

# ***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

# ***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

# ***Playfair Cipher***



- 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).

# Playfair Cipher



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

Contoh kunci:

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

- Jumlah kemungkinan kunci:  
 $25! = 15.511.210.043.330.985.984.000.000$

# Playfair Cipher



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

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	

Baris ke-6 = baris ke-1

Kolom ke-6 = kolom ke-1

# ***Playfair Cipher***



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

# ***Playfair Cipher***



## ■ 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**



# ***Playfair Cipher***



- 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.

# Playfair Cipher



- 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	

- 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**

# Playfair Cipher



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

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	

titik sudut ke-4



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

# ***Playfair Cipher***



- 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:

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

# ***Playfair Cipher***



- Karena ada 26 huruf abjad, maka terdapat  $26 \times 26 = 677$  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.

- 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)

