# Merandom Kunci Stream Chiper menggunakan Playfair Chiper yang Dimodifikasi

Reynald Alexander G 13509006
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
*13509006@std.stei.itb.ac.id*

***Makalah ini akan memaparkan bagaimana algoritma klasik dapat dipadukan dengan algoritma kriptografi modern. Di sini algoritma klasik berperan sebagai alat optimasi atau peningkat kekuatan. Dan di makalah ini akan dibahas bagaimana algoritma Playfair Chiper yang telah dimodifikasi dapat membantu algoritma Chiper Aliran.***

***Index Terms*—Playfair Chiper, Stream Chiper, bit.**

## I. PENDAHULUAN

Informasi adalah pesan atau kumpulan pesan yang terdiri dari order sekuens atau makna yang dapat ditafsirkan dari pesan atau kumpulan pesan. Informasi merupakan data yang telah diberi makna dalam suatu konteks. Informasi merupakan bagian yang penting dalam perjalanan hidup manusia. Ciri khas dari informasi adalah memiliki tenggat waktu tertentu dan berguna hanya untuk yang membutuhkan saja. Contohnya saja adalah tanggal lahir untuk diri sendiri dan kerabat, PIN ATM, surat untuk pengirim dan penerima, dsb.

Informasi ada yang sifatnya rahasia ada yang tidak. Namun demikian banyak sekali informasi yang sifatnya *confidential* yakni tidak untuk sajian untuk masyarakat umum. Sehingga itu kerahasiaan konten dari informasi itu perlu dijaga dan diamankan dari pihak yang tidak berwenang. Seiring berkembangnya zaman, teknologi pun berkembang. Demikian juga dengan pengiriman informasi. Sekarang pengiriman informasi tidak hanya menggunakan surat biasa saja, namun juga dengan menggunakan surat elektronik ataupun media elektronik lainnya seperti web dan lain sebagainya.

Salah satu bentuk pengamanan informasi elektronik ini adalah kriptografi. Kriptografi berasal dari bahasa Yunani yang terdiri dari κρυπτός yang berarti rahasia dan γράφειν yang berarti writing. Kriptografi merupakan studi teknik untuk mengamankan komunikasi dari pihak ketiga. Pada intinya kriptografi diterapkan menggunakan metode enkripsi yakni mengubah isi pesan sehingga tidak terbaca apabila tanpa kunci tertentu. Ada banyak algoritma kriptografi yang beredar saat ini. Namun demikian kriptografi dapat dijadikan dua kategori besar yakni algoritma simetris dan algoritma asimetris. Namun demikian algoritma simetris kebanyakan memiliki kelemahan yakni memiliki pola tertentu, salah satunya saja adalah algoritma chiper aliran. Oleh karena itu digunakanlah metode tambahan untuk dapat menambah kekuatan algoritma yang sudah *obsolete* ini.

## II. DASAR TEORI

### A. Algoritma Kriptografi Simetris

Algoritma kriptografi simetris merupakan algoritma di mana key yang digunakan untuk enkripsi maupun dekripsi adalah sama atau hanya perlu pengubahan sederhana antara kunci enkripsi dan kunci dekripsi. Penerapan kunci algoritma ini bisa bermacam-macam. Ada yang menggunakan huruf, angka, kata, ataupun bit. Algoritma yang menggunakan huruf,angka ataupun kata sebagai kuncinya antara lain adalah Caesar Chiper, Playfair Chiper, Viginere Chiper, dan lain sebagainya. Sedangkan algoritma yang menggunakan satuan bit sebagai pemrosesan kunci dapat dikategorikan menjadi dua kategori, antara lain chiper aliran(*stream chiper*) dan chiper blok(*block* chiper).

Stream chiper beroperasi pada plainteks maupun chiperteks dalam bentuk bit. Operasi dilakukan ke informasi dalam bentuk bit per bit satu demi satu. Chiper ini memiliki kecepatan yang lebih baik jika dibandingkan dengan metode chiper blok, akan tetapi algoritma ini memiliki kelemahan yakni apabila aliran kunci yang digunakan sama, maka serangan pola kunci dapat membongkar informasi yang ada.

Berikutnya adalah chiper blok, chiper blok merupakan chiper yang beroperasi dalam bit dengan cara membagi informasi ke dalam blok-blok yang berukuran tertentu(biasanya 64bit) kemudian dienkripsi setiap bloknya. Chiper blok mengenkripsi data ke dalam blok yang sudah fix. Berbeda dengan chiper aliran, chiper blok memiliki algoritma yang lebih rumit akan tetapi pemecahan dari chiper blok ini hanya dapat dilakukan dengan cara *exhaustive search*. *Contoh*-contoh dari chiper blok adalah DES, AES, RC2, Blowfish, RC5, IDEA, dsb.

### B. Algoritma Chiper Aliran

Chiper aliran merupakan chiper yang mengenkripsikan plainteks menjadi chiperteks bit per bit. Chiper aliran dikenalkan pertama kali oleh Vernam. Konsep dari Vernam chiper adalah mengubah karakter menjadi bentuk bit(0 atau 1). Chiperteks diperoleh dari operasi modulo 2 satu bit plainteks dengan 1 bit kunci.

$c_i = (p_i + k_i) \bmod 2$

Di mana :

$p_i$ : bit plainteks
$k_i$ : bit kunci
$c_i$ : bit chiperteks

Sedangkan plainteks diperoleh dari

$p_i = ( c_i - k_i ) \bmod 2$

Operasi di atas dapat diganti dengan operator XOR, karena operasi XOR identik dengan operasi penjumlahan modulo 2, sehingga persamaan enkripsi dapat ditulis sebagai

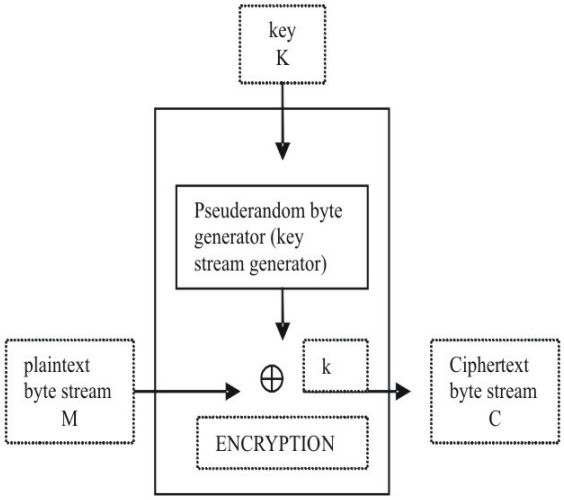
$c_i = p_i \oplus k_i$

Sedangkan proses dekripsi menggunakan persamaan

$p_i = c_i \oplus k_i$

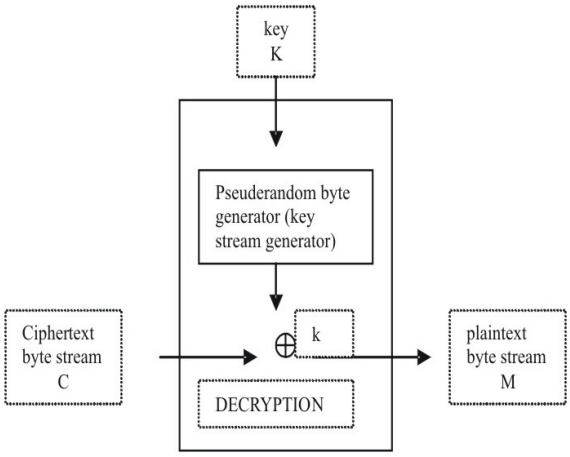
Sebagai catatan adalah proses enkripsi (operasi XOR) dua kali akan menghasilkan plainteks semula.

Aliran-bit-kunci dihasilkan dengan menggunakan *keystream generator*. Prinsip kerja dari pembangkit aliran-bit-kunci ini adalah dengan menggunakan sebuah kunci U, setelah itu kunci U ini diproses secara prosedural oleh pembangkit dan menghasilkan sederetan kunci yang mana panjangnya jika U memiliki panjang n bit maka kunci ini memiliki panjang $2^n - 1$ bit.




**Gambar 1**

Pembangkit aliran-bit-kunci bagian enchiper




**Gambar 2**

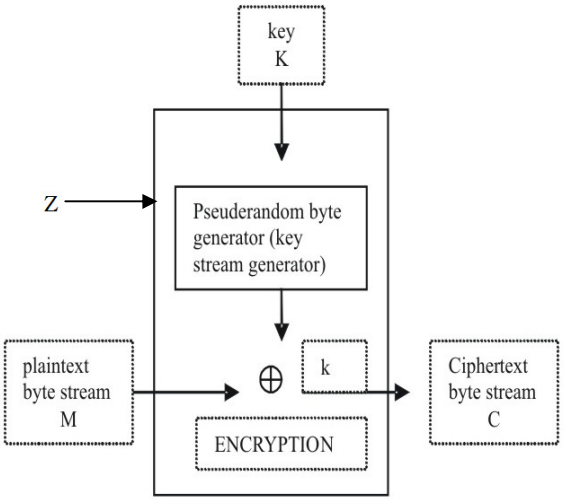
Pembangkit aliran-bit-kunci bagian dechiper

Adapun alternatif lain adalah dengan menggunakan sebuah umpan disimbolkan dengan Z, alternatif ini digunakan karena sifat U yang konstan jadi kunci akan terus berulang apabila hanya menggunakan U, sedangkan apabila menggunakan Z juga, maka kunci yang terbentuk bisa lebih bervariasi asalkan fungsi terhadap Z dan U tidak digunakan lebih dari sekali.
Proses enkripsi menjadi

$C = P \oplus g_u(Z)$

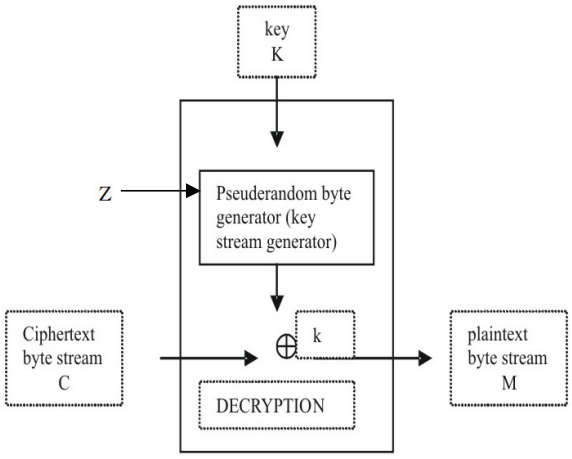
Sedangkan proses dekripsi menjadi

$P = C \oplus g_u(Z)$




**Gambar 3**

Pembangkit aliran-bit-kunci bagian enchiper dengan umpan Z




**Gambar 4**

Pembangkit aliran-bit-kunci bagian dechiper dengan umpan Z

C. Playfair Chiper

Playfair chiper merupakan *polygram chiper*(salah satu tipe chiper substitusi). Algoritma ini ditemukan oleh Sir Charles Wheatstone dan Baron Lyon Playfair. Kunci kriptografi yang digunakan adalah 25 buah huruf yang disusun dalam sebuah bujur sangkar.

Teknik chiper ini menggunakan teknik pengenkripsian pasangan huruf/digram, tidak seperti teknik-teknik enkripsi yang lain. Tujuan dari penggunaan digram ini adalah agar kriptanalisis menjadi semakin sulit terutama dengan analisis frekuensi, karena frekuensi kemunculan huruf-huruf di dalam chiperteks menjadi datar.

Proses pembentukan chiperteks terdiri dari beberapa tahap. Tahap pertama adalah pemisahan plainteks menjadi digram dan mengubah huruf i menjadi huruf j. Setelah itu menyisipkan huruf z di setiap karakter berurutan yang sama. Penambahan tersebut juga dilakukan ketika jumlah huruf bernilai ganjil.

Setelah tahap pemilahan plainteks, berikutnya adalah tahap pembentukan kunci. Kunci terbentuk dari susunan huruf-huruf yang apabila ada yang berulang, huruf tersebut dibuang. Setelah itu sisa huruf yang ada dituliskan di kotak-kotak berikutnya untuk melengkapi tabel kunci tersebut. Adapun algoritma enkripsi Playfair adalah sebagai berikut :

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 dengan 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.

Contoh: Kunci (yang sudah diperluas) ditulis kembali sebagai berikut:

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

**Tabel 1**

Tabel Playfair Chiper

Plainteks (dalam pasangan huruf):

GO OD BR OZ OM SZ SW EZ EP CL EA NZ

Cipherteks:

**FP UT EC UW PO DV TV BV CM BG CS DY**

Namun demikian, playfair chiper tetap memiliki kelemahan. Salah satunya adalah polygram dari chiper ini tidak cukup besar. Kelemahan yang lain adalah bahwa chiper ini tidak dapat dipecahkan dengan analisis frekuensi huruf tetapi dapat diserang dengan analisis kemunculan bigram.

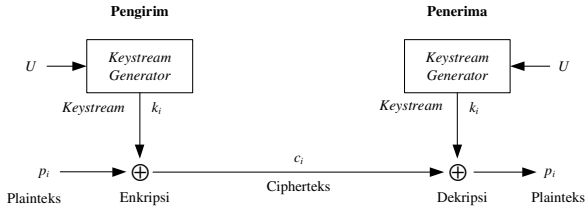
## III. MODIFIKASI CHIPER ALIRAN DENGAN BANTUAN PLAYFAIR CHIPER

Pembahasan di makalah ini dilakukan dalam lingkup Playfair chiper dan chiper aliran dengan batasannya adalah modifikasi untuk memperkuat chiper aliran ini saja. Di dalam makalah ini tidak akan dibahas bagaiman melakukan kriptanalisis terhadap modifikasi chiper tersebut. Dengan adanya modifikasi ini diharapkan chiper aliran tetap memiliki sifat simpel tetapi memiliki kekuatan yang jauh lebih baik daripada chiper aliran biasa.

Tolak ukur yang dapat digunakan sebagai parameter ini hanya ada dua, yakni sudah tercapainya tingkat keacakan yang tinggi(jarak pengulangan pola sangat jauh atau tidak ada). Parameter berikutnya adalah dengan tingkat keacakan tersebut, diharapkan chiper masih mudah digunakan, beda halnya dengan OTP(One Time Pad) chiper yang biaya pengiriman kuncinya saja sudah mahal karena kunci tidak dapat dibangkitkan di pihak penerima pesan.

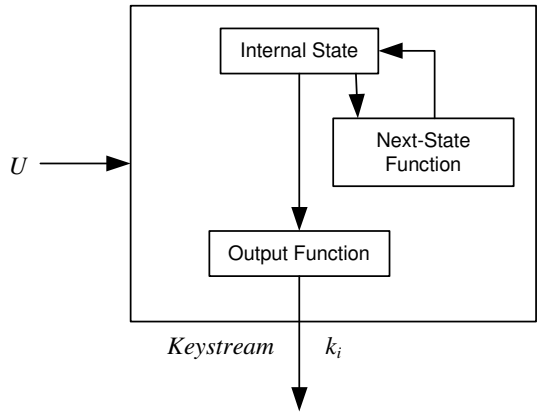
1. Letak penerapan Modified Playfair Chiper

Seperti yang telah dijelaskan sebelumnya bahwa chiper aliran biasa, yakni chiper dengan pembangkit aliran-bit-kunci sederhana sangat rentan terhadap serangan karena memiliki pola berulang.




**Gambar 5**

Gambaran umum dari chiper aliran




**Gambar 6**

Proses di dalam pembangkit aliran-kunci

Di dalam output function inilah algoritma perbaikan tersebut akan digunakan. Sehingga pada akhirnya kurang lebih algoritma ini bekerja layaknya umpan yang mempengaruhi kunci yang dibangkitkan. Umpan di dalam Output Function(Z) di sini adalah kunci dari Playfair Chiper.

2. Cara Kerja Penerapan Playfair Chiper

Berikut ini merupakan contoh tabel penerapan Playfair Chiper yang telah dimodifikasi.

KUNCI : 011010010101

| | | | | |
|---|---|---|---|---|
| 0110 | 1001 | 0101 | 0000 | 0110 |
| 0001 | 0010 | 0011 | 0100 | 0001 |
| 0111 | 1000 | 1010 | 1011 | 0111 |
| 1100 | 1101 | 1110 | 1111 | 1100 |
| 0110 | 1001 | 0101 | 0000 | |

**Tabel 2**

Tabel Playfair dalam bentuk bit

Konsep dari tabel penerapan ini adalah mengubah isi dari tabel menjadi kumpulan bit-bit. Cara menentukan panjang bit adalah dengan menggunakan panjang 8 bit untuk keystream yang akan diolah, mengapa 8 bit? Karena 8 bit merupakan standard pengkodean ASCII dalam bit. Selain itu dengan mengunakan 8 bit, kemungkinan perulangan kunci semakin kecil.

Mengapa penggunaan pendekatan seperti di atas menyebabkan perulangan kunci jauh lebih kecil? Karena tidak ada panjang bit hasil pembangkitan yang memiliki faktor prima 2. Mengapa bisa demikian? Karena perolehan panjang bit tersebut selalu diperoleh dari $2^n - 1$. Jadi tidak peduli berapapun panjang U, kunci yang dihasilkan akan selalu bernilai ganjil.

Oleh karena panjang bit yang diolah memiliki panjang 8 minimal bit atau lebih tepatnya dikelompokkan tiap-tiap 8 bit, maka panjang bit yang ada di tabel harus berukuran 4 bit untuk tiap-tiap selnya. Dengan demikian, keystream dapat dibagi menjadi 2 bagian yang masing-masing memiliki panjang 4 bit, hal seperti ini tidak berbeda jauh dengan cara kerja Playfair Chiper pada umumnya.

Cara kerja dari algoritma ini dapat dijelaskan sebagai berikut

Plainteks(Keystream) : 111101011001000

KUNCI : 011010010101

| | | | | |
|---|---|---|---|---|
| 0110 | 1001 | 0101 | 0000 | 0110 |
| 0001 | 0010 | 0011 | 0100 | 0001 |
| 0111 | 1000 | 1010 | 1011 | 0111 |
| 1100 | 1101 | 1110 | 1111 | 1100 |
| 0110 | 1001 | 0101 | 0000 | |

**Tabel 3**

Tabel Playfair dengan kunci 011010010101

Karena tabel yang digunakan memiliki panjang 4 bit, keystream yang hendak diubah dipecah-pecah menjadi perkelompokan 8 bit untuk masing-masing kelompoknya. Apabila panjang bit kurang, maka diisi oleh perulangan keystream, sehingga apabila operasi tersebut dilakukan akan menghasilkan hasil seperti berikut.

Plainteks : 11110101 10010001 11101011 00100011 11010110 01000111 ...

Chiperteks : 11100000 01100010 10101111 00110100 11001001 10110001 ...

Keuntungan yang diprediksi dari penggunaan Playfair Chiper ini adalah semakin kecilnya peluang kemunculan pola yang sama dan tingkat kesusahan pemecahan playfair chiper yang mustahil. Mengapa tingkat kesukarannya mustahil? Karena sebelumnya analisis bigraph pada Playfair chiperdapat menyebabkan pemecahan sandi yang di dalam Playfair Chiper. Hal itu terjadi karena Playfair Chiper digunakan untuk menyembunyikan pesan dalam bentuk karakter/huruf. Sedangkan di sini, penerapan cara kerja Playfair Chiper digunakan untuk menyembunyikan pesan yang tertulis dalam bentuk bit per bit sedangkan pemrosesannya pun per 4 bit.

## IV. ANALISA HASIL KEYSTREAM GENERATOR DENGAN TAMBAHAN PLAYFAIR CHIPER

Misalkan saja kita ambil contoh tadi untuk kita pecahkan hingga panjang maksimal, yakni hingga perulangan terjadi kembali.

KEYSTREAM :

111101011001000

KUNCI :

011010010101

| | | | | |
|---|---|---|---|---|
| 0110 | 1001 | 0101 | 0000 | 0110 |
| 0001 | 0010 | 0011 | 0100 | 0001 |
| 0111 | 1000 | 1010 | 1011 | 0111 |
| 1100 | 1101 | 1110 | 1111 | 1100 |
| 0110 | 1001 | 0101 | 0000 | |

Plainteks :

11110101 10010001 11101011 00100011 11010110 01000111 10101100 10001111 01011001 00011110 10110010 00111101 01100100 01111010 11001000 11110101

Chiperteks :

11100000 01100010 10101111 00110100 11001001 10110001 01110101 11011011 00001001 11000011 10000100 00101110 00010000 100001011 01111101 11100000

Seperti yang kita lihat di atas, bahwa pola berulang kembali setelah bit ke-120. Kekuatan dari pengaruh algoritma ini dapat meningkat hingga 8 kali lipat dari semula. Dengan semakin panjangnya aliran-bit-kunci yang dibangkitkan, panjang bit yang terenkripsi sebelum pola berulang kembali tentunya akan besar. Sebagai catatan bahwa Plainteks di atas merupakan aliran-bit-kunci yang baru saja dibangkitkan, sedangkan Chiperteks di atas merupakan aliran-bit-kunci yang telah dienkripsikan menggunakan Playfair Chiper.

Berikut ini merupakan hasil analisis dari tambahan Playfair Chiper ini :

1. Kekuatan dari Chiper Aliran bertambah hingga 8 kali lipat
2. Semakin panjang Chiper, pertambahan kekuatan pengamanannya akan bertambah secara eksponensial
3. Kelemahannya adalah masih bisa diserang dengan serangan seperti biasa namun cara yang ditempuh lebih sulit karena panjang kunci bertambah drastis

Berikut adalah sebagian kode Playfair Chiper dalam Java

```
public String[] SeparateIntoEight(String S){
//fungsi ini menghasilkan kunci yang terbagi menjadi 8 per bagian bit
String[] S1= new String[100];
for(int j = 0 ; j < (S.length/8) ; j++){
for(int i = 0 ; i < 8 ; i++){
S1[i]+= S.charAt(i);
}
}
return S1;
}
```

Sedangkan untuk pemrosesan plainteks dengan menggunakan chiper aliran, digunakanlah metode :

1. Mengubah plainteks menjadi bentuk bit per bit
2. Mengenkripsi bit plainteks dengan menggunakan chiper aliran

dan untuk pemrosesan chiperteks menjadi plainteks digunakan metode :

1. Mendekripsi bit chiperteks dengan menggunakan chiper aliran
2. Mengubah bit plainteks menjadi bentuk kata-kata kembali.

Berikut adalah contoh konversinya dengan KUNCI :

11100000 01100010 10101111 00110100 11001001 10110001 01110101 11011011 00001001 11000011 10000100 00101110 00010000 100001011 01111101 11100000 sedangkan untuk enkripsinya tidak dilakukan.

JAKARTA, KOMPAS.com – Presiden Susilo Bambang Yudhoyono mengatakan, proses pemulihan Ibu Negara Ani Yudhoyono, yang telah menjalani operasi menjalani operasi pengangkatan kandung empedu beserta batunya, berjalan baik.

Dalam waktu tidak terlalu lama, Ibu Ani segera aktif kembali mendampingi Presiden. “(Ibu Negara dapat) mendampingi saya dalam mengemban tugas. Terima kasih atas semua doanya,” kata Presiden di Rumah Sakit Pusat Angkatan Darat (RSPAD) Gatot Subroto, Jakarta, Sabtu

01001010 01000001 01001011 01000001 01010010 01010100 01000001 00101100 00100000 01001011 01001111 01001101 01010000 01000001 01010011 00101110 01100011 01101111 01101101 00100000 00101101 00100000 01010000 01110010 01100101 01110011 01101001 01100100 01100101 01101110 00100000 01010011 01110101 01110011 01101001 01101100 01101111 00100000 01000010 01100001 01101101 01100010 01100001 01101110 01100111 00100000 01011001 01110101 01100100 01101000 01101111 01111001 01101111 01101110 01101111 00100000 01101101 01100101 01101110 01100111 01100001 01110100 01100001 01101011 01100001 01101110 00101100 00100000 01110000 01110010 01101111 01110011 01100101 01110011 00100000 01110000 01100101 01101101 01110101 01101100 01101001 01101000 01100001 01101110 00100000 01001001 01100010 01110101 00100000 01001110 01100101 01100111 01100001 01110010 01100001 00100000 01000001 01101110 01101001 00100000 01011001 01110101 01100100 01101000 01101111

## V. KESIMPULAN

Yang dapat ditarik kesimpulan dari analisis di atas adalah bahwa Chiper aliran mendapat kekuatan pengamanan sebanyak 8 kali lipat di mana semakin panjang kunci awal semakin baik. Metode ini tetap bisa diserang menggunakan serangan pada chiper aliran seperti biasa namun tingkat kesulitannya semakin bertambah dengan tingkat transmisi jauh lebih simpel karena dengan sedikit saja kunci terbangkitkan, variasi kunci yang timbul bisa lebih banyak.

## REFERENCES


Munir, Rinaldi, Ir.,M.T. 2005. Diktat Kuliah IF-5054 Kriptografi. Bandung : Informatika ITB

http://en.wikipedia.org/wiki/Playfair_cipher

http://www.simonsingh.net/The_Black_Chamber/playfair_cipher.html

http://informatika.stei.itb.ac.id/~rinaldi.munir/Kriptografi

http://www.crypthography.com


## VII. 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, 20 Maret 2012

ttd

Reynald Alexander G
13509006