Pengembangan Kunci Playfair Cipher dengan Interpretasi Suara

Fitrandi Ramadhan - 13508065
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
if18065@students.if.itb.ac.id

***Abstract*— Playfair cipher menggunakan matriks sebagai kunci pada implementasi enkripsinya. Kunci dibangkitkan dengan menggunakan sebuah keyword yang akan disampaikan kepada penerima pesan. Sejatinya kunci ini dapat pula dibangkitkan menggunakan banyak media lain seperti citra, suara dan lain lain.**

Penggunaan matriks yang berulang untuk setiap ciphertext akan mempermudah kriptanalis untuk menebak pasangan huruf yang digunakan. Data pada masa sekarang telah memiliki ukuran file yang cukup besar dan dari sana dapat dimanfaatkan kelebihan ini untuk membangkitkan sebuah kunci yang tidak berulang dan mengakibatkan pembangkitan matriks playfair cipher yang lebih banyak dan dapat digunakan untuk sekuens plainteks yang lebih panjang. Pada makalah ini akan dianalisis penggunaan playfair cipher dengan menggunakan matriks yang tidak berulang dari hasil generasi interpretasi suara.

***Index Terms*—About Playfair Cipher, Wave, Matriks, Kunci, Kriptografi**

I. PENDAHULUAN

Pengembangan kriptografi selalu bertambah cepat seiring dengan perkembangan teknologi. Hal ini diakibatkan oleh pesatnya perkembangan pemrosesan, penyimpanan dan tentu saja pertukaran data. Pertukaran data inilah yang menjadi poin utama kebutuhan kriptografi di dunia.

Tidak semua informasi dapat dikonsumsi oleh khalayak banyak. Seringkali manusia ingin setiap informasi-informasinya yang ditujukan kepada orang lain ingin mereka sembunyikan, maka dari itu berkembanglah berbagai teknik kriptografi. Pada masa sekarang data atau informasi lebih banyak disimpan dan ditransmisikan dengan sebuah komputer. Data pada komputer ini tentunya tersimpan dalam deretan bit-bit atau representasi biner. Berbagai algoritma modern pun berkembang untuk menyesuaikan sekaligus meningkatkan performansi dari kriptografi ini. Teknik atau metode kriptografi modern ini sebenarnya adalah implementasi atau modifikasi dari algoritma-algoritma kriptografi klasik. Dan salah satu dari algoritma kriptografi klasik yang telah kita kenal adalah Playfair Cipher yang diciptakan oleh Charles Wheatstone dan kemudian dipopulerkan oleh Lord Playfair dan namanya pun diabadikan sebagai nama dari algoritma ini.

Plafair Cipher memanfaatkan sebuah matriks yang terdiri dari 25 huruf latin. Matriks ini dibangkitkan dari urutan huruf-huruf pada sebuah kata kunci atau password. Pada Playfair Cipher dapat dikatakan bahwa jika key telah mencapai suatu treshold komposisi dari huruf tertentu Matriks kunci yang dibangkitkan tidak akan bertambah ataupun berubah lagi. Matriks inipun kemudian digunakan untuk mengenkripsi bi-gram dari seluruh Plainteks. Hal ini menjadi suatu kelemahan dimana berbagai metode kriptanalisis khususnya analisis frekuensi dapat memecahkan metode enkripsi ini dengan cukup mudah apabila kriptanalis mendapatkan tebel frekuensi yang tepat.

Dengan kemampuan komputer modern manusia pun mulai dapat melakukan interpretasi atas berbagai tipe data. Salah satu yang cukup terkenal adalah interpretasi suara. Interpretasi atas suara ini kemudian dapat dilakukan untuk banyak hal. Salah satunya adalah pembangkitan kunci yang mana kunci ini dapat digunakan sebagai kunci enkripsi dan dekripsi. Kunci pada playfair cipher pun dapat pula dibangkitkan dengan meggunakan informasi-informasi yang tersimpan pada suara tersebut. Pada hal ini eksistensi suara dapat digunakan ada Wave sound file.

II. LANDASAN TEORI

A. Kriptografi

Kriptografi diduga telah digunakan oleh manusia sebagai metode perahasiaan pesan sejak 4000 tahun yang lalu dimana bangsa mesir yang menuliskan huruf hieroglyph pada beberapa temuan menggunakan hieroglyph yang tidak standard. Hal ini dapat diinterpretasikan sebagai sebuah pesan yang ingin dirahasiakan dari orang banyak. Yunani pada 400 tahun sebelum masehi pun telah secara eksplisit memperkenalkan sebuah metode kriptografi. Hal ini dilakukan dengan sebuah alat yang dinamakan scytale. Sebuah kayu berbentuk silinder yang mana dapat digunakan untuk melilitkan kertas yang panjang. Pada lilitan ini kemudian dituliskan sebuah pesan. Apabila kertas ini dilepaskan dari batang kayu maka yang akan nampak hanyalah deretan huruf-huruf acak secara

menurun. Pesan dapat dibaca kembali dengan kembali melilitkan kertas pada batang kayu yang memiliki diameter yang sama. Kemudian berkembanglah berbagai algoritma kriptografi klasik lainya Vigenere Cipher yang dipopulerkan oleh Blaise de Vigenere. Vigenere Cipher ini adalah Algoritma stream cipher pertama. Algoritma ini memanfaatkan perhitungan matematika sederhana dengan melakukan subtitusi pada Plainteks. Plainteks di subtitusikan dengan huruf yang merupakan hasil modulus dari Plainteks tersebut dan huruf dari kunci. Kemudian lahir pula sophisticated Block Cipher pertama yaitu Playfair Cipher. Playfair Cipher menggunakan kunci untuk membangkitkan sebuah matriks. Matriks inilah yang kemudian digunakan untuk mengenkripsi Plainteks menjadi Cipherteks. Sebuah algoritma kriptografi klasik yang paling sulit untuk dipecahkan yaitu One-time pad mungkin adalah algoritma kriptografi paling aman sepanjang masa. One-time pad menggunakan sebuah memo yang digunakan sebagai kunci untuk melakukan

enkripi dan dekripsi. Panjang karakter yang dimiliki oleh kunci haruslah lebih besar atau sama dengan Plainteks untuk sebuah algoritma dikatakan sebagai sebuah one-time pad. Sesungguhnya one-time pad hanyalah pengembangan sederhana dari vigenere cipher. Pengirim pesan perlu membuat sebuah kunci yang memiliki panjang yang sama dengan plainteks dan setiap huruf digunakan untuk melakukan enkripsi dengan algoritm vigenere cipher. Dengan kunci yang tidak memiliki suatu pola khusus ini algoritma ini menjadi hampir mustahil untuk dipecahkan. Akan tetapi karena membutuhkan panjang kunci yang relatif tidak efisien algoritma ini sulit untuk diimplementasikan. Pada perang dunia ke-2, Pemerintah Nazi jerman membuat mesin enkripsi yang dinamakan Enigma. Enigma Cipher sendiri menggunakan rotasi dari rangkaian alphabet yang terdapat pada sisi gigi-gigi tersebut untuk mengenkripsi pesan-pesanya.

Pada masa kini dimana kriptografi berkembang seiring dengan perkembangan komputer, kriptografi terbagi menjadi dua. Yang pertama adalah Symmetric Key Algorithm dimana masih sama dengan kebanyakan algoritma kriptografi klasik. Pengirim pesan serta penerima pesan memiliki kunci enkripsi dan kunci dekripsi yang sama. Seluruh algoritma kriptografi klasik merupakan symmetric key algorithm. Yang kedua adalah Asymmetric Key Algorihm, contoh paling sederhana dan paling primitif mungkin adalah pengiriman pos. Pengirim pesan perlu tahu alamat dari penerima pesan. Banyak hal yang dapat mengganggu keamanan dan keselamatan dari pos ini. Penulisan alamat yang salah, pencurian pesan oleh petugas pos, pemalsuan pesan yang dikirimkan oleh orang lain dan lain lain. Hal yang sama dapat terjadi pada Asymmeric Key Cryptography. Dimana dapat saja sebuah pesan dicuri oleh seseorang kemudian orang tersebut mengirimkan public key yang salah kepada penerima asli. Kemudian ditambahkan pula adanya private key. Pada contoh pos tadi private key ini dapat dianalogkan sebagai tanda tangan dari pengirim dimana penerima dapat memeriksa tanda tangan yang dibubuhkan pengirim sehingga dapat diasumsikan tidak dimungkinkan adanya pemalsuan tanda tangan.

B. Playfair Cipher

Dokumen pertama yang tercatat menjelaskan mengenai Playfair Cipher ditulis oleh Charles Wheatstone. Playfair Cipher kemudian dipopulerkan lebih lanjut oleh Lord Playfair yang kemudian namanya diabadikan sebagai nama dari algoritma kriptografi ini. Hal ini dikarenakan ketika pertama kali diajukan pada Kantor Luar Negeri Inggris algoritma ini ditolak karena dianggap sulit untuk dimengerti. Kemudian wheatstone mengajarkan algoritma ini kepada empat pelajar sekolah dimana tiga dari empat pelajar tersebut mengerti penggunaan dari Algoritma itu. Playfair Cipher kemudian digunakan dalam perang dunia pertama sebagai metode perahasiaan pesan yang sifatnya tidak kritikal. Tujuanya agar pada saat kriptanalis musuh berhasil memecahkan pesan yang disampaikan pesan tersebut sudah tak lagi valid.

Playfair Cipher merupakan algoritma kriografi pertama yang tidak menggunakan subtitusi huruf-huruf tunggal pada implementasinya. Algoritma ini menggunakan pasangan huruf dalam implementasinya. Pertama sebuah matriks dibangkitkan dengan menggunakan private key yang dimiliki. Playfair Cipher menggunakan matriks 5x5 yang mana isinya adalah urutan huruf-huruf tak berulang atau unik dari kunci. Berikut proses enkripsi dengan menggunakan Playfair Cipher.

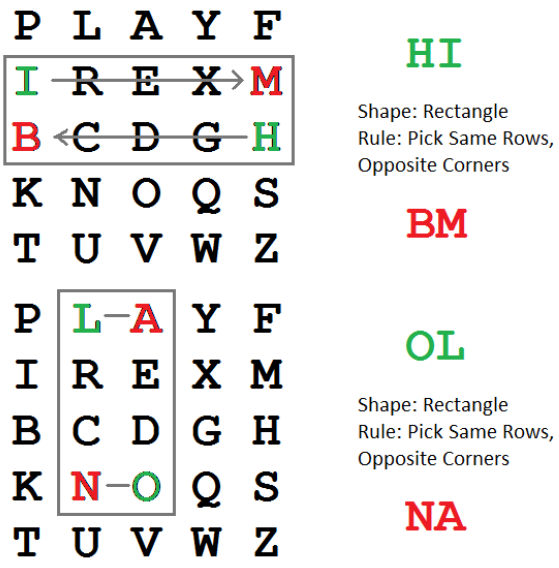

Fig II.B.1

1. Masukkan huruf-huruf pada kunci ke setiap elemen matriks secara unik. Jika terdapat elemen

yang berulang maka huruf tersebut tidak dimasukkan kembali. Kemudian isikan sisa dari alphabet yang tidak terdapat pada kunci secara berurutan ke dalam matriks. Dikarenakan elemen matriks yang hanya berjumlh 25 maka diperlukan pembuangan pada satu buah alphabet. Alphabet yang dibuang biasanya adalah 'J'.

2. Persiapkan Plainteks dengan membuang setiap huruf 'J' dengan menggantinya dengan huruf ‘I’.

3. Bagi Plainteks kepada bigram-bigram atau pasangan huruf. Misalkan pada kata PLAINTEKS pasangan-pasangan hurufnya menjadi PL AI NT EK S.

4. Pada pasangan huruf yang merupakan huruf yang sama seperti pasangan SS pada kata PASSWORD. ganti huruf yang kedua menjadi huruf 'X' atau 'Q'. Hal ini tergantung kesepakatan. Akan tetapi penggunaan huruf 'X' sebagai subitusi lebih umum digunakan.

5. Pada akhir dari pasangan huruf yang ganjil, seperti pada contoh kata PLAINTEKS diatas tambahkan huruf 'X' atau 'Q' di akhir plainteks. Penggunaan huruf ini sama seperti pada langkah 4 dimana huruf yang digunakan merupakan konvensi.

Dua langkah terakhir dilakukan dengan asumsi alphabet 'X' dan 'Q' adalah alphabet yang paling jarang digunakan. Jika langkah persiapan tersebut telah dilakukan maka proses enkripsi sudah dapat dimulai. Aturan dari subtitusi adalah sebagai berikut.

1. Jika kedua huruf pada pasangan huruf terdapat pada baris yang sama, subtitusikan alphabet dengan alphabet yang berada tepat sebelah kanan dari alphabet yang akan dienkripsi. Apabila alphabet berada pada tepi kanan matriks maka tambahkan 1 kolom tambahan pada sebelah kanan yang merupakan kolom paling kiri dari matriks tersebut.

2. Jika kedua alpabet berada pada kolom yang sama, subtitusikan alphabet dengan alphabet yang berada tepat berada di bawah alphabet tersebut. Tambahkan baris pertama di bawah baris terakhir apabila alphabet plainteks terdapat pada baris paling bawah matriks.

3. Jika kedua alphabet berada pada baris dan kolom yang berbeda maka subtitusikan alphabet dengan alphabet yang berada pada baris alphabet tersebut dan berada pada kolom pasanganya.

Setelah semua proses dilakukan pada seluruh plainteks akan didapatkan cipherteks yang telah terenkripsi sesuai dengan aturan-aturan tersebut. Proses dekripsi dari playfair cipher dilakukan dengan menggunakan matriks yang dibangkitkan dengan kunci yang sama. Dekripsi ini dilakukan dengan membalik alphabet-alphabet yang digunakan. Pada aturan pertama proses dekripsi dilakukan dengan mengambil alphabet yang berada tepat dikanan alphabet asal, maka pada dekripsi diambil alphabet dengan posisi tepat di sebelah kiri alphabet dari cipherteks. proses dari bawah ke atas juga dilakukan untuk alphabet pada kondisi 2. Dan pada kondisi 3 didekripsi dengan pembalikan baris kolom, menjadi kolom baris. Huruf-huruf 'X' atay 'Q' yang dihasilkan dari proses dekripsi dapat diartikan secara manual karena alphabet-alphabet tersebut diasumsikan sangat sedikit penggunaanya.

C. Wave Sound Format

Wave Sound Format merupakan sebuah eksistensi file audio standard Microsoft dan IMB. Wave merupakan format audio yang menyimpan data dengan memotong audio menjadi 3 bagian terlebih dahulu. Bagian pertama merupakan RIFF chunk. Dimana disimpan Chunk ID, Chunk Size, dan Format. Kemudian yang kedua adalah fmt sub-chunk dimana disimpan informasi mengenai jumlah channel pada file tersebut, Sample Rate, Bit Depth, dan lain lain. Kemudian yang ketiga adalah data chunk. dimana disini disimpan Subchunk2Size yang adalah ukuran yang terdapat pada data dengan satuan byte.

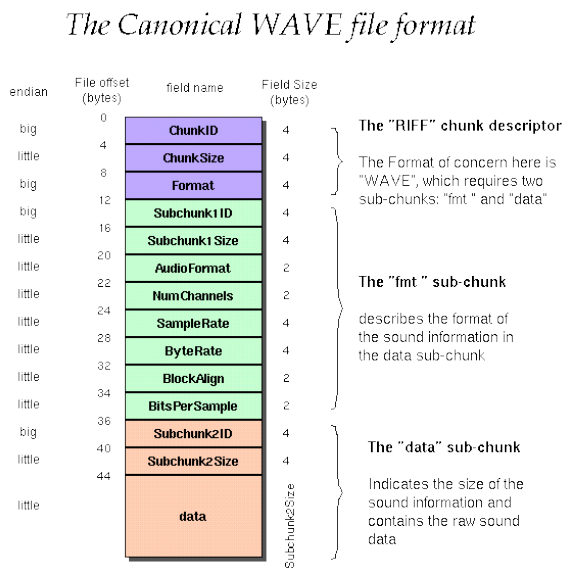

Fig II.C.1

Data yang disimpan pada wave sound format ini dapat diekstraksi yang mana kemudian binary dari data tersebut dapat dimanfaatkan untuk berbagai kebutuhan, salah satunya yang dibahas pada makalah ini yaitu private key kriptografi.

```
private :
        //DATAMEMBER
        string Plainteks;
        string Cipherteks;
        Wave WaveKey;
        char* PlainBigram;
        char* CipherBigram;
        Matrix* MatrixKey;
```

III. ANALISIS DAN IMPLEMENTASI

Playfair Cipher menggunakan satu buah matriks yang dibangkitkan dari alphabet yang terdapat pada kunci secara berurutan. Pada data yang sangat besar bukanlah sesuatu yang aneh apabila sebuah plainteks mengandung pasangan huruf yang sama lebih dari satu kali. Pasangan huruf ini tentunya karena manggunakan matriks yang sama akan menghasilkan pasangan huruf cipherteks yang sama pula. Pasangan huruf yang sama ini dapat menjadi titik lemah dari algoritma Playfair Cipher. Kelemahan ini tentunya dapat menjadi lubang yang dapat dimanfaatkan oleh kriptanalis dengan menggunakan tabel frekuensi kemunculan pasangan huruf. Dengan menggunakan Wave sound format yang relatif merupakan suatu format audio yang berukuran besar maka matriks kunci yang dapat dibangkitkan pun relatif banyak. Dengan ukuran ini dapat diambil asumsi pula bahwa panjang matriks yang merupakan kunci dari enkripsi dan dekripsi ini lebih panjang daripada plainteks yang akan diproses. Dengan asumsi ini, maka kemunculan pasangan huruf yang lebih dari satu kali pada cipherteks dapat diminimalisir dengan signifikan. Hal ini disebabkan dengan adanya matriks kunci yang banyak dan berbeda maka sudah tentu pasangan huruf cipheteks yang dihasilkan akan berbeda pula.

Proses minimisasi kemunculan pasangan huruf yang sama ini tidak lepas dari berapa kali setiap matriks yang ada digunakan. Karena banyaknya matriks, relatif dengan panjang plainteks dapat dilakukan proses enkripsi dengan fungsi satu ke satu. dimana setiap pasangan huruf akan dienkripsi dengan satu buah matriks. Apabila hal ini dilakukan dengan matriks yang unik maka dapat dijamin bahwa hasil pemetaan Plainteks akan menghasilkan cipherteks yang berbeda-beda.

Karena setiap matriks yang dibangkitkan merupakan hasil seed dari nilai yang sama dari potongan-potongan Wave Sound Format tersebut, yang mana pada konteks ini potongan dilakukan dengan memotong setiap frame atau nilai sample dari data, Maka setia kali matriks ini dibangkitkan kembali dari awal himpunan matriks yang dihasilkan akan selalu sama.

```
void PlayfairCipher::fetchMatrixKey() {
        for(int i=0;i<DEFAULT_MATRIXKEYSIZE;i++) {
                randomizeMatrix(i);
        }
}

int PlayfairCipher::getSeed(int x) {
        string candidate = "";
        string temp = "";
        do {
                ostringstream buffer;
                buffer << WaveKey.getData(x);
                candidate = buffer.str();
                cout << candidate << endl;
                x++;
                if(WaveKey.getSize()-
1==WaveKey.getSize()) {
                        x = 0;
                }
        } while(candidate.length()<1 || candidate=="nan" ||
candidate=="0");
        int i = 0;
        int j = 0;
        while(i<3) {
                if(candidate.at(j)!='e' && candidate.at(j)!='.'
&& candidate.at(j)!='-' && candidate.at(j)!='+') {
                        temp += candidate.at(j);
                        i++;
                        // cout << "ngulang-ngulang mulu
ke-" << i << endl;
                }
                j++;
        }
        // cout << "aloha dikit lg" << endl;
        const char* ctemp = temp.c_str();
        // cout << temp << endl;
        return atoi(ctemp);
}


void PlayfairCipher::randomizeMatrix(int i) {
        // cout << "matrix ke-" << i << endl;
        srand(getSeed(i));
        for(int j=0;j<getMatrixKey(i).getHeight();j++) {
                for(int
k=0;k<getMatrixKey(i).getWidth();k++) {
                        char c = '0';
                        c = (char)((rand()%26) + 97);
                        while(isLetterOnMatrix(i,c)) {
                                c++;
                                if(c>122) {
                                        c = 'a';
                                }
                        }
                        MatrixKey[i].setM(j,k,c);
                }
        }
}

bool PlayfairCipher::isLetterOnMatrix(int i, char c) {
        for(int j=0;j<getMatrixKey(i).getHeight();j++) {
                for(int
k=0;k<getMatrixKey(i).getWidth();k++) {
                        if(MatrixKey[i].getM(j,k)==c)
return true;
                }
        }
        return false;
}
```

Untuk proses pembangkitan matriks ini sendiri dapat dilakukan dengan banyak cara. Data dari Wave Sound Format yang digunakan pada implementasi ini yaitu adalah data nyata yang tersimpan. Data ini diekstraksi dan kemudian nilai-nilai yang terdapat pada data tersebut dimanfaatkan untuk pembangkitan. Dalam hal ini untuk mempermudah proses implementasi serta secara tidak langsung menyulitkan kriptanalis dalam menebak matriks yang dibangkitkan, setelah data diekstraksi dari file dilakukan operasi untuk mengcasting data tersebut kedalam sebuah float. Floating point tersebut kemudian disederhanakan dengan casting lebih lanjut kedalam string dan diambil karakter-karakter anggotanya yang adalah digit numerik dan di casting kembali menjadi sebuah integer. Integer inilah yang kemudian menjadi seed pada proses selanjutnya. Pada proses pembangkitan selanjutnya digunakan randomizer dengan seed yang diberikan pada proses sebelumnya. Sifat dari pembangkitan psudo-random generator yang akan membangkitkan urutan angka yang sama kemudian dimanfaatkan untuk membangkitkan matriks dengan urutan huruf-huruf berdasarkan pseudo-random number tersebut dengan operasi modulus. Matriks yang dihidupkan pun dijaga agar pada setiap matriks setiap huruf hasil casting pseudo-random tersebut tidak akan berulang. Proses randomasi dilakukan dengan iterasi hanya sebanyak 25 kali sesuai dengan jumlah elemen matriks dengan aturan-aturan tertentu agar proses tidak terlalu lama.

Proses enkripsi sendiri dilakukan sesuai dengan algritma Playfair Cipher klasik hanya saja dengan matriks-matriks yang berbeda ini sesuai dengan jumlah pengulangan pemakaian matriks-matriks tersebut. Pada implementasi ini terdapat beberapa pembatasan dimana floating point yang diekstrak dari data Wave Sound Format tidak selalu sophisticated untuk diproses. Maka pada pelaksanaanya dipilih pula floating point yang valid. Pada implementasi terdapat beberapa floating point yang mana bernilai nan (not a number). Bilangan-bilangan ini di lewati agar proses perhitungan lebih lanjut berjalan dengan baik.

Untuk memudahkan proses implementasi dan pengujian serta dikarenakan teks yang digunakan untuk uji coba matriks adalah Plainteks yang panjangnya tidak terlalu besar maka matriks digunakan untuk setiap 20 pasangan huruf. Dengan implementasi ini akan didapatkan matriks yang dapat mengenkripsi 40 huruf. Dengan dasar ini maka dapat dikatakan untuk setiap sample atau frame dari Wave Sound Format dapat mengenkripsi 40 huruf. Maka apabila sebuah Wave Sound Format memiliki 1000 frame maka ia dapat mengenkripsi 40000 huruf. Standard frame per detik yang biasa diadopsi adalah 11025, 22050, and 44100 KHz. Maka akan dapat dihitung bagaimana sebuah Wave Sound Format dengan durasi 3 menit dapat mengenkripsi data yang sangat besar.

Untuk proses dekripsi kembali dapat diketahui dengan penyataan sebelumnya bahwa pseudo-random number yang dihasilkan akan selalu sama sehingga pembangkitan kembali matriks-matriks tidaklah sulit.

IV. KESIMPULAN

Pembangkitan matriks kunci pada Playfair Cipher merupakan hal yang feasible untuk dilakukan menggunakan komputer modern. Terdapat alasan lebih khusus daripada dilakukan terlebih dahulu operasi Persiapan dalam pembangkitan kunci matriks. Sample yang didapatkan dari setiap frame dari setiap channel pada Wave File Format yang bersebelahan seringkali yang berbeda sangat sedikit nilainya. Untuk itu perlu dilakukan operasi lain untuk mengacak nilai yang terdapat pada setiap frame atau sample yang memiliki perbedaan sangat sedikit dengan frame sebelahnya.

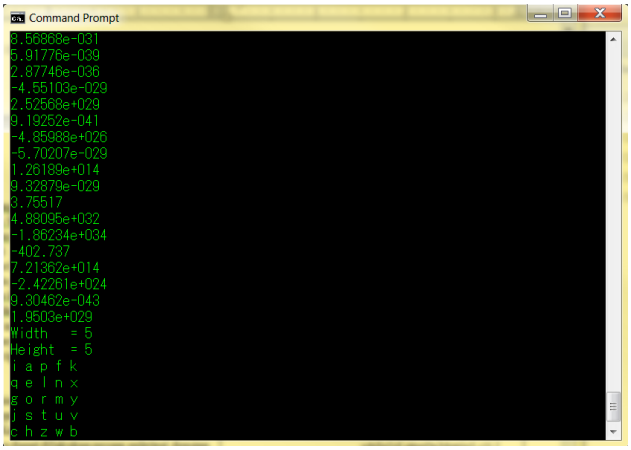

Fig IV.1 Pembangkitan Matriks

Pembangkitan kunci ini sendiri dapat dilakukan dengan berbagai metode yang berbeda. Implementasi yang dilakukan berkenaan dengan paper ini hanya salah satu dari sekian banyak metode pembangkitan kunci sehingga tidak menutup kemungkinan akan ada metode pembangkitan lain yang yang dapat menghasilkan himpunan matriks kunci yang lebih unik dan proses yang lebih efisien.

Keuntungan lebih lanjut dikarenakan kunci ini merupakan file audio dan pembangkitan dapat dilakukan berkali-kali sehingga tidak dibutuhkan kunci lain atau kunci yang biasa digunakan pada penyembunyian informasi pada media (stegnografi).

Matriks yang dibangkitkan dari Wave Sound Format ini relatif sangat banyak. Dengan Sample rate yang sangat besar dapat dibangkitkan pula Himpunan matriks yang memiliki anggota relatif besar. Dari riset ini dengan

sedikit optimasi saja yaitu dengan pembangkitan kunci menggunakan audio file maka dengan pengembangan lebih lanjut, tentunya tidak hanya dengan menggunakan file suara, Playfair Cipher dapat melakukan enkripsi lebih baik lagi.

REFERENCES

[1] Munir, Rinaldi. Pengantar Kriptografi (2013).pptx
[2] Munir, Rinaldi Algoritma Kriptografi Klasik_bag2 (2013).pptx
[3] Anderson, Ross. Security Engineering : A Guide to Building Dependable Distributed Systems
[4] https://ccrma.stanford.edu/courses/422/projects/WaveFormat/ Tanggal akses 16 Maret 2014
[5] M. Bellare, S. Goldwasser and D. Micciancio. Pseudo-Random" Number Generation within Cryptographic Algorithms: the DSS Case.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 19 Maret 2014

Fitrandi Ramadhan 1308065