KARMAPATI

ISSN 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 2, Nomor 6, Agustus 2013

Implementasi *Vigenére Cipher* pada *AJAX* (*Asynchronous Javascript and XML*)

Ida Bagus Redy Santiawan[1], I Gede Mahendra Darmawiguna[2], Made Windu Antara Kesiman[3]
Pendidikan Teknik Informatika
Universitas Pendidikan Ganesha
Singaraja, Bali
Email : goesredy@gmail.com[1], igd.mahendra.d@gmail.com[2], dekndu@yahoo.com[3]

Abstrak—Penelitian ini bertujuan untuk : (1) membuat rancangan Vigenére Cipher pada AJAX (*Asynchronous Javascript and XML*), (2) mengimplementasikan rancangan Vigenére Cipher pada AJAX (*Asynchronous Javascript and XML*). Dalam perancangan dan pengimplementasiannya, digunakan 2 metode utama dalam penerapan argoritma yaitu enkripsi dan dekripsi. Pada metode enkripsi inputan berupa *text* dan keluarannya berupa *ciphertext* serta pada metode dekripsi inputannya berupa *ciphertext* dan keluarannya berupa *text*. Pengujian dilakukan dengan cara *network sniffing* yakni meng-*capture* data yang lalu lalang pada *network*.

Perancangan dan pengimplementasian rancangan aplikasi, digunakan metode *waterfall* atau yang sering disebut dengan *classic life cycle model*. Model *waterfall* ini merupakan model klasik yang bersifat sistematis atau berurutan dalam membangaun perangkat lunak. Model tersebut meliputi beberapa tahapan yakni: (1) *requirements definition*, (2) *system and software design*, (3) *implementation and unit testing*, dan (4) *integration and system testing*.

Implementasi dan pengujian pada penelitian ini adalah suatu Aplikasi Vigenére Cipher pada AJAX yang menggunakan bahasa pemrograman PHP (*server*) dan Javascript (*client*). Dari data hasil uji performansi sistem didapat bahwa sistem mampu menyembunyikan data yang terkirim menuju *network*.

Kata Kunci—Kriptografi, Vigenére Cipher, AJAX, *Network Sniffing, Web Security*

Abstract—This studi aimed to : (1) designing Vigenére Cipher in AJAX (Asynchronous Javascript and XML), (2) implementing Vigenére Cipher in AJAX (Asynchronous Javascript and XML). In designing and implementing the system, it was used 2 main methods in implementation of the encryption and decryption. On the encryption method, plaintext as input and ciphertext as output, and then on the decryption method ciphertext as input and plaintext as output. The test has been done with network sniffing ie capture the data passing on the network.

In designing and implementing the application design, it was used a waterfall method which is usually called as a classic life cycle model. This is a classic model which creates the software systematically and sequentially that includes some stages namely: (1) requirements definition, (2) system and software design, (3) implementation and unit testing, and (4) integration and system testing.

The implementation and testing in this study was a Vigenére Cipher Aplication that were using a PHP for server side and a Javascript for client side. Based on the data of the system performance test, obtained that the system can hide the data sent to the network.

Keywords—Cryptography, Vigenére Cipher, AJAX, Network Sniffing, Web Security

I. PENDAHULUAN

Teknologi saat ini memungkinkan berbagai informasi tersebar ke seluruh pelosok dan juga menjadi semakin terbuka bagi dunia luar. Semakin terbukanya segala sesuatu tersebut justru membuat celah bagi orang-orang yang tidak bertanggung jawab untuk memanfaatkannya. Segala bentuk informasi yang mereka dapatkan digunakan untuk hal-hal yang dapat merugikan banyak pihak yang terkait dengan informasi tersebut.

AJAX (*Asynchronous Javascript and XML*) adalah suatu teknik pemograman berbasis web untuk menciptakan aplikasi web secara interaktif. AJAX digunakan agar sebuah aplikasi web dapat mengambil data atau informasi dari server secara tidak sinkronis tanpa merubah tampilan dan perilaku pada halaman yang ada. Penggunaan AJAX dilakukan dengan *request* dari *client* terhadap *server* secara sinkron, yang kemudian *server* menanggapi *request* tersebut dengan mengirimkan *response*. Keuntungan menggunakan AJAX dapat mengurangi penggunaan *bandwidth*, *load time*, web menjadi lebih interaktif dan cepat, dan mengurangi koneksi ke *server*. Meskipun memiliki keuntungan yang lumayan, akan tetapi tidak diikuti dengan peningkatan terhadap keamanan, terutama saat digunakan untuk menerima informasi rahasia seperti nomor kartu kredit, kata kunci, dan lain sebagainya. Oleh karena itu diperlukan pengenkripsian pada *request* dari *client* maupun *response* dari *server*, sehingga informasi tersebut

ISSN 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 2, Nomor 6, Agustus 2013

tidak dapat dibaca oleh orang yang tidak berhak. Pada pengenkripsian pada AJAX ini menggunakan teknik kriptografi yaitu algoritma Vigenère *Cipher*, karena algoritma ini mudah dimengerti dan dijalankan serta sulit dipecahkan.

Berdasarkan hal-hal tersebut penulis tertarik untuk membuat suatu penerapan enkripsi terhadap AJAX untuk mengurangi tingkat pencurian informasi oleh pihak-pihak yang tidak berhak yang diharapkan dapat melindungi informasi-informasi penting yang dilakukan dalam komunikasi dengan menggunakan AJAX.

II. KAJIAN TEORI

A. *Kriptografi*

Berkembangnya cara pengiriman pesan dan atau penyaluran informasi, berkembang pula cara penyembunyian pesan atau informasi agar pesan atau informasi tersebut tetap tidak bisa diketahui isinya meskipun jika pesan tersebut ditemukan. Lahirlah kemudian sebuah ilmu baru yang dikenal dengan nama Kriptografi yang sangat erat kaitannya dengan keamanan informasi pada suatu media digital.

B. *Pengertian Kriptografi*

Kriptografi berasal dari bahasa Yunani, *crypto* dan *graphia*. *Crypto* berarti *secret* (rahasia) dan *grahia* berarti *writing* (tulisan). Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain.

Para pelaku atau praktisi kriptografi disebut *cryptographers*. Sebuah algoritma kriptografi (*cryptographic algorithm*) disebut *cipher*. Proses yang dilakukan untuk mengamankan sebuah pesan (yang disebut *plaintext*) menjadi pesan yang tersembunyi (disebut *ciphertext*) adalah enkripsi (*encryption*). *Ciphertext* adalah pesan yang sudah tidak dapat dibaca dengan mudah. Menurut ISO 7498-2, terminologi yang lebih tepat digunakan adalah "*encipher*". Proses sebaliknya, untuk mengubah *ciphertext* menjadi *plaintext*, disebut dekripsi (*decryption*).

C. *Sejarah Kriptografi*

Kriptografi mempunyai sejarah yang sangat panjang dan menarik. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalkan oleh orang-orang Mesir lewat *hieroglyph*.

Pada Zaman Romawi Kuno, pada suatu saat Julius Caesar ingin mengirimkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut diacak sehingga orang yang tidak berhak tidak dapat membacanya.

Di India, kriptografi digunakan oleh pecinta (*lovers*) untuk berkomunikasi tanpa diketahui orang. Bukti ini ditemukan di dalam buku Kamasutra yang direkomendasikan agar wanita mempelajari seni memahami tulisan dengan kode.

D. *Tujuan Kriptografi*

Ada empat tujuan mendasar dari kriptografi yang juga merupakan aspek keamanan informasi, antara lain sebagai berikut.

1. Kerahasiaan (*confidentiality*)
2. Integritas data (*data integrity*)
3. Otentikasi (*authentication*)
4. Nirpenyangkalan (non-*repudiation*)

E. *Algoritma Kriptografi*

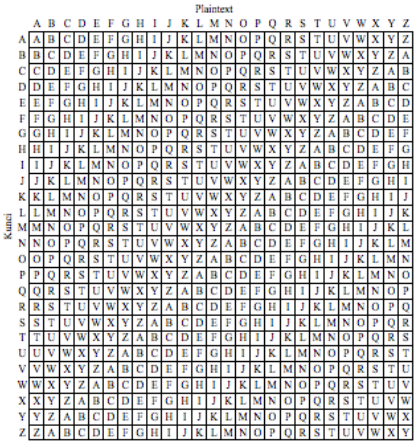
Terminologi algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis. Algoritma Kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar, yaitu :

1. Enkripsi
2. Dekripsi
3. Kunci

F. *Vigenére Cipher*

Vigenère *Cipher* atau kode Vigenère termasuk kode abjad-majemuk (*polyalphabetic substitution cipher*). Dipublikasikan oleh diplomat (sekaligus seorang kriptologis) Perancis, Blaise de Vigenère pada abad 16, tahun 1586. Sebenarnya Giovan Batista Belaso telah menggambarkannya untuk pertama kali pada tahun 1553 seperti ditulis di dalam buku *La Cifra del Sig*. algoritma ini baru dikenal luas 200 tahun kemudian dan dinamakan kode Vigenère atau Vigenère *Cipher*.

Ide dasarnya adalah dengan menggunakan kode Kaisar, tetapi jumlah pergeseran hurufnya yang berbeda-beda untuk setiap periode beberapa huruf tertentu. Untuk mengenkripsi pesan dengan kode Vigenère digunakan *tabula recta* (disebut juga bujursangkar Vigenère) seperti ditunjukan pada Gambar 1.



Gambar 1 : *Tabula Recta* atau bujursangkar Vigenère

Tabula recta digunakan untuk memperoleh teks kode dengan menggunakan kunci yang sudah ditentukan. Jika panjang kunci lebih pendek daripada panjang teks asli

ISSN 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 2, Nomor 6, Agustus 2013

maka penggunaan kunci diulang. Secara matematis enkripsi dengan kode Vigenère bisa dinyatakan sebagai berikut

E(pi)=V(pi,k(i mod m))

III. METODOLOGI

A. *Analisis Masalah Dan Usulan Solusi*

Berdasarkan analisis dari permasalahan yang dijumpai mengenai keamanan data pada jaringan, terdapat beberapa masalah sebagai berikut. 1) Belum banyak pengembang memperhatikan keamanan dari. 2) Banyak pengguna awam yang tidak mengerti bagaimana suatu sistem keamanan itu bekerja. 3) Semakin berkembangnya cara-cara pencurian informasi. 4) Pemilihan pengiriman data menggunakan skema AJAX membuat data yang terkirim melalui *client-server* menjadi teks biasa.

Berdasarkan analisis masalah di atas maka solusi yang dapat diusulkan adalah sebuah perangkat lunak hasil implementasi algoritma Vigenére *Cipher* pada AJAX. Berikut solusi yang dapat diusulkan dari perangkat lunak yang akan dikembangkan. 1) Perangkat lunak ini dapat dijadikan sebagai salah satu acuan untuk mengamankan sistem oleh para pengembang. 2) Kecerobohan pengguna dapat diminimalisasi dengan perangkat lunak ini. 3) Perangkat lunak yang dikembangkan selain mencakup proses request data juga meliputi response data. 4) Pengiriman data dengan skema AJAX akan langsung mengacak data yang dikirim atau diterima.

B. *Analisis Perangkat Lunak*

Adapun beberapa hal yang akan dijelaskan mengenai analisis perangkat lunak ini antara lain: 1) analisis kebutuhan perangkat lunak; 2) tujuan pengembangan perangkat lunak; 3) masukan dan keluaran perangkat lunak; 4) serta model fungsional perangkat lunak. Perangkat lunak yang akan dibangun bernama Vigenére *Cipher Securer*.

1) Kebutuhan Perangkat Lunak

Berdasarkan analisis terhadap pengembangan Vigenére *Cipher Securer*, terdapat beberapa proses yang dapat diimplementasikan sebagai berikut. a) Melakukan operasi pengambilan data yang akan diamankan. b) Melakukan operasi pembacaan data dan penentuan operasi yang akan dilakukan (enkripsi atau dekripsi). c) Melakukan perhitungan substitusi pada *tabula recta* untuk menerapkan algoritma Vigenére *Cipher* dan menghasilkan data terenkripsi atau dekripsi. d) Melakukan pengiriman atau penerimaan data pada hubungan client-server.

2) Tujuan Pengembangan Perangkat Lunak

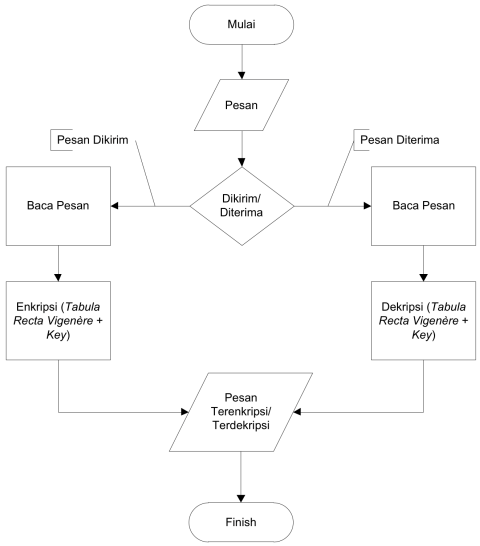
Adapun tujuan dari pengembangan perangkat lunak ini adalah meningkatkan kemampuan pengamanan data pada setiap aplikasi web yang memakai perangkat lunak ini.

3) Masukan dan Keluaran Perangkat Lunak

1. Masukan : a. *Plaintext* atau teks biasa jika proses yang akan dilakukan adalah enkripsi. b. *Ciphertext* atau teks teracak jika proses yang akan dilakukan adalah dekripsi. c. *Key* atau kunci yang digunakan untuk proses enkripsi atau dekripsi.
2. Keluaran : a. *Plaintext* atau teks biasa jika proses yang akan dilakukan adalah dekripsi. b. *Ciphertext* atau teks teracak jika proses yang akan dilakukan adalah enkripsi. c. *Key* atau kunci yang digunakan untuk proses enkripsi atau dekripsi.

4) Model Fungsional Perangkat Lunak

Model fungsional dari perangkat lunak Vigenére *Cipher Securer* digambarkan dengan menggunakan Bagan Alir (*Flowcart*). Berikut bagan alir dari implementasi Vigenére *Cipher* pada AJAX dapat dilihat pada Gambar 2.



Gambar 2 : Bagan Alir Implementasi Vigenére *Cipher* pada AJAX (*Asynchronous Javascript and XML*)

C. *Perancangan Perangkat Lunak*

Pada perancangan perangkat lunak implementasi Vigenére *Cipher* pada AJAX ini terdapat beberapa tahapan yang dilalui, yaitu batasan perancangan perangkat lunak, perancangan arsitektur perangkat lunak, dan perancangan struktur data perangkat lunak.

1) Batasan Perancangan Perangkat Lunak

Adapun batasan yang terdapat dalam perancangan perangkat lunak implementasi

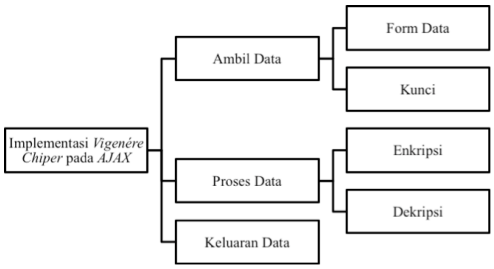
ISSN 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 2, Nomor 6, Agustus 2013

Vigenére *Cipher* pada AJAX yang akan dibuat ini sebagai berikut.

- Data yang dapat diolah oleh perangkat lunak adalah data berupa teks.
- Perangkat lunak belum mampu menangani data berupa file.

2) Perancangan Arsitektur Perangkat Lunak

Perancangan arsitektur perangkat lunak menggambarkan bagian-bagian modul, struktur ketergantungan antar modul, dan hubungan antar modul dari perangkat lunak yang dibangun. Pada bagian ini terdapat *structure chart* sebagai kendali fungsional yang digambarkan seperti Gambar 3 untuk perangkat lunak implementasi Vigenére *Cipher* pada AJAX.



Gambar 3 *Structure Chart* Perangkat Lunak Implementasi Vigenére *Cipher* pada AJAX (*Asynchronous Javascript and XML*)

3) Perancangan Struktur Data Perangkat Lunak

Struktur data yang digunakan dalam perangkat lunak bermacam-macam, akan tetapi struktur data utama yang digunakan dalam perangkat lunak implementasi Vigenére *Cipher* pada AJAX ini adalah struktur data *string* dan atau *array of char*.

IV. PEMBAHASAN

A. *Implementasi Perangkat Lunak*

Implementasi perangkat lunak Vigenére *Cipher Securer* terdiri dari lingkungan implementasi perangkat lunak, batasan implementasi perangkat lunak, implementasi arsitektur perangkat lunak, dan implementasi struktur data perangkat lunak.

1) Lingkungan Implementasi Perangkat Lunak

Perangkat lunak Vigenére *Cipher Securer* ini dikembangkan pada lingkungan perangkat keras komputer mobile (Notebook) yang memiliki spesifikasi sebagai berikut.

a. *Processor* Intel Core i7 Quad Core 2.2 GHz
b. *Memory* 8 GB 1333 MHz DDR3
c. Video Intel HD Graphics 3000 dan AMD Radeon HD 6750M 512 MB
d. Monitor 15.4” LED-backlit

Pada lingkungan perangkat lunak komputer, perangkat lunak Vigenére Cipher Securer dijalankan pada lingkungan:

a. Sistem Operasi Mac OS X Lion 10.7.5
b. Bahasa Pemrograman untuk perangkat lunak Vigenére Cipher Securer yang digunakan adalah PHP dan Javascript
c. Aplikasi yang dikembangkan dalam penelitian ini adalah aplikasi berbasis web

2) Batasan Implementasi Perangkat Lunak

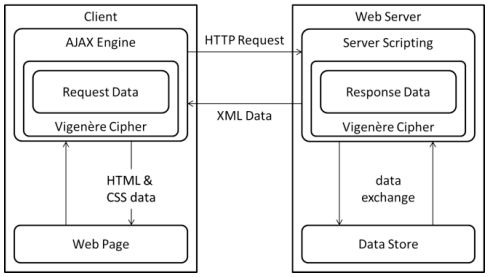
Adapun batasan yang terdapat dalam implementasi perangkat lunak implementasi Vigenére *Cipher Securer* ini adalah sebagai berikut.

a. Data yang dapat diolah oleh perangkat lunak adalah data berupa teks.
b. Perangkat lunak belum mampu menangani data berupa file.

3) Implementasi Arsitektur Perangkat Lunak

Sesuai dengan hasil perancangan arsitektur perangkat lunak, dapat diimplementasikan 2 fungsi utama yang digunakan untuk membuat Vigenére *Cipher Securer*, yakni fungsi untuk enkripsi dan dekripsi.

Secara umum implementasi dari perangkat lunak ini dapat dilihat pada Gambar 4.



Gambar 4 : Gambaran Umum Implementasi Vigenére *Cipher Securer*

4) Implementasi Struktur Data Perangkat Lunak

Struktur data utama yang digunakan dalam perangkat lunak Vigenére *Cipher Securer* ini adalah struktur data *string* dan atau *array of char*.

B. *Pengujian Perangkat Lunak*

Pengujian perangkat lunak merupakan proses menjalankan dan mengevaluasi sebuah perangkat lunak untuk menguji apakah perangkat lunak sudah memenuhi persyaratan atau belum untuk menentukan perbedaan antara hasil yang diharapkan dengan hasil sebenarnya.

1) Tujuan Pengujian Perangkat Lunak

ISSN 2252-9063
Kumpulan Artikel Mahasiswa Pendidikan Teknik Informatika (KARMAPATI)
Volume 2, Nomor 6, Agustus 2013

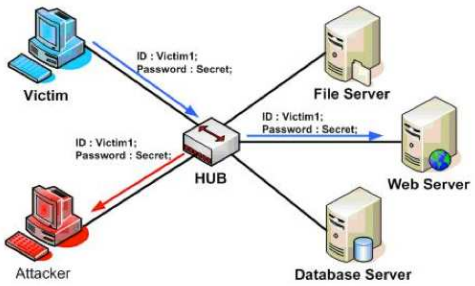
Tujuan pengujian berdasarkan konsep pengujian dikelompokkan menjadi dua yaitu pengujian fungsional (*black box testing*) dan pengujian konseptual/struktural (*white box testing*).

2) Pelaksanaan Pengujian Perangkat Lunak

Berdasarkan perancangan pengujian perangkat lunak, pengujian perangkat lunak Vigenére *Cipher Securer* ini dilakukan langsung oleh penulis, dan oleh ahli algoritma untuk uji kebenaran algoritmanya.

Pengujian perangkat lunak untuk uji fungsionalitas sistem dalam melakukan penyembunyian data pada jaringan. Pengujian implementasi terhadap perangkat lunak ini dilakukan dengan meng-*capture* paket data yang lalu lalang pada suatu *network* dengan bantuan sebuah aplikasi *packet sniffing*.

Adapun skenario penyerangan yang digunakan adalah skenario *Man In The Middle*. Skenario ini dilakukan dengan cara menangkap semua paket yang lalu lalang pada suatu *network*. Penyerang (*Attacker*) akan menyadap seluruh data yang ditransmisikan melalui *network* dimana korban melakukan transmisi data. Berikut gambaran skenario penyerangan yang dilakukan penyerang terhadap korbannya dapat dilihat pada Gambar 5.



Gambar 5 Skenario Penyerangan *Man In The Middle*

Berikut hasil pengujian pengiriman data tanpa penerapan perangkat lunak Vigenére *Cipher Securer* dapat dilihat pada Gambar 6 dan pengujian pengiriman data dengan penerapan perangkat lunak Vigenére *Cipher Securer* dapat dilihat pada Gambar 7.

Gambar 6 : Tanpa Vigenére *Cipher Securer*

Gambar 7 : Dengan Vigenére *Cipher Securer*

3) Evaluasi Hasil Pengujian Perangkat Lunak

Secara umum pelaksanaan pengujian perangkat lunak berlangsung dengan lancar, baik pada saat pengujian fungsionalitas sistem maupun saat pengujian algoritma oleh ahli algoritma. Dari hasil pengujian fungsionalitas sistem ketika berusaha menyembunyikan data, data yang terdeteksi pada jaringan sudah tidak dapat dibaca lagi karena teks yang terkirim pada jaringan sudah terenkripsi sehingga dapat dikatakan sudah layak digunakan sebagai perlindungan data pada saat mengalir menuju jaringan. Pengujian algoritma yang telah dilakukan oleh ahli algoritma sudah berhasil dengan baik, ini terbukti dari tanda sesuai pada uji algoritma.

V. SIMPULAN

Berdasarkan hasil analisis, implementasi dan pengujian pada penelitian ini, maka dapat diambil simpulan sebagai berikut.

1. *Vigenére Cipher Securer* dirancang menggunakan Bagan Alir (*Flowcart*) dengan 2 alur utama yakni pengiriman dan penerimaan data.
2. *Vigenére Cipher Securer* diimplementasikan menggunakan bahasa pemrograman PHP untuk basis *server* serta Javascript untuk basis *client* dengan menggunakan 2 jenis algoritma utama, yakni enkripsi dan dekripsi.

REFERENSI

[1] Ariyus, Dony. 2008. Pengantar Ilmu Kriptografi: Teori, Analisis, dan Implementasi. Yogyakarta: Penerbit Andi.

[2] Babin, Lee. 2007. Beginning Ajax with PHP: From Novice to Professional. New York: Apress.
[3] Gilmour, Ken. 2012. Network Eavesdropping. https://www.owasp.org/index.php/Network_Eavesdropping , (diakses tanggal 20 Jui 2013)
[4] Girsang, Truman Tuah. 2012. Analisis Kerahasiaan Data Menggunakan Algoritma Vigenere Cipher Dalam Sistem Pengamanan Data. Medan: Universitas Sumatera Utara.
[5] Munir, Rinaldi. 2006. Kriptografi. Bandung: Penerbit Informatika.
[6] Widodo, Dyan Hari. 2011. Implementasi Algoritma Enkripsi Dengan Metode Modifikasi Vigenere Cipher Dalam Aplikasi Pengiriman SMS Pada Ponsel Blackberry. Yogyakarta: Amikom.