IMPLEMENTASI ALGORITMA *HILL CIPHER* DENGAN MODIFIKASI PROSES MENGGUNAKAN ALGORITMA *CAESAR CIPHER* PADA FILE DOKUMEN PLAINTEXT

Skripsi

Untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1

Program Studi Teknik Informatika

Disusun oleh
Muhammad Azzam Mujaddid
13650023

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS ISLAM NEGERI SUNAN KALIJAGA
YOGYAKARTA
2017

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-07/R0

PENGESAHAN SKRIPSI/TUGAS AKHIR

Nomor : B-1389 /Un.02/DST/PP.05.3/ 05 /2017

Skripsi/Tugas Akhir dengan judul : Implementasi Algoritma *Hill Cipher* dengan Modifikasi Proses Algoritma *Caesar Cipher* pada File Dokumen Plaintext

Yang dipersiapkan dan disusun oleh :
Nama : Muhammad Azzam Mujaddid
NIM : 13650023
Telah dimunaqasyahkan pada : 2 Mei 2017
Nilai Munaqasyah : A-

Dan dinyatakan telah diterima oleh Fakultas Sains dan Teknologi UIN Sunan Kalijaga

TIM MUNAQASYAH :

Ketua Sidang

Sumarsono, M. Kom
NIP. 19710209 200501 1 003

Penguji I

Agung Fatwanto, Ph.D
NIP.19770103 200501 1 003

Penguji II

M. Didik R Wahyudi, M.T
NIP.19760812 200901 1 015

Yogyakarta, 8 Mei 2017
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

Dr. Murtono, M.Si
NIP. 19691212 200003 1 001

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : 1 Bendel Laporan Skripsi

Kepada
Yth. Dekan Fakultas Sains dan Teknologi
UIN Sunan Kalijaga Yogyakarta
di Yogyakarta

Assalamu'alaikum wr. wb.

Setelah membaca, meneliti, memberikan petunjuk dan mengoreksi serta mengadakan perbaikan seperlunya, maka kami selaku pembimbing berpendapat bahwa skripsi Saudara:

Nama : Muhammad Azzam Mujaddid
NIM : 13650023
Judul Skripsi : IMPLEMENTASI ALGORITMA *HILL CIPHER* DENGAN MODIFIKASI PROSES MENGGUNAKAN ALGORITMA *CAESAR CIPHER* PADA FILE DOKUMEN PLAINTEXT

sudah dapat diajukan kembali kepada Program Studi Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Kalijaga Yogyakarta sebagai salah satu syarat untuk memperoleh gelar Sarjana Strata Satu dalam Prodi Teknik Informatika

Dengan ini kami mengharap agar skripsi/tugas akhir Saudara tersebut di atas dapat segera dimunaqsyahkan. Atas perhatiannya kami ucapkan terima kasih.

Wassalamu'alaikum wr. wb.

Yogyakarta, 25 April 2017
Pembimbing

Sumarsono, S.T,M.Kom
NIP. 19710209200501 1 003

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertanda tangan di bawah ini :

Nama : Muhammad Azzam Mujaddid

NIM : 13650023

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi dengan judul "**Implementasi Algoritma *Hill Cipher* Dengan Modifikasi Proses Menggunakan Algoritma *Caesar Cipher* Pada File Dokumen Plaintext**" tidak terdapat karya yang pernah diakjukan untuk memperoleh gelar kesarjanaan di suatu Perguruan Tinggi, dan sepanjang pengetahuan saya juga tidak terdapat karya atau pendapat yang pernah ditulis atau diterbitkan oleh orang lain, kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 25 April 2017

Yang menyatakan,

Muhammad Azzam Mujaddid
NIM .13650023

KATA PENGANTAR

Puji syukur kehadirat Allah SWT yang telah memberikan rahmat serta karunia nikmatnya, sehingga penyusun masih dapat merasakan nafas yang penuh nikmat atas anugerah yang diberikan dalam penyelesaian skripsi ini.

Shalawat serta salam semoga senantiasa tercurah kepada Nabi Muhammad SAW , semoga kita kelak mendapat syafaatnya di yaumul akhir nanti. Skripsi ini disusun guna memenuhi sebagian persyaratan mendapatkan gelar Sarjana Teknik Informatika pada Program Studi Teknik Informarika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dalam kesempatan ini penulis menyampaikan terimakasih yang sebesar besarnya kepada:

1. Bapak Dr. Murtono M.Si ,Selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga
2. Bapak Dr. Bambang Sugiantoro, M.T , selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga
3. Kedua orangtua yang senantiasa memberikan dukungan.
4. Bapak Sumarsono S.T, M.Kom, selaku Dosen Pembimbing yang dengan sabar membimbing, mengarahkan , memberikan nasihat dan saran selama penyuunan skripsi.
5. Bapak Nurocman S.Kom M.Kom , selaku Dosesn penasihat akademik yang telah memberikan banyak bimbingan kepada penulis dan mahasiswanya dengan baik.

6. Seluruh Dosen Program Studi Teknik Informatika UIN Sunan Kalijaga yang selama ini memberikan ilmunya pada masa perkulaiahan kepada penulis.
7. Mas Chariz Fauzan , atas bimbingan dan ilmunya sehingga skripsi ini dapat terselesaikan dengan baik.
8. Mas zahid, noto, towi, tri, dan segenap kawan kawan asrama darul hikmah yang senantiasa memberikan support.
9. Reza , Yazid , Towi, Fauzi dan seluruh teman teman Teknik Informaika UIN Sunan Kalijaga angkatan 2013

Penulis menyadari tentu masih banyak kekurangan dalam Penulisan laporan skripsi ini, sehingga kritik serta saran dari pembaca sangat Penulis harapkan. Semoga dapat dijadikan sebagai dasar penyempurnaan penelitian selanjutnya.

Yogyakarta, 17 April 2018

Muhammad Azzam M
NIM.13650023

HALAMAN PERSEMBAHAN

Menulis adalah bagian dari mengabadikan masa , menjadikan setiap waktu sebagai rasa yang wajib di himpun dalam asa. Merangkai kolase kenanagan yang sudah telalu banyak untuk dibiarkan begitu saja. Menulis adalah mempersaksikan atas titah Tuhan, *nuuun, wal-qolami wa maa yasthuruuun* – Demi pena dan apa yang mereka tuliskan –

Dengan mencermati tiap kata dalam bait bait tulisan, Allah karuniakan fikiran untuk merenungkan betapa besar karunia yang telah diberikan kepada Manusia. Sebab itu menulis akan membingkai kebesaran karunia Allah.

Dengan mengharap ke ridhaan dan keberkahan Allah, penulisan skripsi ini dengan sepenuh hati Penulis persembahkan untuk Kedua orangtua yang senantiasa memberikan keteladanan serta dukungan baik secara moril maupun materil, beliau adalah Bapak Imam Jayadi beserta Ibu Siti Fatonah. Selanjutnya semoga Allah karunikan kasih dan sayang atas keteguhan hati dalam mendedikasikan segenap jiwa , raga dan waktunya untuk senantiasa memberikan arahan, nasihat, teladan dan doa yang baik kepada penulis.

HALAMAN MOTTO

"Kepandaian adalah kelicikan yang menyamar. Kebodohan adalah kebaikan yang bernasib buruk. Banyak orang yang cerdas! Banyak orang yang pandai. Tapi kecerdasan dan kepandaiannya itu hanya diperuntukkan untuk tujuan yang keji-keji belaka. Itu banyak terjadi , dan engkau tak boleh memasukkan dirimu kedalam golongan orang yang seperti itu."

-MH Ainun Najib-

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

IMPLEMENTASI ALGORITMA *HILL CIPHER* DENGAN MODIFIKASI PROSES MENGGUNAKAN ALGORITMA *CAESAR CIPHER* PADA FILE DOKUMEN PLAINTEXT

M Azzam Mujaddid

13650023

INTISARI

Pentingnya menjaga keamanan dokumen plaintext melalui proses enkripsi dalam kriptografi, berbagai algortima menawarkan proses yang beragam dalam melakukan enkripsi maupun dekripsi. Algoritma hill cipher memiliki keunikan diantara algoritma kriptografi klasik lainnya sebab menggunakan perkalian matriks dalam prosesnya. Namun ini menjadi kelemahan karena kunci yang digunakan adalah berbentuk matriks sehingga sangat mudah ditebak apabila proses enkripsi maupun dekripsi dilakukan dengan kunci matriks sudah pasti menggunakan algoritma hill cipher.

Penelitian yang akan dilakukan adalah melakukan implementasi algoritma kriptografi dengan modifikasi proses. Algoritma yang akan di gunakan adalah hill cipher dengan modifikasi proses subtitusi caesar cipher. Cara kerja dari algortima hill cipher adalah degan menggunakan perkalian matriks kunci. Matriks kunci yang digunakan memiliki ordo 2x2 serta modifikasi proses terletak pada kombinasi penentuan karakter awal menggunakan substitusi 3 caesar cipher.

Dalam penelitian ini memberikan hasil bahwa algortima modifikasi tersebut dapat di implementasikan dan memberikan alteranatif dalam proses kriptografi. Hasil pengujian yang di dapat adalah semakin banyak jumlah karakter yang diproses waktu yang dibutuhkan akan semakin lama. Besaran determinan juga mempengaruhi waktu dan ukuran selama poses berlangsung. Terjadi penambahan 1 karakter jika karakter awal proses enkripsi berjumlah ganjil. Proses enkripsi dapat berjalan dan dapat dilakukan dekripsi sesuai dengan aturan yang ditentukan.

Kata Kunci : Kriptografi , *Hill Cipher , Caesar Cipher* , Plaintext

THE IMPLEMENTATION OF HILL CIPHER ALGORITM WITH CAESAR CIPHER MODIFICATION PROCESS ON PLANINTEXT DOCUMENT

M Azzam Mujaddid

13650023

ABSTRACT

The importance of maintaining the security of plaintext documents through the encryption process in cryptography, various algorithms offer a variety of processes for encryption and description. The hill cipher algorithm is unique among other classical cryptographic algorithms because it uses matrix multiplication in the process. But this is a weakness because the key used is in the form of matrix so it is very easy to guess if the process of encryption or decryption is done with the key matrix is definitely using the hill cipher algorithm.

The research that will be done is to implement cryptographic algorithm with process modification. Algorithm that will be used is hill cipher with modification process of caesar cipher substitution. The working of the hill cipher algorithm is to use the matrix multiplication of keys. The key matrix to be used has a 2x2 order and process modification lies in a combination of initial character determination using a substitution of 3 caesar ciphers.

In research conducted to give results that algortima modification can be implemented and provide alteranatif in cryptography process. Test results obtained is the more the number of characters processed the time required will be longer. The magnitude of the determinant also affects time and size during the poses. A 1 character increment occurs if the initial character of the encryption process is an odd number. Encryption process can run and descriptions can be done in accordance with the rules specified.

Keyword : Crypthography , *Hill Cipher* , *Caesar Cipher* , Plaintext

BAB I
PENDAHULUAN

1.1 Latar Belakang

Dewasa ini , perkembangan teknologi informasi dan komunikasi sangat pesat, ditandai dengan kemudahan dalam mendapatkan akses terhadap perkembangan teknologi. Teknologi informasi telah menjadi bagian penting dari berbagai bidang kehidupan. Banyak sekali kemudahan yang ditawarkan. Teknologi informasi tidak dapat terlepas dari berbagai aspek kehidupan manusia. Salah satu kemudahan dari pesatnya perkembangan teknologi informasi adalah kemudahan pengelolaan file. Dahulu penulisan suatu dokumen memerlukan media berupa kertas, namun saat ini penulisan dan penyimpanan data dapat dilakukan secara digital. Dengan kemudahan yang disediakan kemajuan teknologi pengelolaan dokumen secara digital berbanding lurus teradap tingkat keamanan dari suatu dokumen digital, karena dokumen digital yang bersifat lemah, menyebabkan setiap orang dapat menlakukan akses terhadap dokumen tersebut ketika memiliki filenya secara legal ataupun ilegal. Maka hal ini memerlukan perhatian khusus dari segi kemanan, apalagi dokumen tersebut bersifat rahasia, hanya orang orang tertentu yang berhak mengakses dokumen tersebut.

Kriptografi adalah salah satu alternatif pemecahan masalah keamanan dokumen digital. Sebab dalam kriptografi dokumen akan di ubah menjadi karakter tertentu sesuai kunci pembangkit yang diberikan, proses ini disebut dengan enkripsi. Hanya orang yang memiliki kunci yang dapat melakukan proses dekripsi

atau menerjemahkan dokumen digital tersebut. Salah satu dari sekian banyak algoritma enkripsi dalam kriptografi adalah algoritma *Hill cipher*. Algoritma *hill cipher* menggunakan pembangkit kunci dengan matriks. Karakter pada dokumen asli akan di ubah menjadi karakter baru sesuai dengan aturan perkalian matriks.

Algoritma *hill cipher* merupakan salah satu algotima kunci simetris, dimana menggunakan matriks sebagai kunci untuk melakukan enkripsi dan dekripsi. Dasar teori matriks yang digunakan dalam *Hill cipher* antara lain adalah perkalian antar matriks dan melakukan invers pada matriks. Metode ini diciptakan oleh Lester S.*Hill* pada tahun 1929, algoritma *hill cipher* merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah kunci matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. Dengan melakukan implementasi Algoritma *Hill cipher* pada file dokumen tentu akan menjaga keamanan dari dokumen tersebut. Salah satu kelemahan algoritma *Hill cipher* adalah ketika kunci yang berbentuk matriks diketahui, maka otomatis proses kriptografi bisa dipastikan menggunakan algoritma *hill cipher*, karena hanya algoritma ini yang menggunakan kunci matriks. Perlu adanya modifikasi dalam proses enkripsi dan dekripsi.

Dengan melakukan modifikasi menggunakan algoritma *caesar cipher* dalam proses penentuan karakter awal dalam implementasi algoritma *hill cihper* akan memberikan alternatif agar hasil dari enkripsi tidak dengan mudah diketahui dan dipecahkan.Selain itu pemilihan modifikasi menggunakan algoritma caesar cipher dikarenakan kedua algoritma ini menggunakan metode subtitusi dan metode transposisi yang mudah dilakukan di komputer, kombinasi dari kedua teknik

kriptografi klasik ini menghasilkan tingkat keamanan yang lebih baik (Mishra,2013) *Caesar cipher* adalah bagian dari algoritma kriptografi klasik populer dimana setiap huruf pada *plaintext*, digantikan oleh huruf lain yang memliki selisih posisi tertentu dalam alfabet, *caesar cipher* menggeser tiap karakter sesuai dengan kunci yang diberikan. Dalam hal ini akan dilakukan penentuan karakter awal dengan subtitusi 3 karakter rotas seperti contoh dasar pada algoritma subtitusi *caesar cipher*. Penelitian sebelumnya tentang implementasi algoritma *hill cipher* dan caesar cipher dilakukan dengan menggunakan bahasa pemrograman PHP serta pada objek berbentuk database pada TB Mitra Jepara (Santosa,2015). Pada penelitian tersebut terfokus pada enkripsi database yang terdiri dari karakter angka.

Dalam kombinasi antara *hill cipher* dengan *caesar cipher* akan diberikan kunci berupa matriks 2 x 2, matiks kunci merupakan matriks invertible atau matriks yang mempunyai invers. Matriks berordo 2 x 2 dipilih sebagai kunci karena memiliki kesederhanaan proses yang sama dengan matriks berordo lain , adanya kesamaan proses implementasi dengan matriks berordo diatasnya dapat menjadi pertimbangan pemilihan kunci matriks berordo 2x2. Sehingga dalam proses enkripsi dan dekripsi hanya perlu menggunakan kunci matriks , namun dalam pengolahannya akan dikombinasikan antara perkalian matriks dengan penentuan karakter awal dari subtitusi caesar cipher.

Dokumen dengan ekstensi *txt atau plaintext sering digunakan untuk melakukan penyimpanan data data , dikarenakan ukuran file yang relatif ringan. Mengingat kemanan data dokumen tersebut, dibutuhkan alternatif keamanan

yang dapat menjaga kerahasiaan data tersebut. Sehingga data dokumen tersebut hanya bisa diakses oleh orang orang yang memliki kepentingan atas dokumen tersebut, jika dokumen tersebut secara diam diam dicuri oleh pihak lain maka pihak lain tidak mengerti akan isi dokumen tersebut.

Perlu adanya alternatif dalam menjaga file dokumen ,s alah satu alternatifnya adalah dengan melakukan implementasi algoritma kriptografi *Hill cipher* yang dimodifikasi dengan algoritma caesar cipher sehingga data dokumen digital memiliki keamanan yang kuat dan menjaga kerahasiaan data yang ada. Alternatif dalam melakukan implementasi Algoritma ini dapat dilakukan dengan bantuan pemrograman berbahasa java, sehingga tidak di implementasikan secara manual, mengingat data yang dijaga kerahasiaannya adalah data yang bersifat digital. Kemudian akan dilakukan pengujian kinerja algoritma tersebut.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang diatas, maka rumusan masalah yang akan dibahas adalah "Bagaimana melakukan implementasi algoritma kriptografi *Hill cipher* dengan modifikasi proses menggunakan algoritma *caesar cipher* untuk enkripsi dan dekripsi file dokumen plaintext"

1.3 Batasan Masalah

Agar penelitian ini lebih terarah dan tidak menyimpang dari rumusan masalah yang ada, maka batasan masalah dari penelitian ini hanya membahas mengenai proses enkripsi dan dekripsi menggunakan algoritma kriptografi *Hill cipher* dengan kunci matriks berordo 2 x 2 yang dikombinasikan dengan caesar cipher.

Penelitian ini akan berfokus pada dokumen berekstensi *txt yang berisi karakter alfabet.

1.4 Tujuan Penelitian

Penelitian ini bertujuan untuk melakukan pengkajian dan implementasi algoritma kriptografi *hill cipher* dengan modifikasi proses pada enkripsi dan dekripsi data file dokumen plaintext.

1.5 Manfaat Penelitian

Manfaat penelitian ini dapat membantu mengamankan dokumen dan dari penelitian ini dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan dekripsi di dalam data file dokumen menggunakan algoritma kriptografi *hill cipher* dan cipher subtitusi. Penelitian ini dapat digunakan sebagai refrensi dalam pembahasan mengenai pengembanan algoritma *hill cipher*, sehingga dapat memberikan inspirasi baru untuk pengembangan yang lebih baik.

1.6 Keaslian Penelitian

Penelitian tentang implemntasi algoritma *hill cipher* dengan melakukan modifikasi proses menggunakan algoritma *caesar cipher* sudah pernah dilakukan oleh peneliti lain namun dalam kombinasi yang berbeda dan pada objek database.

1.7 Sistematika Penulisan

Dalam penelitian ini, penulis melakukan sistem penulisan dalam lima bab , yaitu :

BAB I PENDAHULUAN

Berisi tentang latar belakang , perumusan masalah, batasan masalah, tujuan penelitian , manfaat penulisan, keaslian penelitian dan sistematika penulisan.

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Berisi tentang pejelasan penelitian yang pernah dilakukan sebelumnya dan landasan teori singkat mengenai kriptografi, algoritma *hill cipher* , algoritma caesar cipher, dan kunci matriks.

BAB III METODE PENELITIAN

Berisi tentang desain penelitian dan subyek penelitian serta alat yang diperlukan dalam pelaksanaan penelitian

BAB IV HASIL DAN PEMBAHASAN

Berisi tentang analisis mengenai proses kerja dari algoritma kriptografi *Hill cipher* dan Caesar cipher serta kombinasi dua algoritma tersebut pemrograman.

BAB V KESIMPULAN DAN SARAN

Berisi tentang kesimpulan yang diperoleh secara keseluruhan setelah menyelesaikan penelitian dan saran saran terhadap pengembangan yang selanjutnya.

BAB V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah dilakukan pengkajian dan implementasi algortima *hill cipher* dengan modifikasi proses pada enkripsi dan dekripsi dokumen plaintext dapat diambil kesimpulan sebagai berikut :

1. Penelitian ini berhasil melakukakan pengkajian dan menerapkan algoritma hill cipher dengan modifikasi untuk proses enkripsi dan deksripsi menggunakan subtitusi algortima caesar cipher pada dokumen plaintext dengan menggunakan matriks kunci berordo 2x2.
2. Penelitian ini berhasil menerapkan proses enkripsi dan dekripsi menggunakan algoritma hill cipher modifikasi menggunakan pemrograman java.
3. Proses enkripsi berpengaruh pada ukuran file, setelah dilakukan proses enkripsi ukuran file berkurang, menjadi sesuai dengan jumlah karakter, apabila dalam file memiliki karakter ganjil makan akan bertambah satu karakter sebagai penggenap. Semakin besar ukuran file waktu yang dibutuhkan semakin lama.
4. Ukuran file sebelum proses enkripsi dan sesudah proses dekripsi meliliki perbedaan, namun isi file memiliki jumlah karakter yang sama pada kasus karakter genap
5. Besar determinan matriks kunci berpengaruh pada waktu proses dari proses enkripsi maupun proses dekripsi.

5.2 Saran

Penelitian ini dapat dikembangkan menjadi penelitian yang lebih baik lagi dengan melakukan saran sebagai berikut :

1. Menggunakan kombinasi proses enkripsi maupun deskripi dengan algoritma lain.
2. Mengimplemetasian dengan bahasa lain akan memperkaya fitur yang disediakan termasuk jenis file yang dapat di enrkipsi maupun dekripsi sehingga aplikasi dapat dipergunakan sebagaimana mestinya .
3. Memperhatikan perubahan ukuran file sebelum dan sesudah diproses. Sehingga dapat mengidentifikasi perbedaan yang terjadi disebabkan oleh apa.
4. Dapat melakukan proses dengan tipe file yang lebih beragam.

DAFTAR PUSTAKA

Annelis, S. 2010. *Pengkodean Pesan Menggunakan Perpaduan nCaesar Cipher dan RSA Pada Kriptografi Hibrida.* Skripsi. Universitas Andalas.

Febriansyah,2015 ”*Analisis dan perancangan keamanan data menggunakan Algoritma Kriptografi DES (Data Encryption Standard)* Universitas Bina Darma

Forouzan, Behrouz.2010 *Cryptogrphy and Netwprk Security*. MCGraw-*Hill*, Newyork.

Lusiana, Veronica 2015*“ Implementasi Kriptografi pada file Dokumen menggunakan Algoritma AES-128*”

Munir, Rinaldi 2006. Diktat kuliah IF5054 Kriptografi. Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, ITB

Mishra, Anupama.2013. *Enhancing Security of Caesar Cipher using different Method.*IJRET. Vol 2. P 332.

Prayudi, Yudi, Idham Halik. 2005. *Studi Analisis Algoritma Rivest Code 6 (RC6) Dalam Enkripsi/Dekripsi Data*. Seminar Nasional Aplikasi Teknologi Informasi 2005 (SNATI 2005), Yogyakarta.

Puspita, Niken Prima dan Nurdin Bahtiar 2014 “*Kriptografi Hill cipher dengan menggunakan operasi Matriks*” Matematika. UNDIP Semarang

Sadikin, Rifki. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Penerbit Andi, Yogyakarta

Sansasni, S. 2008. *Penggunaan Aritmatika Modulo dan Balikan Modulo pada modifikasi Algoritma Knapsack* . *Makalah* Bandung. Teknik Informatika ITB Bandung

Security, Komputer. 2009. *Teknik Keamanan Komputer, Enkripsi & Dekripsi.* http://security-komputer.blogspot.com/2009/12/teknik-kemanan-komputerenkripsi.html. Diakses 20 Maret 2017 11.50

Wirdasari, Dian. 2008. *Prinsip Kerja Kriptografi dalam Mengamankan Informasi*, Jurnal SAINTIKOM Vol.5 No.2.

Yliandaru, Adam Rotal 2015 “ *Teknik Kriptogradi Hill cipher menggunakan Matriks*” STEI ITB Bandung.

LAMPIRAN

LAMPIRAN SOURCE CODE

Source Code Enkripsi

```
    public String enkripText(String plaintext,
    int[][] password) {
            HillChiper_Enkripsi Enkrip = new
    HillChiper_Enkripsi();
            String hasil =
    Enkrip.hitungEnkripsi(plaintext, password);
            return hasil;   }
```

Fungsi membagi karakter menjadi 2 blok

```
String teksnya = text;
        if (teksnya.length() % 2 == 0) {
            teksnya = text;
        } else {
            teksnya = text + ".";
        }
        assert teksnya.length() % 2 == 0;
        teks2karakter = new String[teksnya.length()
/ 2];
        for (int index = 0; index <
teks2karakter.length; index++) {
            teks2karakter[index] =
teksnya.substring(index * 2, index * 2 + 2);

System.out.println(teks2karakter[index]);
        }
        return teksnya;
    }
```

Fungsi Mengkonversi dari Abjad ke angka

```
hasilKonversi = new String[text.length][2];
             for (int i = 0; i < text.length; i++) {
            String char1 = text[i].substring(0, 1);
            String char2 = text[i].substring(1);

            for (int j = 0; j < abjad.length; j++) {
                if (char1.equals(abjad[j])) {
                    char1 = String.valueOf(angka[j]);
                }
                if (char2.equals(abjad[j])) {
                    char2 = String.valueOf(angka[j]);
                }
            }

            if (hasilKonversi[i][0] == null) {
                hasilKonversi[i][0] = char1;

                if (hasilKonversi[i][1] == null) {
                    hasilKonversi[i][1] = char2;

                }
            }
        }

        for (int n = 0; n < hasilKonversi.length; n++)
{
            for (int p = 0; p <
hasilKonversi[0].length; p++) {
                System.out.print(hasilKonversi[n][p] +
" ");
            }
            System.out.println("");
        }

        return hasilKonversi;
    }
```

Fungsi utama dalam proses Enkripsi

```
int kunciK0B0 = kunci[0][0];
        int kunciK0B1 = kunci[0][1];
        int kunciK1B0 = kunci[1][0];
        int kunciK1B1 = kunci[1][1];

        hasilHitungKunci = new String[angka.length][2];

        for (int n = 0; n < angka.length; n++) {
            int konvert =
Integer.parseInt(angka[n][0]);
            int konvert1 =
Integer.parseInt(angka[n][1]);
            int hasil = (kunciK0B0 * konvert) +
(kunciK0B1 * konvert1);
            int hasil1 = (kunciK1B0 * konvert) +
(kunciK1B1 * konvert1);

            System.out.println(hasil + " " + hasil1);

            hasil = hasil % modulo;
            hasil1 = hasil1 % modulo;


            //   System.out.println(hasil + " " +
hasil1);

            if (hasilHitungKunci[n][0] == null) {
                hasilHitungKunci[n][0] =
String.valueOf(hasil);
                if (hasilHitungKunci[n][1] == null) {
                    hasilHitungKunci[n][1] =
String.valueOf(hasil1);
                }
            }
        }
```

Fungsi akhir proses enkripsi

```
for (int i = 0; i < hasilHitungKunci.length; i++) {
            for (int j = 0; j <
hasilHitungKunci[0].length; j++) {
                //
System.out.print(hasilHitungKunci[i][j]+" ");
```

```
                for (int k = 0; k < angka.length; k++)
{
                    if
(hasilHitungKunci[i][j].equals(String.valueOf(angka[k])
)) {
                        hasilEnkripsi = abjad[k];
                        totalHasilEnkrip =
totalHasilEnkrip + hasilEnkripsi;
                    }
                }
            }
        }
        System.out.println(totalHasilEnkrip);
        return totalHasilEnkrip;
```

Source Code Dekripsi

```
public String dekripText(String plaintext, int[][]
password) {
        HillChiper_Dekripsi Dekrip = new
HillChiper_Dekripsi();
        String hasil = Dekrip.hitungDekripsi(plaintext,
password);
        return hasil;
    }
```

Fungsi mencari Invers dadi matriks Kunci

```
int determinan = (matriks[0][0] * matriks[1][1]) -
(matriks[0][1] * matriks[1][0]);
        System.out.println("Determinan : " +
determinan);
        if (determinan == 0) {
            System.out.println("Matrik tidak memiliki
invers");
```

```
        } else if(determinan < 0){
            JOptionPane.showMessageDialog(null, "Kunci
Tidak Memenuhi Syarat");
        }else {

            int d = matriks[1][1];
            int c = -(matriks[1][0]);
            int b = -(matriks[0][1]);
            int a = (matriks[0][0]);

            matrikInvers[0][0] = d;
            matrikInvers[0][1] = b;
            matrikInvers[1][0] = c;
            matrikInvers[1][1] = a;

            int MultiplikatifDet = 0;
            for (MultiplikatifDet = 0; MultiplikatifDet
< 1000; MultiplikatifDet++) {
                if ((determinan * MultiplikatifDet) %
modulo == 1 % modulo && determinan>0) {
                    MultiplikatifDet =
MultiplikatifDet;
                    System.out.println("MultiPlikatif =
" + MultiplikatifDet);
                    break;
                }
            }

            for (int i = 0; i < matrikInvers.length;
i++) {
                for (int j = 0; j <
matrikInvers[0].length; j++) {
                    if (matrikInvers[i][j] < 0) {
                        matrikInvers[i][j] = modulo -
(Math.abs(matrikInvers[i][j]) % modulo);
                    } else {
                        matrikInvers[i][j] =
matrikInvers[i][j] %modulo;
                    }
                    matrikInvers[i][j] =
matrikInvers[i][j]*MultiplikatifDet ;
                    matrikInvers[i][j] =
matrikInvers[i][j]%modulo ;
                }
                System.out.println("");
            }
```

```
            for (int i = 0; i < matrikInvers.length;
i++) {
                for (int j = 0; j <
matrikInvers[0].length; j++) {
                //
System.out.print(matrikInvers[i][j] + " ");
                }
                System.out.println("");
            }

        }
        return determinan;
    }
```

Fungsi membagi teks menjadi 2 blok

```
String teksnya = text;
        if(teksnya.length() % 2 == 0){
            teksnya = text ;
        }else{
            teksnya = text + "." ;
        }
        assert teksnya.length() % 2 == 0 ;
        System.out.println(teksnya.length());
        Hasil_pisahkanTeks = new
String[teksnya.length() / 2];
        for (int index = 0; index <
Hasil_pisahkanTeks.length; index++) {
            Hasil_pisahkanTeks[index] =
teksnya.substring(index * 2, index * 2 + 2);

System.out.println(Hasil_pisahkanTeks[index]);
        }
        return teksnya;
    }
```

Fungsi merubah Abjad ke Angka

```
asil_AbjadKeAngka = new String[text.length][2];

        for (int i = 0; i < text.length; i++) {
            String char1 = text[i].substring(0, 1);
            String char2 = text[i].substring(1);

            for (int j = 0; j < abjad.length; j++) {
```

```
                if (char1.equals(abjad[j])) {
                    char1 = String.valueOf(angka[j]);
                }
                if (char2.equals(abjad[j])) {
                    char2 = String.valueOf(angka[j]);
                }
            }

            //System.out.print(char1 + " ");
            //System.out.println(char2 + " ");
            if (Hasil_AbjadKeAngka[i][0] == null) {
                Hasil_AbjadKeAngka[i][0] = char1;
                //System.out.print(hasilKonversi[i][0]
+ " ");
                if (Hasil_AbjadKeAngka[i][1] == null) {
                    Hasil_AbjadKeAngka[i][1] = char2;
                    //
System.out.println(hasilKonversi[i][1] + " ");
                }
            }
        }

        for (int n = 0; n < Hasil_AbjadKeAngka.length;
n++) {
            for (int p = 0; p <
Hasil_AbjadKeAngka[0].length; p++) {

System.out.print(Hasil_AbjadKeAngka[n][p] + " ");
            }
            System.out.println("");
        }

        return Hasil_AbjadKeAngka;
    }
```

Fungsi merubah dari Angka ke abjad

```
for (int i = 0; i < hasilHitungKunci.length; i++) {
            for (int j = 0; j <
hasilHitungKunci[0].length; j++) {
                //
System.out.print(hasilHitungKunci[i][j]+" ");
                for (int k = 0; k < angka.length; k++)
{
                    if
(hasilHitungKunci[i][j].equals(String.valueOf(angka[k])
```

```
)) {
                        hasilDeskrip = abjad[k];
                        totalHasilDeskrip =
totalHasilDeskrip + hasilDeskrip;
                    }
                }
            }
        }

        System.out.println(totalHasilDeskrip);
        return totalHasilDeskrip;
```

Fungsi akhir proses dekripsi

```
HillChiper_Dekripsi yuk = new HillChiper_Dekripsi();
        yuk.hitungInvers(kunci);
        yuk.pisahkanTeks(text);
        yuk.AbjadKeAngka(Hasil_pisahkanTeks);
        yuk.perhitunganKunci(Hasil_AbjadKeAngka,
matrikInvers);
        yuk.AngkaKeAbjad(hasilHitungKunci);
        return totalHasilDeskrip;
```

CURICULUM VITAE

Nama Lengkap : MUHAMMAD AZZAM MUJADDID

Jenis Kelamin : LAKI-LAKI

TTL : MADIUN, 29 MEI 1996

ALAMAT 1 : GEPLAK 01/01 KARAS MAGETAN

ALAMAT 2 : Jl.BIMOKURDO GK 1 YOGYAKARTA

EMAIL : MUJADDID29@GMAIL.COM

NO HP : 089679319845

Jenjang	Nama Sekolah	Tahun
TK	RA Al Ikhlas Mantren	2001-2003
SD	SDIT Al Ikhlas Mantren	2003-2009
SMP	SMPN 1 Karangrejo	2009-2011
SMU	MAN 2 MADIUN	2011-2013
S1	UIN SUNAN KALIJAGA	2013-2017