Implementasi Algoritma Playfair Cipher pada Penyandian Data

Sartika Dewi Br. Surbakti
STMIK Budi Darma Medan, JL. Sisingamangaraja Np. 338 Simpang Limun Medan
Email: tickha.chaberbie@gmailcom

Abstrak

Kriptografi adalah ilmu pengetahuan dan seni menjaga message-message agar tetap aman *(secure)*. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Penyandian yang pertama kali dibuat dengan menggunakan algoritma clasic. algoritma ini menumpukan keamanannya pada kerahasian algoritma yang digunakan. Namun algoritma ini tidak efisien saat digunakan untuk berkomunikasi dengan banyak orang karena algoritmanya masih sangat sederhana dan masih sangat mudah untuk dipecahkan, sehingga informasi atau data penting yang ingin dirahasiakan dengan mudah dapat diketehui orang lain atau orang yang tidak bertanggungjawab. Dengan menggunakan papan kunci berbentuk 5x5, dapat mengenkripsi plainteks (data teks asli yang akan dienkripsi) dan mendekripsi cipherteks (data teks yang telah dienkripsi) dengan mengelompokkannya dengan menghilangkan huruf J dari plainteks. Papan kunci dibangkitkan secara acak oleh perangkat lunak sehingga setiap proses penyandian (enkripsi dan dekripsi) dapat menggunakan kunci yang berbeda-beda. Perangkat lunak ini digunakan juga untuk membuktikan kebenaran hasil enkripsi dan dekripsi dari Playfair Cipher dengan papan kunci kubus.

Kata Kunci : Keamanan, Enkripsi, Dekripsi, Algoritma playfair cipher

Abstract

Cryptography is the science and art of keeping messages secure. In cryptography there are two main concepts namely encryption and decryption. Encoding was first made using a classic algorithm. This algorithm builds its security on the confidentiality of the algorithm used. However, this algorithm is inefficient when used to communicate with many people because the algorithm is still very simple and still very easy to solve, so that important information or data that you want to keep secret can be easily discovered by other people or people who are not responsible. By using a 5x5 key board, it can encrypt plaintext (the original text data to be encrypted) and decrypt ciphertext (encrypted text data) by grouping it by removing the letter J from the plaintext. Keyboards are generated randomly by the software so that each encoding (encryption and decryption) process can use different keys. This software is also used to prove the encryption and decryption results from the Playfair Cipher with the cube key board.

Keywords: Security, Encryption, Decryption, Playfair Cipher Algorithm

1. PENDAHULUAN

Pemakaian teknologi komputer sebagai salah satu aplikasi dari teknologi informasi sudah menjadi suatu kebutuhan, karena banyak pekerjaan yang dapat diselesaikan dengan cepat, akurat, dan efisien. Keamanan (*security*) dalam *document* adalah hal yang sangat penting dan tidak dapat diabaikan. Lebih-lebih jika *document* yang dikelola bersifat penting dan rahasia. Tentunya pemilik data tidak ingin *document* yang mereka miliki diketahui atau bahkan diubah oleh orang lain yang tidak berhak[1].

Oleh karena itu, dikembangkanlah kriptografi, yaitu ilmu dan seni untuk menjaga keamanan *document*. Kriptografi merupakan salah satu metode pengamanan data yang dapat digunakan untuk menjaga kerahasiaan data, keaslian data, serta keaslian pengiriman. Metode ini bertujuan agar informasi yang bersifat rahasia yang dikirim melalui telekomunikasi umum tidak dapat diketahui atau dimanfaatkan oleh orang yang tidak berkepentingan atau yang tidak berhak[2], [3].

Algoritma *Playfair cipher* adalah salah satu bagian dari kriptografi klasik yaitu salah satu algoritma kunci simetri yang merupakan metode *polygram cipher*. Algoritma *Playfair cipher* menggunakan papan kunci yang berbentuk bujur sangkar dalam melakukan penyandian. Papan kunci ini berukuran 5X5, dimana setiap bagian papan kunci mewakili huruf-huruf dalam alfabet (abjad) dengan menghilangkan huruf j dari abjad setiap elemen bujursangkar berisi huruf yang berbeda satu sama lain[4].

2. LANDASAN TEORI

2.1 Defenisi Kriftografi

Kata kriptografi berasal dari bahasa Yunani, "*kryptós*" yang berarti tersembunyi dan "*gráphein*" yang berarti tulisan. Sehingga kata kriptografi dapat diartikan berupa frase "tulisan tersembunyi". Dalam kamus bahasa Inggris Oxford diberikan pengertian kriptografi yaitu "Sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan mengguanakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dapat dipahami oleh pihak-pihak yang memproses kunci [5]. Secara historis ada empat kelompok yang berkontribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (lovers) [6].

2.2 Algoritma Kriptografi

Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atsa pesan tersebut. Algoritma kriptografi terdiri dari tiga fungsi dasar[7]:

1. Enkripsi merupakan hal yang sangat penting dalam kriptografi, merupakan pengamanan data yang dikirim agar terjadi kerahasiaannya. Pesan asli disebut *plaintext*, yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan sebagai cipher atau kode dengan menggunakan algoritma yang untuk mengkodekan data yang kita inginkan.
2. Depenelitian merupakan kebalikan dari proses enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya (teks asli), disebut dengan depenelitian pesan. Algoritma yang digunakan untuk depenelitian tentu berbeda dengan algoritma yang digunakan untuk enkripsi.
3. Kunci adalah yang dipakai untuk melakukan enkripsi dan depenelitian. Kunci terbagi menjadi dua bagian, kunci rahasia (*private key*) dan kunci umum (*public key*).

2.3 Algoritma Playfair Cipher

Playfair Cipher merupakan salah satu algoritma kriptografi klasik yang ditemukan oleh Sir Charles Wheatstone akan tetapi dipromosikan oleh Baron Lyon Playfair pada tahun 1854. Algoritma kriptografi ini mengenkripsi pasangan huruf, bukan huruf tunggal seperti pada algoritma kriptografi klasik lainnya. Tujuan utamanya adalah untuk mempersulit analisis frekuensi dengan menyetarakan jumlah frekuensi kemunculan huruf-huruf di dalam *ciphertext* [8].

Kunci di dalam algoritma ini selalu memiliki panjang sebanyak 25 karakter yang disusun menjadi tabel acuan berukuran 5 x 5. Kunci ini mengandung seluruh huruf di dalam

alphabet kecuali huruf "j" yang dileburkan dengan huruf "i". Untuk mempermudah pembuatan kunci, pertama-tama tentukan kata yang akan menjadi kunci. Kata tersebut lalu dihilangkan seluruh huruf "j" yg terkandung di dalamnya. Kemudian kata tersebut di konkatenasi dengan teks "abcdefghiklmnopqrstuvwxyz" dan pada akhirnya dari hasil yang diperoleh akan dihilangkan seluruh kemunculan huruf yang berulang.[4]

Tabel 1. Contoh kunci

S	A	R	T	I
K	B	C	D	E
F	G	H	L	M
N	O	P	Q	U
V	W	X	Y	Z

3. HASIL DAN PEMBAHASAN

3.1 Analisa Dan Logika Metode

Algoritma playfair cipher adalah salah satu Classic Cipher (Sandi Klasik) yang menggunakan tehnik manual simetrik enkripsi dan merupakan salah satu sandi substitusi berpasangan (digraf) pertama di Dunia. Algoritma playfair cipher menggunakan matriks 5 x 5 dengan masukan yang terdiri dari 25 karakter dan membuang J yang ada didalam alfatbet.

Jumlah jumlah kemungkinan kunci pada sandi playfair adalah 25!=15.511.210.043.330.985.984.000.000.

A. Proses Enkripsi

Enkripsi merupakan sebuah proses dimana data teks asli diubah menjadi data teks rahasia. Sebelum melakukan enkripsi, pesan yang akan dienkripsi (*plainteks*) diatur terlebih dahulu sebagai berikut:

1. Semua spasi dan karakter yang bukan alfabet harus dihilangkan dari plainteks.
2. Jika ada huruf J pada palinteks maka ganti huruf tersebut dengan huruf I.
3. Pesan yang akan dienkripsi ditulis dalam pasangan huruf (*digraf*). Jika ada huruf yang sama dalam pasangan huruf, maka sisipkan huruf X atau Z di tengahnya. Huruf yang disisipkan sebaiknya huruf X karena sangat kecil kemungkinan terdapat huruf X yang sama dalam *digraf*, tidak seperti huruf Z, contohnya dalam kata FUZZY.
4. Jika jumlah huruf pada plainteks adalah ganjil maka pilih sebuah huruf tambahan yang dipilih oleh orang yang mengenkripsi dan tambahkan di akhir plainteks. Huruf tambahan dapat dipilih sembarang misalnya huruf Z atau X.
5. Kunci dimasukkan dalam tabel ukuran 5 x 5 dengan aturan tidak boleh ada huruf yang berulang.

Contoh:

KAMI MAHASISWA BUDIDARMA

1. KAMIMAHASISWABUDIDARMA
2. KAMIMAHASISWABUDIDARMA
3. KA MI MA HA SI SW AB UD IA RM A
4. KA MI MA HA SI SW AB UD IA RM AZ
5. SARTIK

Penyelesaian :
Plainteks :KAMI MAHASISWA BUDIDARMA

= KAMIMAHASISWABUDIDARMA
Plainteks yang sudah diatur : KA MI MA HA SI SW AB UD ID AR MA
Kunci : SARTIKA
Menjadi : SARTIK
Diperluas menjadi: SARTIKBCDEFGHLMNOPQUVWXYZ

S	A	R	T	I
K	B	C	D	E
F	G	H	L	M
N	O	P	Q	U
V	W	X	Y	Z

Proses enkripsi untuk setiap *digraf* adalah sebagai berikut:

1. Jika kedua huruf tidak terletak pada baris dan kolom yang sama, maka huruf pertama menjadi huruf yang sebaris dengan huruf pertama dan sekolom dengan huruf kedua. Huruf kedua menjadi huruf yang sebaris dengan huruf kedua dan yang sekolom dengan huruf pertama.
2. Jika kedua huruf terletak pada baris yang sama maka huruf pertama menjadi huruf setelahnya dalam baris yang sama, demikianjuga dengan huruf kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua.
3. Jika kedua huruf terletak pada kolom yang sama maka huruf pertama menjadi huruf setelahnya dalam kolom yang sama, demikian juga dengan huruf kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi huruf pertama dan kedua, pergeserannya ke arah huruf kedua.

HASIL:
Maka dari percobaan diatas dapat diperoleh hasil enkripsi sebagai berikut :
Plainteks : KA MI MA HA SI SW AB UD ID AR MA
Cipherteks : BS EI GI GR AS VA BG QE TE RT GI

B. Proses Dekripsi

Proses dekripsi sangat mirip dengan proses enkripsi dan lebih mudah dilakukan karena proses dekripsinya adalah kebalikan dari proses enkripsi.
Dimana:
Plainteks : BSEIGIGRASVABGQETERTGI
Plainteks yang sudah diatur: BS EI GI GR AS VA BG QE TE RT GI
Kunci : SARTIKA
Menjadi : SARTIK
Diperluas menjadi: SARTIKBCDEFGHLMNOPQUVWXYZ
HASIL:
Maka dari percobaan diatas dapat diperoleh hasil dekkripsi sebagai berikut :
Plainteks : BS EI GI GR AS VA BG QE TE RT GI
Cipherteks : KA MI MA HA SI SW AB UD ID AR MA

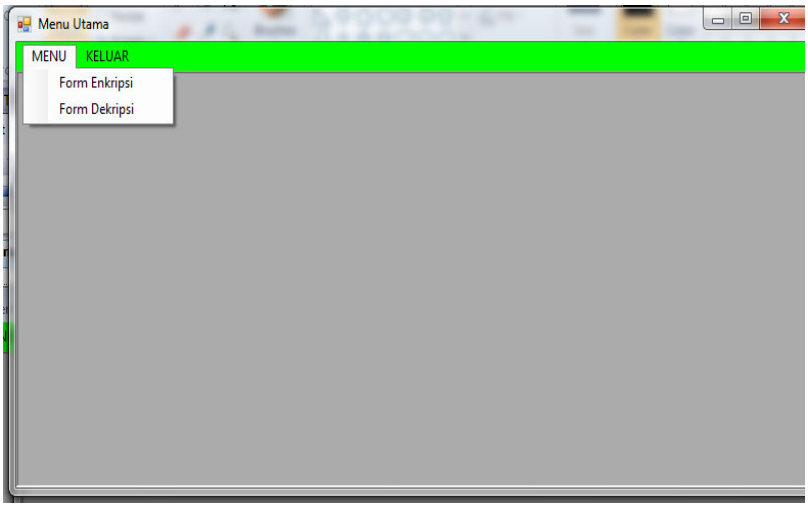
4. ALGORITMA DAN IMPLEMENTASI

1.1 Algoritma playfair cipher

Deklarasi Variabel :
Depenelitian
Input P ⟵ Plainteks
K ⟵ Kunci
Hitung ⟵ Hitung Proses
Output HE ⟵ Hasil enkripsi
HD ⟵ Hasil Dekripsi
Proses :
P = data yang dienkripsi
K = kunci
Hitung = ambil dua plainteks
For i = I to P = jumlah karakter
Hitung = P ke – i
Jika P ke- i = tidak terletak pada kolom yang sama, maka
HE = huruf sebaris dan sekolom
Jika tidak P ke- i = kedua hurup terletak pada baris yang sama, maka
HE = huruf setelah huruf P ke- i
Jika tidak P ke- I =kedua hurup terletak pada kolom yang sama maka
HE = kuruf setelah P ke- i
Selesai
End for
P = HE
K = Kunci
Hitung = ambil
For I = I to HE
Jika HE ke-I = tidak terletak pada kolom yag sama, maka
HD = huruf sebaris dan sekolom
Jika HE ke- I = kedua hurup terletak pada kolom yang sama, maka
HD = huruf setelah huruf HE ke-i
Jika HE ke- I = kedua huruf terletak pada kolom yang sama, maka
HD = huruf pertama setalah huruf HE ke-i
Selesai
End for
Selasai

Setelah mendapatkan hasil tampilan *form* interface, selanjutnya dilakukan pengujian terhadap penerapan algoritma playfair cipher melalui interface yang sudah dirancang. Tahap-tahap yang dilakukan dalam pengujian adalah:

1. Tampilan Menu Utama
   Dalam tampilan pengujian menu utama ini akan disajikan beberapa menu pilihan yang dapat diakses oleh penguna. Menu pilihan yang disediakan adalah Menu Utama, Menu Enkripsi, Menu Dekripsi, Menu Keluar. Berikut ini adalah tampilan menu Utama:



Gambar 1 Tampilan Pengujian Menu Utama

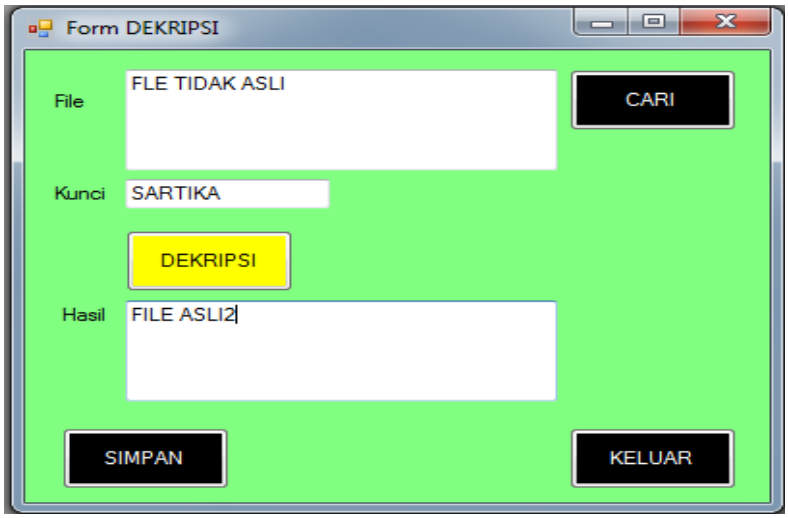
2. Tampilan Menu Enkripsi

Pada pengujian *form* enkripsi dapat dijelaskan bahwa proses penyandian yang telah dipilh berhasil dilakukan, dimana data yag ada pada *textbox* yaitu KAMI MAHASISWA BUDIDARMA dirubah dalam alfabet yang berbeda atau tidak sesuai dengan data pada pesan dokumen aslinya. Berikut ini adalah tampilan menu enkripsi:

Gambar 2 Tampilan Pengujian Menu Enkripsi

3. Menu Deskripsi

Proses pengembalian data pesan dokumen (enkripsi) kebalikan dari pada *form* Enkripsi dimana pesan yang ada pada *textbox* berhasil dilakukan perubahan kebentuk aslinya. Berikut ini adalah tampilan menu dekripsi:



Gambar 3 Hasil Pengujian *Form* Dekripsi

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan pembahasan yang sebelumnya, maka dapat diambil beberapa kesimpulan sebagai berikut:

1. Algoritma playfair cipher adalah algoritma yang menggunakan tehnik manual simetrik enkripsi dan merupakan salah satu sandi substitusi berpasangan (digraf) pertama di Dunia. Algoritma playfair cipher menggunakan matriks 5 x 5 (dengan masukan yang terdiri dari 25 karakter dan membuang J yang ada di dalam alfatbet). Dengan melakukan proses penyandian agar membatasi orang yang tidak berhak atas informasi atau data yang dimiliki oleh si pengirim untuk dibaca karena pesan sudah dienkripsi dan dapat menjaga kerahasiaan pesan atau informasi data-data yang ada dalam sebuah komputer.
2. Perancangan aplikasi penyandian data dengan *Visual Basic.Net 2008*. Adalah salah aplikasi yang sangat membantu dalam melakukan penyandian data, disamping itu dapat membantu menjelaskan materi yang ada.

5.2 Saran

Berikut merupakan saran-saran untuk pengembangan lebih lanjut terhadap Implementasi Algoritma Playfair Cipher Pada Penyandian Data:

1. Dalam pnyandian Algoritma Playfair Cipher hanya dapat menyandikan alfabet saja dan menghilangkan huruf J yang, maka dari itu penulis berharap agar dapat menggunakan algoritma yang lain yang dapat menyandikan selain alfabet.
2. Aplikasi dalam penyandian data dokumen tidak hanya dibangun dengan menggunakan *Visual Basic.Net 2008,* namun dapat menggunakan aplikasi yang lain.

DAFTAR PUSTAKA

[1] R. Munir, "Kriptografi," *Inform. Bandung*, 2006.

[2] H. D. M. H. Hutahaean, "Aplikasi Pembelajaran Kriptograpi berbasis Mobile menggunakan Computer Assisted Instruction," vol. 4, no. 1, pp. 2–5, 2019.

[3] D. Ariyus, "Kriptografi keamanan data dan komunikasi," *Yogyakarta Graha Ilmu*, 2006.

[4] A. M. Mhd. Zulfansyuri Siambaton, "Modifikasi Algoritma Playfair Cipher Dengan Pengurutan Array Pada Matriks," *J. Ilmu Komput. dan Inform.*, vol. 02, no. April, pp. 66–71, 2018.

[5] Www.ssh.com, "Cryptography for Practitioners," 2019. [Online]. Available: https://www.ssh.com/cryptography. [Accessed: 14-Dec-2019].

[6] T. Limbong *et al.*, "The implementation of computer based instruction model on Gost Algorithm Cryptography Learning," in *IOP Conference Series: Materials Science and Engineering*, 2018, vol. 420, no. 1, p. 12094.

[7] A. M. Hasibuan, "Rancang Bangun Aplikasi Keamanan Data Menggunakan Metode AES Pada Smartphone," *MEANS (Media Inf. Anal. dan Sist.*, vol. 2, no. 1, pp. 29–35, Jun. 2017.

[8] D. D. Santoso and P. Tarigan, "Penerapan Algoritma Playfair Cipher sebagai Penyandian Kunci Dalam Pengamanan File Teks dengan Algoritma Rijndael," *Pelita Inform. Budi Darma*, vol. 17, pp. 59–64, 2018.