Modifikasi Playfair Cipher dengan Matrix 6x6 dan Pasangan Kunci

Gabrielle Wicesawati Poerwawinata-13510060[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13510060@std.stei.itb.ac.id

Abstraksi-Makalah ini mengulas modifikasi dari Playfair Cipher. Matriks Playfair Cipher yang sebelumnya berukuran 5x5 akan dimodifikasi menjadi matriks 6x6. Pada matriks 6x6 ini 10 tempat yang kosong pada matriks akan diisikan dengan karakter ASCII yang lain. Penentuan karakterASCII yang akan diisikan akan dijelaskan pada bab selanjutnya. Penambahan karakter ASCII yang lainnya pada matriks diharapkan akan menambah kesulitan penebakan pasangan monoalphabetic antara plaintext dan ciphertext. Metode enkripsi yang akan dijelaskan berikutnya mempunyai suatu cara tambahan yang akan membuat plainteks tersebut lebih sulit untuk ditebak bigram atau trigramnya.

***Index Terms*—Ciphertext, plaintext, playfair cipher, transposisi matrix, kriptografi.**

I. PENDAHULUAN

Kriptografi berasal dari bahasa Greek yang berarti pesan tersembunyi. Kriptografi adalah praktik dan ilmu untuk mengamankan pesan dari pihak ketiga. Kriptografi dibagi menjadi dua jenis yaitu Asymmetric Key Cryptography dan Symmetric Key Cryptography. Pada Symmetric Key Cryptography dibagi menjadi dua jenis yaitu subtitusion cipher dan transposition cipher.

Pada Playfair Cipher ini, metode subtitusi cipher dibuat lebih rumit daripada subtitusi pada Vigenere Cipher. Oleh karena itu Playfair Cipher lebih sulit untuk diterka daripada teknik Vigenere Cipher. Playfair Cipher megenkripsi pasangan huruf bukan huruf tunggal seperti pada cipher klasik lainnya.

Playfair Cipher pada asalnya menggunakan matriks bujursangkar 5x5 dan 26 huruf ditempatkan pada matriks tersebut. Huruf I dan J biasanya ditempatkan dalam satu sel pada matriks tersebut. Pada modifikasi Cipher ini tidak ada huruf yang ditempatkan pada suatu sel pada matriks.

Modifikasi matriks ini juga memungkinkan pasangan huruf yang sama tidak hanya disisipi dengan huruf z, tetapi bisa dengan huruf-huruf atau karakter ASCII yang lainnya. Modifikasi tidak hanya dilakukan pada perubahan struktur matriks Playfair tetapi juga enkrispi dari huruf cipher dengan satu huruf kunci. Lalu selanjutnya dilakukan perubahan dan penambahan pada peletakkan huruf-huruf cipher.

II. PLAYFAIR CIPHER

Playfair Cipher menggunakan matriks 5x5. Kunci ang digunakan untuk proses enkripsi dituliskan pertama. Penulisan kunci ini dapat dituliskan secara berurutan pada kolom atau baris. Sisa dari sel-sel matriks yang lainnya digunakan untuk mengisikan sisa huruf yang lainnya yang belum dituliskan pada matriks tersebut. Misalkan kunci yang dipakai adalah kata "KUNCI" maka matriks playfair akan diisikan dengan susunan huruf seperti tabel

Tabel 1: Penyusunan Karakter pada Matriks Playfair

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

Aturan enkripsi dari pasangan-pasangan huruf plaintext adalah:

1. Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.
2. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti denga huruf di bawahnya.
3. Jika dua huruf tidak pada baris yang sama atau kolom yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini.

Kata yang bisa dijadikan sebagai kunci adalah kata yang tidak mempunyai huruf yang berulang didalamnya. Jika mempunyai sebuah kunci yang mempunyai huruf yang berulang didalamnya maka cukup dituliskan sekali huruf-huruf yang berulang tersebut. Contoh dari permasalahan tersebut adalah sebagai berikut, digunakan kunci "SAYA MAU MAKAN IKAN". Maka kunci tersebut dapat disingkat menjadi *string* "SAYMUKNI".

Jika kita akan mengenkripsi sebuah pesan seperti "MARI KITA SERANG", maka huruf-huruf pada pesan tersebut akan dikelompokkan berpasangan dengan huruf di dekatnya. Sehingga dengan menggunakan aturan pada

Playfair Cipher pesan tersebut akan dikelompokkan dan dienkripsi sebagai berikut:

Plaintext : MARI KITA SERANG
Diagraphs : MA RI KI TA SE RA NG
Ciphertext : EG TN UI PF YM PD KL

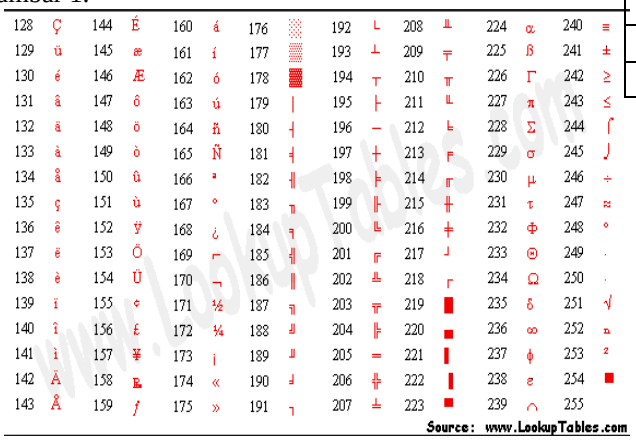
Enkripsi pesan oleh pasangan-pasangan huruf ini membuat Playfair Cipher mudah ditebak karena pasangan huruf yang sama misalnya pasangan huruf "SE" pada plaintext akan selalu diubah menjadi pasangan huruf "YM " pada ciphertext.

III. PLAYFAIR CIPHER YANG DIMODIFIKASI

Pada matriks 5x5, jika pada kunci terdapat huruf I dan J secara bersamaan maka harus dipilih untuk menggantikan huruf J dengan huruf I atau sebaliknya. Playfair Cipher yang dimodifikasi ini akan menyelesaikan masalah tersebut, karena tidak ada huruf yang diletakkan pada sel matriks yang sama.

Dengan adanya penambahan karakter ASCII maka huruf bigram yang sama pada plaintext tidak hanya dapat disisipi dengan huruf X atau Z, tetapi dapat juga menggunakan karakter ASCII yang tersedia pada matriks. Urutan karakter ASCII yang digunakan berurutan dari karakter ASCII yang pertama ditemukan dari pasangan huruf kunci dan seterusnya.

Karakter ASCII yang dimasukkan pada matriks menggunakan extended ASCII codes. Nilai desimal dari masing-masing extended ASCII codes ditunjukkan pada Gambar 1.



Gambar 1 Tabel Extended ASCII Codes

Alasan digunakan ASCII codes ini adalah agar pemilihan karakter ASCII yang dapat dipakai untuk penyisipan huruf lebih bebas dan tidak berpengaruh banyak terhadap makna pesan pada saat dekripsi. Perhitungan karakter ASCII ini menggunakan cara menghitung dari Vigenere Cipher dengan menggunakan extended ASCII codes. Untuk mengisi matriks, harus didapatkan 10 buah karakter ASCII yang berbeda. Dari sebuah kunci yang dipakai masing-masing hurufnya dipasangkan dengan masing-masing huruf yang lain. Misalkan digunakan kunci "KEYWORD", sehingga karakter-karakter ASCII yang didapatkan adalah sebagai berikut

1. Huruf K dan E dipasangkan, maka (int K+int E+256)%256 = 144(É)
2. Huruf K dan Y dipasangkan, maka (int K+int Y+256)%256=164(ñ)
3. Huruf K dan W dipasangkan, maka(int K+int W+256)%256 = 162(ó)
4. Huruf K dan O dipasangkan, maka (int K+int O+256)%256 = 154(Ü)
5. Huruf K dan R dipasangkan, maka (int K+int R+256)%256 = 157(¥)
6. Huruf K dan D dipasangkan, maka (int K+int D+256)%256 = 143(Å)
7. Huruf E dan Y dipasangkan, maka(int E +int Y+256)%256 = 158(Pts)
8. Huruf E dan W dipasangkan, maka (int E+intW+256)%256 = 156(£)
9. Huruf E dan O dipasangkan, maka (int E+int O+256)%256 = 148(ö)
10. Huruf E dan D dipasangkan, maka(int E+int D+256)%256 = 137(ë)

Penempatan karakter ASCII yang sudah didapakan ini ditaruh secara horizontal pada sisa baris matriks yang belum terisikan. Sehingga matriks playfair cipher yang didapatkan adalah sebagai berikut:

Tabel 2 Matriks Playfair Cipher Modifikasi

K	E	Y	W	O	R
D	A	B	C	F	G
H	I	J	L	M	N
P	Q	S	T	U	V
X	Z	É	ñ	ó	Ü
¥	Å	Pts	£	ö	ë

Pengubahan metode Playfair Cipher ini tidak hanya pada matriksnya saja tetapi juga pada proses enkripsi pesan. Pada metode sebelumnya untuk melakukan enkripsi pesan, *string* pesan tersebut dipecah menjadi pasangan-pasangan huruf. Tetapi kelemahan dari metode itu adalah kriptanalis pada frekuensi kemunculan huruf pada cipherteks. Pada metode modifikasi ini, pesan tidak hanya dipecah menjadi pasangan-pasangan huruf, tetapi juga dipasangkan dengan huruf pada kunci. Hal tersebut dapat mengurangi potensi untuk dapat dilakukan kriptanalis dengan melihat frekuensi kemunculan huruf. Ilustrasi dari modifikasi metode enkripsi Playfair Cipher adalah sebagai berikut:

Plaintext : GOOD BROOMS SWEEP CLEAN

Pasangan huruf : GO OD BR OO MS SW EE PC LE AN

Karena ada pasangan huruf yang sama maka pasangan huruf disisipi oleh karakter ASCII, sehingga didapatkan:

GO OD BR OÉ OM Sñ SW Eó EP CL EA NÜ

Kunci : KEYWORD

Pasangan huruf plaintext and kunci:

GO OD BR OÉ OM Sñ SW Eó EP CL EA NÜ

K E Y W O R D K E Y W O

Ciphertext : FDRK KEFA GBYW YWóñ FMUó VTYÉ PTKY ORZX KEQZ LJTS ACIL VUëö

Untuk memudahkan proses enkripsi maka kunci yang akan dipasangkan pada pasangan plaintext hanya satu huruf untuk sepasang plaintext. Lalu pada penulisan ciphertext, hasil playfair pada pasangan plaintext juga dituliskan dengan aturan:

1. Ambil pasangan huruf yang pertama yaitu GO. GO pada playfair cipher akan menghasilkan FR.
2. FR dari proses sebelumnya, masing-masing hurufnya akan di playfair cipher kembali dengan huruf K yang didapatkan dari kunci. Huruf F dipasangkan dengan huruf K akan didapatkan huruf D. Huruf R dipasangkan dengan huruk K akan didapatkan huruf K.
3. Pada proses ini akan didapatkan dua buah pasang huruf ciphertext untuk sepasang huruf plaintext. Pasangan huruf tersebut adalah FR dan DK.
4. Lalu pada penulisan ciphertext dengan melihat besar integer dari huruf K. Huruf K mempunyai nilai 43, yang berarti angka tersebut ganjil. Sehingga pasangan ciphertext yang didapatkan langsung dari playfair dengan plaintext ditempatkan pada posisi ganjil.
5. Ciphertext yang didapatkan untuk plaintext GO adalah FDRK dengan huruf F dan R ditempatkan pada posisi ganjil dikarenakan nilai K yang ganjil.
6. Proses ini dilakukan berulang untuk pasangan-pasangan plaintext berikutnya.

Ciphertext dari plaintext dengan menggunakan algoritma ini akan bertambah jumlah hurufnya menjadi dua kali lipatnya. Hal ini dikarenakan sepasang huruf plaintext akan dienkripsi menjadi dua pasang huruf ciphertext. Hasil ciphertext dari metode ini hanya akan mengaburkan pasangan-pasangan huruf yang muncul dari playfair cipher dari plaintext.

Dilakukan pengujian terhadap sebuah text dengan modifikasi Playfair Cipher ini.

Plaintext

ketika kita mengalami keseleo sakit yang kita alami biasanya disebabkan oleh adanya jaringan atau pembuluh darah yang robek akibat salah posisi atau terjatuh dengan melakukan pijatan langsung setelah mengalami cedera

Kunci : KEYWORD

Plaintext akan dibagi-bagi menjadi pasangan huruf dan akan disisipkan karakter extended ASCII codes. Huruf-huruf pada plaintext ini diubah menjadi huruf *uppercase* pada saat proses enkripsi.

KE TI KA KI TA ME NG AL AM IK ES EL EO SA KI TY AN GK IT AÉ AL AM IB IA SA NY AD IS EB AB KA NO LE HA DA NY AJ AR IN GA NA TA UP EM BU LU HD AR AH YA NG RO BE KA KI BA TS AL AH PO SI SI AT AU TE RJ AT UH DE NG AN ME LA KU KA NP IJ AT AN LA NG SU NG SE TE LA HM EN GA LA MI CE DE RA

Hasil enkripsi dengan modifikasi pada matriks saja didapatkan

EY QL ED EH QC IO NV CI FI HE YQ WI YR QB EH SW GI DR LQ BZ CI FI JA QI QB JR BA JQ YA BC ED MR IW ID AB JR BI GE JH DB IG QC VQ OI FS MT PH GE DI EB VN KR AY ED EH CB UI CI DI UK QJ QJ CQ FQ QW YN CQ PM AK VN GI IO IC OP ED HV JL CQ GI IC VN TV VN QY QW IC IN RI DB IC NJ AW AK EG

Hasil enkripsi yang didapatkan dengan modifikasi matriks dan playfair cipher dengan kunci didapatkan

YW ZI YB YL UF NR HP DH AQ JY QT OM WR PC YP QO BJ CK MU GÜ FH DH II SI TY MK GG HP WD AA YB LO MO NG BC HK AQ BY LL FF NN PF PP RQ BQ Lñ UM NK DH YD QI WK CW YF YN FC PP AQ BJ TE UM VN FP DP ZO YJ LT UU GE PG DH QR JB RT YF NÜ HH DP AQ JB TL UU ÜV PB PO QA JJ KL AF NG HH DO IY YB

Hasil enkripsi yang didapatkan dengan modifikasi matriks, playfair cipher dengan kunci dan peletakkan huruf cipher ini didapatkan

EYYW QZLI EYDB EYHL QUCF NIRO HNPV CDIH FAIQ HJEY YWQT WOIM WYRR PQCB EYHP SQWO GBIJ DCRK LMQU GBÜZ FCHI FDIH JIAI QSII QTBY JMRK GBGA HJPQ YWAD BACA EYDB MLRO IMWO NIGD BACB JHRK BAIQ GBEY JLHL DFBF NING PQFC VPQP ORIQ FBSQ MLTñ PUHM NGKE DDHI EYBD VQNI KWRK ACYW EYDF YENH FCCB UPTP CAIQ DBIJ UTKE QUJM VQNJ FCPQ FDQP QZWO YYNJ CLQT PUMU GAEK PVGN GDIH IQOR IJCB ORPT EYDF NHÜV HJHL CDQP GAIQ IJCB VTNL TUVU ÜVVN QPYB QPWO IQCA IJNJ RKIL DABF NIGC HNHJ ADWO AIKY EYGB

Proses dekripsi dimulai dengan mengkelompokkan huruf-huruf ciphertext menjadi 4 huruf per kelompok. Kelompok yang terdiri dari 4 huruf tersebut dipasangkan dengan satu huruf kunci secara berurutan untuk masing-masing kelompok. Lalu melihat nilai dari huruf kunci untuk dua pasang huruf ciphertext. Jika huruf kunci untuk dua pasang ciphertext tersebut ganjil, maka ambil huruf-huruf dengan urutan ganjil. Jika huruf kunci genap, maka ambil huruf-huruf dengan urutan genap. Misalkan pada ciphertext FDRK, dengan kunci K, maka huruf-huruf yang diambil adalah huruf F dan R saja, karena nilai K adalah ganjil. Huruf D dan K pada kata tersebut tidak dihiraukan. Huruf F dan R akan membentuk sebuah perpotongan segiempat yang akan menghasilkan nilai GO sebagai plaintext.

Misalkan diambil satu baris pertama sebagai contoh dekripsi.

Ciphertext:

EYYW QZLI EYDB EYHL QUCF NIRO HNPV CDIH FAIQ HJEY

Kunci:

K E Y W O R D K E Y

Maka pasangan huruf ciphertext yang diambil untuk dilakukan dekripsi adalah

EY QL ED EH QC IO NV CI FI HE

Plaintext yang didapatkan dari potongan ciphertext tersebut adalah:

KETIKAKITAMENGALAMIK

IV. Analisis

Pada enkripsi dengan modifikasi matriks saja, pasangan-pasangan huruf yang sama tetap diterjemahkan menjadi pasangan huruf yang sama juga. Misalnya pada pasangan huruf KA akan diterjemahkan menjadi pasangan huruf ED. Lalu pasangan huruf SI SI pada kata POSISI diterjemahkan menjadi QJ QJ. Kemunculan huruf yang sama ini memungkinkan untuk dilakukan kriptanalis.

Pada enkripsi dengan modifikasi matriks dan juga playfair cipher kembali dengan huruf -huruf kunci dihasilkan variasi walapun huruf tersebut sama. Misalnya pada huruf SI SI pada kata POSISI diterjemahkan menjadi huruf UM VN.

V. Kesimpulan

Algoritma Playfair Cipher menghasilkan sebenarnya akan tetap akan menghasilkan pasangan huruf dengan frekuensi yang dapat ditebak. Pasangan huruf plaintext harus tetap dituliskan pada ciphertext karena akan tidak mungkin untuk dilakukan dekripsi jika hasil playfair dari plaintext tersebut tidak disimpan. Hal ini yang menyebabkan Playfair Cipher dapat dilakukan kriptanalis dengan melihat frekuensi kemunculan huruf.

Modifikasi dari algoritma Playfair Cipher ini hanya akan mengaburkan peletakkan dari pasangan-pasangan huruf cipehertext. Selain itu juga didukung dengan sepuluh karakter ASCII tambahan untuk menambah variasi huruf yang dapat disisipkan untuk pasangan huruf plaintext yang sama atau untuk huruf plaintext yang tidak mempunyai pasangan pada akhir dari teks.

References

[1] http://www.cs.berkeley.edu/~bh/pdf/v1ch12.pdf

[2] http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi/2012-2013/Algoritma%20Kriptografi%20Klasik_bag2%20(2013).ppt , diakses pukul 10:00PM

[3] http://www.google.com/imgres?sa=X&espvd=210&es_sm=122&tbm=isch&tbnid=IvVP_xaycIIKOM%3A&imgrefurl=http%3A%2F%2Fwww.asciitable.com%2F&docid=JMtOixefP_tDJM&imgurl=http%3A%2F%2Fwww.asciitable.com%2Findex%2Fextend.gif&w=573&h=335&ei=Lh8nU-TNA4Oxrgf4voDwBw&zoom=1&ved=0CG8QhBwwAg&iact=rc&dur=202&page=1&start=0&ndsp=11, diakses pukul 11:17PM

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

ttd

Gabrielle Wicesawati P /13510060