Nama-nama Kelompok Ganjil :

1. Fahim Afifuddin (201851007)
2. Dliyaur Rahman Muhammad (201851011)
3. Muhammad Hamzah Fanzuri (201851019)
4. Deva Fungki J (201851167)

Kelas : 4E

Algoritma Kriptografi Playfair Chiper

1. Pengertian Algoritma Playfair Chipher

   Playfair Cipher ditemukan oleh Sir Charles Wheatstone (1802-1875) pada tahun 1854, dan dipopulerkan oleh Baron Lyon Playfair (1819-1898), yang namanya diabadikan untuk algoritma ini. Meskipun algoritma Playfair ini sudah tidak aman untuk kegunaan dunia saat ini, Playfair cipher banyak digunakan dan cukup efektif pada jamannya. Playfair cipher pertama kali digunakan oleh tentara Inggris pada perang Boer dan masih digunakan pada Perang Dunia I. Playfair Cipher merupakan suatu algoritma kriptografi klasik yang termasuk ke dalam polygram cipher, dimana plainteks diubah menjadi bentuk poligram dan proses enkripsi dekripsi dilakukan untuk poligram tersebut. Kunci kriptografinya adalah 25 buah huruf yang disusun di dalam bujursangkat 5x5 dengan menghilangkan huruf J dari abjad. Kemungkinan kuncinya adalah 25!. Susunan kunci di dalam bujursangkar diperluas dengan menambahkan kolom keenam dan baris keenam. Basis keenam merupakan baris pertama, sementara kolom keenam berisi kolom pertama. Pada umumnya, kunci yang digunakan adalah serangkaian kata yang mudah dimengerti.

2. Karakteristik dari Playfair Cipher
   a. Merupakan salah satu cipher subtitusi
   b. Jumlah karakter pada cipher teks akan selalu genap
   c. Perhitungan frekuensi kemunculan akan menghasilkan tidak lebih dari 25 karakter huruf, karena huruf J tidak akan pernah muncul
   d. Jika terjadi perulangan panjang, akan muncul pada interval yang regular, dan dalam banyak kasus, akan berulang dalam jumlah karakter yang genap
   e. Banyak kemungkinan transformasi untuk suatu bigram.
3. Metode Playfair Cipher
   - Playfair cipher atau bisa juga disebut Playfair square adalah teknik enkripsi simetrik yang termasuk dalam sistem substitusi digraph.
   - Sistem sandi ini mengenkripsi pasangan huruf(digraph),
   - Oleh karena itu sistem ini lebih sulit untuk dipecahkan jika dibandingkan dengan system substitusi sederhana seperti caesar atau viginere

4. Mengatur Pesan yang akan dienkripsikan
    a. Ganti huruf dengan J (bila ada) dengan huruf I
    b. Tulis pesan dalam pasangan huruf
    c. Jangan sampai ada pasangan huruf yang sama. Jika ada, sisipkan Z di tengahnya
    d. Jika jumlah huruf ganjil, tambahkan Z di akhir
5. Algoritma dalam enkripsi
    a. Jika ada dua huruf terdapat pada baris kunci yang sama maka tiap huruf diganti dengan huruf di kanannya (pada kunci yang sudah diperluas)
    b. Jika dua huruf terdapat pada kolom kunci yang sama maka tiap huruf diganti dengan huruf di bawahnya (pada kunci yang sudah diperluas)
    c. 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
    d. Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari 3 huruf yang digunakan sampai sejauh ini
6. Contoh dari Algoritma Playfair Cipher
    a. Contoh dari **Fahim Afifuddin (201851007)):**

Contoh Kunci:

Kemungkinan Kunci Playfair Cipher

Kemudian Susunan kunci (Cipher) dalam bujursangkar diperluas dengan menambahkan baris keenam dan kolom keenam. sehingga menjadi:

Kemungkinan Kunci Playfair Cipher

Kemudian untuk melakukan Enkripsi, Pesan yang akan dienkripsi diatur terlebih dahulu sesuai ketentuan sebagai berikut:

- Ganti huruf J (jika ada) dengan huruf I
- Tulis pesan dalam pasangan huruf (huruf berpasangan dua-dua / bigram).
- Jangan ada pasangan huruf yang sama (misal AA / BB). Jika ada, sisipkan Z di tengahnya
- Jika jumlah huruf ganjil (sehingga ada yang tidak punya pasangan), tambahkan huruf Z di akhir

Contoh Enkripsi Pesan dengan Playfair Cipher:

Plaintext (Pesan Asli): GOOD BROOMS SWEEP CLEAN → Tidak ada huruf J, maka langsung tulis pesan dalam pasangan huruf,
menjadi: GO OD BR OZ OM SZ SW EZ EP CL EA NZ

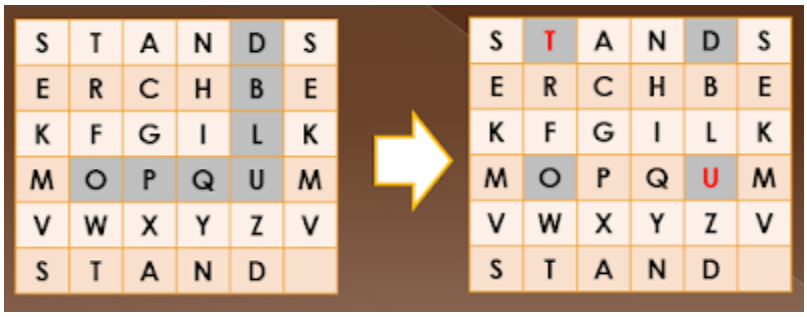
Algoritma enkripsi (Ketentuan Enkripsi):

- Seandainya 2(dua) huruf terdapat pada kolom kunci yang sama, maka setiap huruf diganti dengan huruf di bawahnya.
- Seandainya 2(dua) huruf terdapat pada baris kunci yang sama, maka setiap huruf diganti dengan huruf di kanannya.
- Seandainya 2(dua) huruf tidak pada kolom yang sama atau baris yang sama, maka huruf pertama diganti dengan huruf pada perpotongan baris huruf pertama dengan kolom huruf kedua. kemudian Huruf kedua diganti dengan huruf pada titik sudut keempat dari persegi panjang yang dibentuk dari tiga huruf yang digunakan sampai sejauh ini.

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

Contoh Kunci Playfair Cipher

Pada contoh di atas, enkripsi OD menjadi UT, dapat di ilustrasikan sebagai berikut:



Ilustrasi Enkripsi dengan Playfair Cipher

Kunci dapat juga dipilih dari kalimat spesifik yang mudah diingat. Misalnya:
Plaintext (Pesan Asli): TEKNIK INFORMATIKA UDINUS

Kunci (Ciphertext): J**AL**AN NA**KU**LA
Kunci baru dibentuk dengan menuliskan hanya *karakter tunggal*, selain huruf J, dan ditambah sisa dari 26 alfabet, menjadi: Kunci
Baru: **ALNKU**BCDEFGHIMOPQRSTVWXYZ. Kemudian masukkan kunci baru ke dalam bujur sangkar:

Ilustrasi Enkripsi dengan Playfair Cipher

b. Contoh dari **Dliyaur Rahman Muhammad (201851011) :**
Plaintext : **ALDYZK PERGI KE KAMPUS**
Key : **ANAK HILANG**
Maka key yang digunakan adalah **ANKHILG**
Dengan matriks:

Kunci ditambah huruf alphabet

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

Kunci Dilebarkan

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

Hasil

Plaintext	AL	DY	ZK	PE	RG	IK	EK	AM	PU	SZ
Chipertext	LE	CZ	XI	EF	WF	AH	MA	KE	UZ	UX

Maka **ALDYZK PERGI KE KAMPUS** Menjadi **LECZXIEFWFAHMAKEUZUX**

Kesimpulan ;

1. Karena terdapat 26 huruf abjad (A-Z), maka terdapat 26 kali 26 = 677 bigram, sehingga identifikasi bigram individual menjadi lebih sulit.
2. Sayangnya ukuran poligram di dalam Playfair cipher tidak cukup besar, hanya dua huruf sehingga Playfair cipher tidak aman.
3. Walaupun Playfair susah dipecahkan menggunakan analisis frekuensi relatif huruf, namun Playfair Cipher bisa dipecahkan (ditembus) dengan analisis frekuensi pada pasangan huruf.
4. Dengan memakai frekuensi tabel / tabel kemunculan pasangan huruf dalam Bahasa Inggris dan cipherteks yang banyak, Playfair bisa dipecahkan.
5. Karena pada Bahasa Inggris kita dapat mendapatkan frekuensi kemunculan pasangan huruf, contohnya pasangan huruf HE dan TH yang merupakan pasangan huruf yang paling sering muncul (Sering muncul dalam Bahasa Inggris).

c. Contoh dari **Muhammad Hamzah Fanzuri (201851019) :**

Plainteks : PA ENTIK BAIK SEKALI

Kunci : EGI ANDRIANA

1. Susun dahulu hurufnya, huruf yang sudah disebutkan tidak dituliskan lagi EGIANDR kemdian jika terdapat huruf J makan diganti dengan huruf I.
2. Selanjutnya tambakan dengan huruf abjad sisanya yang tidak terdapat pada kunci tadi **BCFHKLMOPQSTUVWXYZ** menjadi **EGIANDRBCFHKLMOPQSTUVWXYZ**
3. Masukkan ke dalam bujur sangkar

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

4. Selanjutnya kunci diperluas untuk masuk kedalam proses enkripsi

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

5. Hilangkan semua karakter yang bukan huruf abjad
6. Tidak terdapat huruf J, maka langsung lakukan pasangan huruf
7. Jika ada pasangan huruf yang sama, sisipkan huruf Z Jika telah dipasangkan

PA EN TI KB AI KS EK AL IZ

PA menjadi **TE**
EN menjadi **GE**
TI menjadi **TA**
KB menjadi **LR**
AI menjadi **NA**
KS menjadi **LQ**
EK menjadi **GH**
AL menjadi **IM**
IZ menjadi **NX**

Setelah proses enkripsi selesai, hasil enkripsinya adalah :
Plaintext **: PA EN TI KB AI KS EK AL IZ**
Ciphertext **: TE GE SA LR NA LQ GH IM NX**

d. Contoh dari **Deva Fungki J (201851167) :**

Contoh:

Plaintext = RIVALRY HONDRO

Kunci = BUDIDARMA

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

Bujursangkar Kunci

Penyelesaian (lihat ketentuan)

Cek plaintext mengandung huruf "J" atau tidak, selanjutnya membuat plaintext menjadi huruf berpasang-pasangan :

RI VA LR YH ON DR O

Dari pasangan huruf tersebut cek ada tidak huruf yang berpasangan dengan huruf yang sama (lihat ketentuan diatas), selanjutnya jika ada pasangan huruf berjumlah ganjil maka (lihat ketentuan diatas).

RI VA LR YH ON DR O

Maka Proses Enskripsi Playfair Cipher (lihat ketentuan enskripsi diatas)

a. RI berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf R di ganti dengan huruf E, dan huruf I diganti dengan huruf B maka hasil enkripsi pasangan huruf RI = EI
b. VA berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf V di ganti dengan huruf Z, dan huruf A diganti dengan huruf B maka hasil enkripsi pasangan huruf VA = ZB
c. LR berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf L di ganti dengan huruf G, dan huruf R diganti dengan huruf E maka hasil enkripsi pasangan huruf LR = GE

d. YH berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf Y di ganti dengan huruf W, dan huruf H diganti dengan huruf L maka hasil enkripsi pasangan huruf YH = WL
e. ON berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf O di ganti dengan huruf T, dan huruf N diganti dengan huruf G maka hasil enkripsi pasangan huruf ON = TG
f. DR berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf D di ganti dengan huruf B, dan huruf R diganti dengan huruf C maka hasil enkripsi pasangan huruf huruf DR = BC
g. OZ berada pada baris dan kolom yang berbeda pada bujungsangkar kunci, maka huruf O di ganti dengan huruf T, dan huruf Z diganti dengan huruf V maka hasil enkripsi pasangan huruf huruf OZ = TV

Hasil proses enkripsi :

EI ZB GE WL TG BC TV

PROSES PENGERJAAN TUGAS (SCREEN SHOOT)