MODIFIKASI ALGORITMA PLAYFAIR CIPHER DENGAN MATRIKS 5X19 DAN TEKNIK EKSPANSI KRIPTOGRAFI PADA PESAN PLAINTEXT

Skripsi

Untuk memenuhi sebagian persyaratan
mencapai derajat Sarjana S-1
Program Studi Teknik Informatika

Disusun oleh :

Amiroh Mujahidah

14650031

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

2018

HALAMAN PENGESAHAN

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

PENGESAHAN SKRIPSI/TUGAS AKHIR
Nomor : B-537/UIN.02/D.ST/PP.01.1/07/2018

Skripsi/Tugas Akhir dengan judul : " Modifikasi Algoritma Playfair Cipher dengan Matriks 5x19 dan Teknik Ekspansi Kriptografi pada Pesan Plaintext"

Yang dipersiapkan dan disusun oleh :
Nama : Amiroh Mujahidah
NIM : 14650031
Telah dimunaqasyahkan pada : 8 Juni 2018
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

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

Penguji II

Aulia Faqih Rifa'i, M. Kom
NIP.19860306 201101 1 009

Yogyakarta,2 Juli 2018
UIN Sunan Kalijaga
Fakultas Sains dan Teknologi
Dekan

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

HALAMAN PERSETUJUAN

Universitas Islam Negeri Sunan Kalijaga FM-UINSK-BM-05-03/R0

SURAT PERSETUJUAN SKRIPSI/TUGAS AKHIR

Hal : Persetujuan Skripsi
Lamp : -

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 : Amiroh Mujahidah
NIM : 14650031
Judul Skripsi : "Modifikasi Algoritma Playfair Cipher Dengan Matriks 5x19 dan Teknik Ekspansi Kriptografi Pada Pesan 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 Program Studi 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, 06 Juni 2018
Pembimbing

Sumarsono, M.Kom
NIP. 19710209 200501 1 003

HALAMAN PERNYATAAN KEASLIAN

SURAT KETERANGAN KEASLIAN SKRIPSI

Saya yang bertanda tangan dibawah ini:

Nama : Amiroh Mujahidah

NIM : 14650031

Program Studi : Teknik Informatika

Fakultas : Sains dan Teknologi

Menyatakan bahwa skripsi saya yang **berjudul "Modifikasi Algoritma Playfair Cipher Dengan Matriks 5x19 Dan Teknik Ekspansi Kriptografi Pada Pesan Plaintext"** merupakan hasil penelitian saya sendiri, tidak terdapat karya yang pernah diajukan untuk memperoleh gelar kesarjanaan di suatu perguruan tinggi, dan bukan plagiasi karya orang lain kecuali yang secara tertulis diacu dalam naskah ini dan disebutkan dalam daftar pustaka.

Yogyakarta, 06 Juni 2018

Yang menyatakan,

Amiroh Mujahidah

NIM. 14650031

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 syafa'atnya di yaumul akhir. Skripsi ini disusun guna memenuhi sebagian persyaratan mendapat gelar Sarjana Teknik Informatika pada Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga Yogyakarta. Dalam kesempatan ini penulis menyampaikan terimakasih sebesar-besarnya kepada :

1. Bapak Prof. Yudian Wahyudi, MA, Ph.D, selaku Rektor UIN Sunan Kalijaga Yogyakarta.
2. Bapak Dr. Murtono M.Si , selaku Dekan Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
3. Bapak Dr. Bambang Sugiantoro, M.T , selaku Ketua Program Studi Teknik Informatika Fakultas Sains dan Teknologi Universitas Islam Negeri Sunan Kalijaga.
4. Bapak Sumarsono S.T, M.Kom, selaku Dosen Pembimbing serta Dosen Penasihat Akademik yang dengan sabra membimbing, mengarahkan, memberikan nasihat dan saran kepada penulis selama penyusunan skripsi maupun menyelesaikan proses akademik.
5. Kedua orangtua yang senantiasa memberikan dukungan.

6. Seluruh Dosen Program Studi Teknik Informatika UIN Sunan Kalijaga yang selama ini memberikan ilmunya pada masa perkuliahan kepada penulis.
7. Seluruh teman-teman Teknik Informatika angkatan 2014 atas segala dukungannya kepada penulis.

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

Yogyakarta 21 Mei 2018

Amiroh Mujahidah
NIM. 14650031

HALAMAN PERSEMBAHAN

Dengan mengucap segala syukur atas selesainya Skripsi ini, saya persembahkan nikmat ini dengan mengucapkan seluruh rasa terimakasih kepada:

1. Rabbul'alamin, ALLAH SWT, atas segala rahmat, nikmat, kasih sayang dan karunia-Nya yang begitu melimpah hingga tak mampu saya sebutkan.
2. Nabiyullah, Muhammad SAW, panutan, suri tauladan, motivator terbesar ku.
3. Abi-Umi yang ku cintai, Abi Sudaryono dan Umi Nur Laily, segala dukungan terbaik selalu diberikan untuk ku.
4. Kedua saudaraku, Mas Azzam dan Adek Fatiyah, yang selalu menyayangi dan menyemangati aku.
5. Seluruh tim Teknik Informatika UIN angkatan 2014, yang selalu mendukung dan menyemangati dalam menempuh perjalanan dunia kampus.

Kepada seluruh rekan yang tak bisa disebutkan satu per satu, ucapan terimakasih terbesar ku ucapkan, semoga Allah senantiasa melimpahkan kasih sayang dan karunia-Nya kepada kalian, sehingga seluruh kebaikan yang telah kalian berikan akan dibalas-Nya dengan kebaikan berlipat ganda.

~ Terimakasih ~

HALAMAN MOTTO

"….Maka sesungguhnya bersama kesulitan ada kemudahan. Sesungguhnya bersama kesulitan ada kemudahan. Maka apabila engkau telah selesai (dari suatu urusan), tetaplah bekerja keras (untuk urusan yang lain). Dan hanya kepada Rabb mu lah engkau berharap."

Q.S Al-Insyirah (94) : 5 - 8

Dunia ini seperti bermain *game* , Allah tidak akan meletakkan mu pada level2 *game* ini jika engkau belum menyelesaikan seluruh tantangan di level1. Ketika Allah menguji mu pada salah satu tantangan di level1 tapi engkau tidak mampu melewatinya, maka Allah tetap meletakkanmu pada level1 hingga engkau pantas masuk pada level2.

~ Hamba ALLAH ~

DAFTAR ISI

DAFTAR GAMBAR

DAFTAR TABEL

INTISARI

Kriptografi atau teknik menyembunyikan pesan dapat menjadi solusi agar terhindar dari kejahatan *cyber crime*. Playfair Cipher merupakan salah satu algoritma kriptografi yang dapat menyembunyikan pesan dengan membentuk kunci pesan dalam bentuk matriks kunci berbentuk bujursangkar ukuran 5x5 untuk menampung 25 karakter huruf kapital dengan menghilangkan huruf J dan menggantikannya dengan huruf I. Kemudian menjadikan pesan plaintext ke dalam pasangan huruf (*bigram*) untuk dilakukan proses enkripsi dengan beberapa aturan dan ketentuan pada algoritma ini. Sehingga terbentuk ciphertext yang memiliki panjang karakter yang sama dengan plaintext nya.

Mekanisme algoritma playfair cipher inilah yang menjadi kelemahan dari playfair cipher, keterbatasan dalam menampung karakter, penghilangan huruf J yang menyebabkan ambigu serta panjang karakter plaintext dan ciphertext yang sama sehingga mudah untuk dipecahkan dengan frekuensi kemunculan bigram. Modifikasi algoritma playfair cipher dengan memperluas matriks kunci 5x19 dengan 95 karakter untuk menampung banyak karakter (huruf kapital, kecil, angka, simbol) dan menghilangkan ambiguitas serta teknik ekspansi kriptografi untuk membentuk hasil ciphertext yang berbeda dengan plaintext nya dapat menjadi solusi dari kelemahan playfair cipher. Tujuan dari penelitian ini untuk menghasilkan algoritma modifikasi playfair cipher yang dapat menutupi kelemahan playfair cipher dan menghasilkan perbedaan panjang karakter pada hasil implementasi plaintext dan ciphertext dari modifikasi playfair cipher.

Kata Kunci : Playfair Cipher, Matriks Kunci, Teknik Ekspansi Kriptografi

ABSTRACT

Cryptography is techniques to hide messages can be a solution to avoid this crime. Playfair Cipher is one of the cryptographic algorithms that can hide the message well because it forms a message key in matrix form. Playfair ciphers form a 5x5 square-shaped key matrix to hold up to 25 characters of capital letters by omitting the letter J and replace it with the letter I. Then make the plaintext message into the bigram pairs to do the encryption process with some rules and conditions in this algorithm. Thus formed ciphertext which has the same character length as its plaintext.

This mechanism of the playfair cipher algorithm is the weakness of the playfair cipher, the limitations in holding the characters, the removal of the letter J that causes ambiguity and the length of plaintext characters and the same ciphertext making it easy to solve with the frequency of occurrence bigram. The modification of the playfair cipher algorithm by extending the 5x19 key matrix with 95 characters to hold many characters (capital letters, small, numbers, symbols) and eliminating ambiguity and cryptographic expansion techniques to form different ciphertext results with its plaintext can be a solution to the weakness of playfair cipher. The purpose of this study was to produce a playfair cipher modification algorithm that could cover the weakness of playfair cipher and result in differences in character length on plaintext and ciphertext implementation results from playfair cipher modification.

Keywords: Playfair Cipher, Key Matrix, Cryptography Expansion Technique

BAB I

PENDAHULUAN

1.1 Latar Belakang

Teknologi digital dimasa kini yang semakin canggih telah membuat perubahan besar terhadap dunia, lahirnya berbagai macam teknologi digital yang semakin maju telah banyak bermunculan. Berbagai kalangan telah mudah dalam mengakses suatu informasi melalui banyak cara, serta dapat menikmati fasilitas dari teknologi digital dengan bebas dan tak terkendali. Teknologi digital komunikasi merupakan salah satu yang berkembang pesat di kalangan masyarakat dewasa ini sebagai sarana menyampaikan dan menerima informasi dari orang lain. Komunikasi *visual* yang dahulu menggunakan surat dalam bentuk kertas yang dikirimkan melalui seorang kurir kini telah terdigitalisasi melalui chat *online* ataupun email tanpa membutuhkan perantara seorang kurir dan tidak memerlukan waktu yang lama, segala nya dapat terproses dengan cepat melalui teknologi digital. Tetapi semakin berkembangnya teknologi digital justru semakin banyaknya kejahatan yang terdeteksi.

Perkembangan kemajuan teknologi informasi saat ini, semakin memudahkan para pelaku kejahatan komputer (*cyber crime*), atau yang sering disebut dengan istilah *cracker, script kiddies, carder, lamer* ataupun istilah nama yang lain, dengan menyalahgunakan teknologi komputer tersebut untuk mendukung kegiatannya, dimana aktivitas mereka sangat mengganggu privasi seseorang. Oleh karena itu diperlukan sebuah alternatif yang aman sehingga dapat

mempersulit para pelaku kejahatan komputer untuk melakukan aktivitasnya, dan membantu para pengguna teknologi dalam hal pengamanan data yang diakses tersebut. Kemudahan untuk mengakses dan mendapatkan berbagai informasi pun mudah untuk didapatkan dengan adanya internet. Internet merupakan kependekan dari *interconnection-networking*, yaitu seluruh jaringan komputer yang saling terhubung menggunakan standar global *transmission control protocol* (TCP). Tentuya dibalik setiap kemudahan mengakses untuk mendapatkan infromasi, ada beberapa oknum jahat yang berusaha untuk memanfaatkan berbagai informasi yang dengan sangat mudah untuk diperoleh. Kejahatan yang biasa terjadi memakan korban disemua kalangan dan terjadi di semua bidang profesi dengan tujuan dan maksud tertentu, mulai dari anak-anak hingga orang dewasa, mulai dari individual hingga pada kelompok, mulai dari kelompok usaha kecil hingga pada perusahaan besar, dimana ada persaingan pasti ada strategi untuk mendapatkan kemenangan. Bahkan sebuah negara pun mendapatkan ancaman dengan adanya kemudahan memperoleh sebuah data. Masalah dalam pengamanan informasi tersebut dapat diatasi dengan suatu metode yang disebut dengan kriptografi.

Kriptografi dapat mengubah pesan rahasia menjadi pesan acak yang (*ciphertext)* yang tidak memiliki makna sehingga pesan rahasia hanya dapat terbaca oleh pihak yang berhak, namun teknik ini memiliki kelemahan yaitu pesan acak yang ditampilkan dapat menimbulkan kecurigaan sehingga memungkinkan pelaku kejahatan untuk memanipulasi serta memodifikasi pesan acak *(ciphertext)* yang mengakibatkan pesan rahasia menjadi rusak. Enkripsi merupakan sebagian

dari kriptografi, dan merupakan hal yang sangat penting agar keamanan pesan yang dikirimkan bisa terjaga kerahasiaannya.

Enkripsi bisa diartikan dengan cipher atau kode, dimana pesan asli (*plaintext*) diubah menjadi kode-kode tersendiri sesuai metode yang disepakati oleh kedua belah pihak, baik pihak pengirim pesan maupun penerima pesan (Pramono.A dan Sujjada.A).

Kriptografi telah menjadi bagian penting dalam dunia teknologi informasi saat ini. Hampir semua penerapan teknologi informasi menggunakan kriptografi sebagai alat untuk menjamin keamanan dan kerahasiaan informasi. Karena itu pulalah, kriptografi menjadi ilmu yang berkembang pesat. Dalam waktu singkat, amat banyak bermunculan algoritma-algoritma baru yang dianggap lebih unggul daripada pendahulunya. Algoritma modern yang banyak bermunculan pun bermula dari teknik-teknik pada algoritma klasik. Terdapat banyak jenis algoritma klasik dalam kriptografi, salah satunya Algoritma Playfair Cipher.

Menurut Stallings (2010) Algoritma Playfair Cipher menggunakan papan kunci yang berbentuk bujursangkar dalam melakukan penyandian. Papan kunci ini berukuran 5x5, dimana setiap bagian dalam papan kunci mewakili huruf-huruf dalam alphabet (abjad) dengan menghilangkan huruf J dari abjad. Setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain. Playfair Cipher memiliki beberapa kelemahan, papan kunci yang hanya mampu menampung 25 huruf abjad dalam format kapital, penghilangan huruf J dalam rangkaian papan kunci bujursangkar menyebabkan ambiguitas saat memodifikasi pesan informasi.

Sehingga dalam perkembangannya banyak peneliti yang mengembangkan algoritma ini sesuai dengan kebutuhan penggunaan di era modern, beberapa penelitian mengembangkan dengan cara menggabungkan dengan metode klasik lainnya, ada pula yang mengembangkan dengan cara memperlebar papan kunci bujursangkar menjadi beberapa matriks yang mampu menampung banyak karakter baik huruf kapital, huruf kecil, angka maupun simbol-simbol. Namun, meninjau dari adanya berbagai penelitian yang telah dilakukan penulis menemukan kelemahan lain yang belum teratasi yakni panjang karakter *plaintext* yang sama dengan *ciphertext* yang dihasilkan sehingga penyandian ini masih memiliki kemungkinan untuk dapat dipecahkan dengan frekuensi kemunculan.

Untuk mempersulit para pelaku kejahatan komputer dalam memecahkan pesan informasi yang diamankan menggunakan algoritma playfair cipher, berdasar kelemahan tersebut maka penulis mencoba meneliti mengembangkan algoritma Playfair Chiper dengan cara pengembangan papan kunci berdasarkan jumlah karakter yang dapat dicetak melalui papan *keyboard* yakni dengan matriks berukuran 5x19 yang digabungkan dengan teknik ekspansi kriptografi untuk menghasilkan panjang karakter yang berbeda antara *plaintext* dan *ciphertext* yang dihasilkan. Sehingga diharapkan mampu menambah keamanan sebuah pesan informasi. Oleh karena penulis memilih judul "**Modifikasi Algoritma Playfair Chiper dengan Matriks 5x19 dan Teknik Ekspansi Kriptografi pada Pesan Plaintext**" untuk meningkatkan keamanan pada Algoritma Playfair Cipher.

1.2 Rumusan Masalah

Berdasarkan penjelasan dari latar belakang diatas, maka rumusan masalah yang akan dibahas adalah :

1. Bagaimana menyusun algoritma modifikasi dari Algoritma Playfair Cipher?
2. Bagaimana hasil implementasi plaintext dan ciphertext dari modifikasi Algoritma Playfair Cipher?

1.3 Batasan Masalah

Agar penelitian lebih terarah dan tidak menyimpang dari rumusan masalah yang ada, maka batasan masalah dari penelitian ini adalah :

1. Pesan yang digunakan berupa karakter *printable ASCII* yang terdapat pada keyboard.
2. Algoritma yang akan dimodifikasi adalah Algoritma Playfair Cipher.
3. Modifikasi menggunakan matriks berukuran 5x19 dan teknik ekspansi kriptografi.

1.4 Tujuan Penelitian

Tujuan dari penelitian ini, yaitu :

1. Menghasilkan algoritma modifikasi playfair cipher yang dapat menutupi kelemahan dari Algoritma Playfair Cipher.
2. Mengetahui hasil implementasi plaintext dan ciphertext dari modifikasi Algoritma Playfair Cipher.

1.5 Manfaat Penelitian

Manfaat penelitian ini yaitu :

1. Dapat membantu mengamankan pesan teks.
2. Dapat menambah pengetahuan dan wawasan penulis tentang kriptografi khususnya dalam hal proses enkripsi dan dekripsi pesan teks dari modifikasi algoritma playfair cipher.
3. Penelitian ini dapat digunakan sebagai referensi dalam pembahasan mengenai pengembangan algoritma playfair cipher, sehingga dapat memberikan inspirasi baru untuk pengembangan yang lebih baik.

1.6 Keaslian Penelitian

Penelitian tentang modifikasi algoritma playfair cipher sudah pernah dilakukan oleh peneliti lain namun dengan panjang matriks dan kombinasi yang berbeda serta hasil enkripsi dan dekripsi yang berbeda dari penelitian yang dilakukan oleh penulis.

1.7 Sistematika Penulisan

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

BAB I PENDAHULUAN

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

BAB II TINJAUAN PUSTAKA DAN LANDASAN TEORI

Berisi tentang penjelasan penelitian yang pernah dilakukan sebelumnya dan landasan teori mengenai kriptografi, algoritma playfair cipher, teknik dasar kriptografi 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 modifikasi algoritma playfair cipher serta analisis hasil implementasi pesan plaintext, enkripsi dan dekripsi.

BAB V KESIMPULAN DAN SARAN

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

BAB V

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Setelah dilakukan pengkajian dan implementasi terhadap modifikasi algoritma playfair cipher dapat diambil kesimpulan :

1. Algoritma Playfair Cipher hanya mampu menampung 25 huruf kapital menggunakan matriks 5x5 dengan menggantikan huruf J menjadi I menyebabkan hasil dekripsi ambigu dengan plaintextnya, maka modifikasi dengan memperluas matriks kunci menjadi 5 x 19 mampu menampung 95 karakter berupa huruf kapital, huruf kecil, angka dan simbol tanpa adanya penggantian/penghilangan huruf J, sehingga hasil dekripsi dapat terbaca seperti pesan plaintext nya.
2. Algoritma Playfair Cipher menjadikan pesan plaintext ke dalam pasangan huruf (*bigram*) sehingga terbentuk ciphertext yang memiliki panjang karakter sama dengan plaintext yang menyebabkan dapat dilakukan kripanalisis dengan frekuensi kemunculan bigram. Maka teknik ekspansi kriptografi mampu menghasilkan panjang karakter ciphertext lebih panjang dari plaintextnya agar sulit untuk dipecahkan.
3. Jika persyaratan atau kondisi yang terdapat dalam ketentuan algoritma terpenuhi akan menyebabkan pesan hasil dekripsi berbeda dengan plaintext.

4. Modifikasi algoritma playfair cipher ini memiliki kelemahan yakni dapat dilakukan kripanalisis dengan frekuensi kemunculan, akan tetapi membutuhkan usaha yang lebih daripada algoritma playfair biasa.

5.2 Saran

Penelitian ini dapat dikembangkan menjadi penelitian yang lebih baik lagi dengan melakukan saran di bawah ini :

1. Modifikasi matriks kunci dengan melakukan random dinamis agar semakin sulit dipecahkan.
2. Memperluas atau menambah algoritma teknik ekspansi kriptografi, sehingga membentuk ciphertext yang semakin panjang.
3. Menghilangkan karakter “X” dan “Z” pada hasil proses dekripsi.
4. Menggunakan kombinasi proses enkripsi dan dekripsi dengan algoritma lain.
5. Mengimplementasikan algoritma pada pesan berbentuk file.

DAFTAR PUSTAKA

A. Menezes, P. van Oorschot and S. Vanstone, 1996, *Handbook of Applied Cryptography*, CRC Press, Boca Raton.

Ananda Hariati, dkk. 2018. *Kombinasi Algoritma Playfair Cipher dengan Metode Zig-Zag dalam Penyandian Teks*. Medan : STMIK Budi Darma Medan

Fadhillah Azmi dan Rina Anugrahwaty. 2017. *Analisis Matriks 5 x 7 pada Kritografi Playfair Cipher*. Medan : Politeknik Ganesha

Hakim, Hasanul. 2014. *H-Playfair Cipher*. Bandung : Institut Teknologi Bandung

Kromodimoeljo, Sentot. 2009. *Teori & Aplikasi Kriptografi* . Indonesia : SPK IT Consulting

Kurniawan, Y. 2004. *Kriptografi Keamanan Internet dan Jaringan Komunikasi*. Bandung: Informatika.

Munir, R. (2006). *Diktat Kuliah Studi Teknik Informatika*. Bandung: Informatika

Munir, R. (2008). *Kriptografi*. Bandung: Informatika

Nurkifli, E. Haodudin. 2014. *Modifikasi Algoritma Playfair dan Menggabungkan dengan Linear Feedback Shift Register (LFSR)*. Karawang : Universitas Singaperbangsa Karawang

Rio, Nicholas. 2014. *Rubic Cipher Algorithm.* Bandung : Institut Teknologi Bandung

Sadikin, R. 2012. *Kriptografi untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java*. Yogyakarta: ANDI.

Suriski Sitinjak, Yuli Fauziah, and Juwairiah, *Aplikasi Kriptografi File Menggunakan Algoritma Blowfish*, in Seminar Nasional Informatika 2010 (semnasIF 2010), Yogyakarta, 2010, pp. C-79.

Toisutta, Eka Yusrianto. 2017. *Penerapan Kombinasi Playfair Cipher dan Digraph Cipher*. Bandung : Institut Teknologi Bandung

LAMPIRAN

Lampiran Source Code

Fungsi Utama Input Keyword-Plaintext

```
public static void main(String[] args){
    Skrip5 pf = new Skrip5();
  }
     // main run of the program, Playfair method
  private Skrip5(){

    // prompts user for the keyword to use for
encoding & creates tables
    System.out.println("Please input the keyword for
the Playfair cipher.");
    Scanner sc = new Scanner(System.in);
    String keyword = parseString(sc);
    while(keyword.equals(""))
      keyword = parseString(sc);
    System.out.println();
    table = this.cipherTable(keyword);

    // prompts user for message to be encoded
    System.out.println("Please input the message to
```

```
be encoded");
    System.out.println("using the previously given
keyword");
    String input = parseString(sc);
    while(input.equals(""))
      input = parseString(sc);
    System.out.println();

    // encodes and then decodes the encoded message
    String output = cipher(input);
    String decodedOutput = decode(output);

    // output the results to user
    this.printTable(table);
    this.printResults(output,decodedOutput);
  }

  private String parseString(Scanner s){
    String parse = s.nextLine();
    return parse;
  }
```

Fungsi Membentuk Matriks Kunci

```
// creates the cipher table based on some input string
(already parsed)
  private String[][] cipherTable(String key){
    String[][] playfairTable = new String[5][19];
    String keyString = key +
"ABCDEFGHIJKLMNOPQRSTUVWXYZabcdefghijklmnopqrstuvwxyz12
34567890!@#$%^&*() -=_+,./?[]\\{}|;':<>`~\"";
    // fill string array with empty string
    for(int i = 0; i < 5; i++)
      for(int j = 0; j < 19; j++)
        playfairTable[i][j] = "";

    for(int k = 0; k < keyString.length(); k++){
      boolean repeat = false;
      boolean used = false;
      for(int i = 0; i < 5; i++){
        for(int j = 0; j < 19; j++){
          if(playfairTable[i][j].equals("" +
keyString.charAt(k))){
            repeat = true;
          }else if(playfairTable[i][j].equals("") &&
!repeat && !used){
```

```
            playfairTable[i][j] = "" +
keyString.charAt(k);
            used = true;
          }
        }
      }
    }
    return playfairTable;
  }
```

Fungsi Mencetak Matriks Kunci

```
// prints the cipher table out for the user
  private void printTable(String[][] printedTable){
    System.out.println("This is the cipher table from
the given keyword.");
    System.out.println();

    for(int i = 0; i < 5; i++){
      for(int j = 0; j < 19; j++){
        System.out.print(printedTable[i][j]+" ");
      }
      System.out.println();
```

```
    }
    System.out.println();
  }
```

Fungsi Seleksi Bigram

```
 private String cipher(String in){
    length = (int) in.length() / 2 + in.length() % 2;

    // insert x between double-letter digraphs &
redefines "length"
    for(int i = 0; i < (length - 1); i++){
      if(in.charAt(2 * i) == in.charAt(2 * i + 1)){
        in = new StringBuffer(in).insert(2 * i + 1,
'X').toString();
        length = (int) in.length() / 2 + in.length()
% 2;
      }
      System.out.println(length);
      System.out.println(in);
      System.out.println();
    }
     // adds an Z to the last digraph, if necessary
```

```
    String[] digraph = new String[length];
    for(int j = 0; j < length ; j++){
      if(j == (length - 1) && in.length() / 2 ==
(length - 1))
        in = in + "Z";
      digraph[j] = in.charAt(2 * j) +""+ in.charAt(2
* j + 1);
//      System.out.println(digraph[j]);
//      System.out.println();
    }

    // encodes the digraphs and returns the output
    String out = "";
    String[] encDigraphs = new String[length];
    encDigraphs = encodeDigraph(digraph);
    for(int k = 0; k < length; k++)
      out = out + encDigraphs[k];
    return out;
  }
```

Fungsi Enkripsi

```
// encodes the digraph input with the cipher's
specifications
  private String[] encodeDigraph(String di[]){
    String[] enc = new String[length];
    for(int i = 0; i < length; i++){
      char a = di[i].charAt(0);
      char b = di[i].charAt(1);
      int r1 = (int) getPoint(a).getX();
      int r2 = (int) getPoint(b).getX();
      int c1 = (int) getPoint(a).getY();
      int c2 = (int) getPoint(b).getY();

     int r3, r4;
     int c3, c4;
      // case 1: letters in digraph are of same row,
shift columns to right
      if(r1 == r2){
        c1 = (c1 + 1) % 19;
        c2 = (c2 + 1) % 19;
        c3 = (c1 + 1) % 19;
        c4 = (c2 + 1) % 19;
        r4 = r1;
```

```
        r3 = r2;


      // case 2: letters in digraph are of same
column, shift rows down
      }else if(c1 == c2){
        r1 = (r1 + 1) % 5;
        r2 = (r2 + 1) % 5;
        r3 = (r1 + 1) % 5;
        r4 = (r2 + 1) % 5;
        c3 = c1;
        c4 = c2;


      // case 3: letters in digraph form rectangle,
swap first column # with second column #
      }else{
        int temp = c1;
        c1 = c2;
        c2 = temp;
        c3 = c1;
        r3 = (r1 + 1) % 5;
        c4 = c2;
        r4 = (r2 + 4) % 5;
```

```
      }


      //performs the table look-up and puts those
values into the encoded array
      enc[i] = table[r1][c1] + "" + table[r3][c3]+ ""
+ table[r2][c2]+ "" + table[r4][c4];
      System.out.println(enc[i]);
      System.out.println();
    }
    return enc;
  }
```

Fungsi Dekripsi

```
// decodes the output given from the cipher and
decode methods (opp. of encoding process)
  private String decode(String out){
    String decoded = "";
    for(int i = 0; i < out.length() / 4; i++){
      char a = out.charAt(4*i);
      char b = out.charAt(4*i+2);
      int r1 = (int) getPoint(a).getX();
      int r2 = (int) getPoint(b).getX();
```

```
      int c1 = (int) getPoint(a).getY();
      int c2 = (int) getPoint(b).getY();

      if(r1 == r2){
        c1 = (c1 + 18) % 19;
        c2 = (c2 + 18) % 19;
      }else if(c1 == c2){
        r1 = (r1 + 4) % 5;
        r2 = (r2 + 4) % 5;
      }else{
        int temp = c1;
        c1 = c2;
        c2 = temp;
      }
      decoded = decoded + table[r1][c1] +
table[r2][c2];
      System.out.println(decoded);
      System.out.println();
    }
    return decoded;
  }
```

Fungsi Mendapatkan Posisi Karakter

```
// returns a point containing the row and column of
the letter
  private Point getPoint(char c){
    Point pt = new Point(0,0);
    for(int i = 0; i < 5; i++)
      for(int j = 0; j < 19; j++)
        if(c == table[i][j].charAt(0))
          pt = new Point(i,j);
    System.out.println(pt);
    return pt;
  }
```

Perintah Output Enkripsi-Dekripsi

```
// prints results (encoded and decoded)
  private void printResults(String enc, String dec){
    System.out.println("This is the encoded
message:");
    System.out.println(enc);
    System.out.println();
    System.out.println("This is the decoded
message:");
    System.out.println(dec);
  }
}
```

CURICULUM VITAE

Nama	:	Amiroh Mujahidah
Tempat, Tanggal Lahir	:	Bantul, 21 April 1996
Jenis Kelamin	:	Perempuan
Alamat	:	Jl. Pasopati No.42 Maesan Rt.02 Tamanan Banguntapan Bantul
Agama	:	Islam
Email	:	fathikar.am@gmail.com
No.Hp	:	085799388725

Riwayat Pendidikan :

2002-2008 : SD Qurrota A'yun

2008-2011 : SMPIT Abu Bakar

2011-2014 : SMA Negeri 1 Jetis

2014-2018 : S1 Teknik Informatika
UIN Sunan Kalijaga Yogyakarta