.com/kasus-pencurian-data-terbesar-2017/amp/>. 10 Mei 2018 (21.00).
- Isnaeni, Akhmad .2017. Implementasi Kriptografi Menggunakan Algoritma Vigenere Dan Columnar Pada Data Transaksi Pengambilan Uang Melalui Atm.*Skripsi*.Semarang:Program Studi Pendidikan Teknik Informatika dan Komputer Universitas Negeri Semarang. Semarang.

- McDonald, N.G. 2009. *Past, Present, And Future Methods of Cryptography and Data Encryption*. Research Review. Utah : Department of Electrical and Computer Engineering University of Utah.
- Pabokory, F.N., Indah F. A., Awang H.K. 2015. Implementasi Kriptografi Pengamanan Data Pada Pesan Teks, Isi File Dokumen, dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard. *Jurnal Informatika Mulawarman* 10 (1): 20-31.
- Patelia, Ramesh M dan Shilpan Vyas. 2014. A Review and Analysis on Cyclomatic Complexity . *Oriental Journal Of Computer Science & Technology* 122 (21): 382-384.
- Pramanik, M.B. 2014. Implementation of Cryptography Technique using Columnar Transposition. *International Journal of Computer Application* :19-23.
- Pressman, Roger S. 2010. *Software engineering : a practitioner's approach / Roger S. Pressman. -7th ed.* New York: McGraw-Hill Companies.
- Saputra, Agus, Ridho Taufiq Subagio dan Saluky. 2012. Membangun Aplikasi E-Library Untuk Panduan Skripsi, Jakarta : PT.ELEX Media Komputindo.
- Sitohang, H.T. 2018. Sistem Informasi Pengagendaan Surat Berbasis Web pada Pengadilan Tinggi Medan. *Journal Of Informatic Pelita Nusantara* Vol.3(1):6-9.
- Soewito, Benfano. 2017. *STATISTIK KEJAHATAN DI INTERNET*. <https://mti.binus.ac.id/2017/06/08/statistik-kejahatan-di-internet/>. 10 Mei 2018 (21.35).
- Stallings, W. 2011. *Cryptography and Network Security: Principles and Practice*. 5th ed. New York : Pearson Education Inc.
- Unicode.2017. *What is Unicode?* . <http://unicode.org/standard/WhatIsUnicode.html>. 1 Agustus 2018 (20.30).
- Wibowo, A.T. 2013. Pembuatan Aplikasi E-Commerce Pusat Oleh-Oleh Khas Pacitan pada Toko Sari Rasa Pacitan. *Indonesian Journal on Networking and Security* Vol. 2 (4):62-67.
- Wilson, P.I dan M. Garcia. 2006. A Modified Version of the Vigenere Algorithm. *International Journal of Computer Science and Network Security* 6(3B) : 140-143.