Kriptografi

Teknik Playfair Cipher

Sindhu Rakasiwi



Objectives



- Mahasiswa mendapatkan penjelasan mengenai sejarah, teknik penggunaan playfair cipher
- Mahasiswa mendapatkan penjelasan mengenai langkah-langkah penerapan playfair cipher



Termasuk ke dalam polygram cipher.

Ditemukan oleh Sir Charles Wheatstone namun dipromosikan oleh Baron Lyon Playfair pada tahun 1854.



Sir Charles Wheatstone



Baron Lyon Playfair



Cipher ini mengenkripsi pasangan huruf (digram) atau digraf), bukan huruf tunggal seperti pada cipher klasik lainnya.

Tujuannya adalah untuk membuat analisis frekuensi menjadi sangat sulit sebab frekuensi kemunculan huruf-huruf di dalam cipherteks menjadi datar (flat).



Kunci kriptografinya 25 buah huruf yang disusun di dalam bujur sangkar 5x5 dengan menghilangkan huruf J dari abjad.

Contoh kunci:

S	Т	Α	N	D
E	R	С	Н	В
K	F	U	Ι	L
М	0	Р	Q	U
V	M	Χ	Y	Z

Jumlah kemungkinan kunci: 25!=15.511.210.043.330.985.984.000.000



Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam.

S	Т	А	N	D	S
E	R	\cup	Н	В	E
K	F	G	I	L	K
M	0	Р	Q	U	M
V	M	Χ	Y	Z	V
S	Т	А	N	D	

Baris ke-6 = baris ke-1 Kolom ke-6 = kolom ke-1



- Pesan yang akan dienkripsi diatur terlebih dahulu sebagai berikut:
 - Ganti huruf J (bila ada) dengan I
 - 2. Tulis pesan dalam pasangan huruf (bigram).
 - Jangan sampai ada pasangan huruf yang sama.
 Jika ada, sisipkan z di tengahnya
 - 4. Jika jumlah huruf ganjil, tambahkan huruf z di akhir



Contoh:

Plainteks: GOOD BROOMS SWEEP CLEAN

→ Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf:

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



Algoritma enkripsi:

- Jika dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya.
- Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya.
- 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	Т	А	N	D	S
E	R	С	Н	В	E
K	F	G	I	L	K
М	0	Р	Q	U	M
V	M	Х	Y	Z	V
S	Т	А	N	D	

Plainteks (dalam pasangan huruf):

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

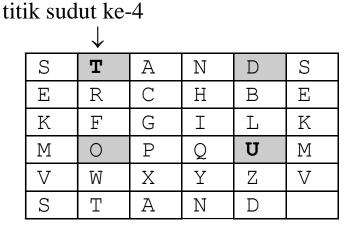
Cipherteks:

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



Enkripsi OD menjadi **UT** ditunjukkan pada bujursangkar di bawah ini:

S	Т	А	N	D	S
E	R	\cup	Н	В	E
K	F	U	I	L	K
М	0	Р	Q	ט	M
V	M	Χ	Y	Z	V
S	Т	А	N	D	





Kunci dapat dipilih dari sebuah kalimat yang mudah diingat, misalnya:

JALAN NAKULA SEBELAS

Buang huruf yang berulang dan huruf J jika ada:

ALNKUSEB

Lalu tambahkan huruf-huruf yang belum ada (kecuali J):

ALNKUSEBCDFGHIMOPQRTVWXYZ

Masukkan ke dalam bujursangkar:

А	L	N	K	U
S	E	В	\cup	D
F	Ġ	Н	I	М
0	Р	Q	R	Т
V	M	Χ	Y	Z



- Karena ada 26 huruf abjad, maka terdapat 26 x 26 = 677 bigram, sehingga identifikasi bigram individual lebih sukar.
- Sayangnya ukuran poligram di dalam Playfair cipher tidak cukup besar, hanya dua huruf sehingga Playfair cipher tidak aman.
- Meskipun Playfair cipher sulit dipecahkan dengan analisis frekuensi relatif huruf-huruf, namun ia dapat dipecahkan dengan analisis frekuensi pasangan huruf.
- Dalam Bahasa Inggris kita bisa mempunyai frekuensi kemunculan pasangan huruf, misalnya pasangan huruf TH dan HE paling sering muncul.
- Dengan menggunakan tabel frekuensi kemunculan pasangan huruf di dalam Bahasa Inggris dan cipherteks yang cukup banyak, Playfair cipher dapat dipecahkan.

Sumber



- Rinaldi Munir, ITB
- Aisyatul Karima, UDINUS
- Bruce Scheier, (2001), Applied Cryptography,
 John Willey & Sons Inc, Canada
- Cobb, Chey, (2004), Cryptography for Dummies, John Willey & Sons Inc, Canada
- Stalling William, (2003), Cryptography and Network Security, Prentice Hall, USA

Quiz



1. P = nama sendiri

K = TEKNIK INFORMATIKA

C???

(point 35)

2. P = Suka Belajar Kriptografi

K = Playfair Cipher

C???

(point 35)

3. P = Tulis pesan dalam bigram

K = Indonesia Negara Kaya dan Jaya

C???

(point 30)



