**Anggota Kelompok:**

1. **Patrick Sungkharisma 05111740000041**
2. **Jonathan Alphabert S. 05111740000053**
3. **Fandi Pranata Jaya 05111740000056**
4. **Yovi Agustian 05111740000125**

**Play Fair Cipher**

Program ini merupakan program yang digunakan untuk mengenkripsi ataupun mendekripsikan sebuah file menggunakan metode Play Fair cipher Program ini menggunakan key "QUATERVOIS" Untuk proses pembuatannya kami menggunakan IDE Visual Studio Code

**Penjelasan Code dari PlayFair**

Pada program kami, terdapat dua file yaitu structure.h dan fair.cpp. Di dalam structure.h terdapat semua hal yang dibutuhkan pada saat decrypt dan encrypt. Dalam file structure terdapat dua struktur data.

1. **Matrix 5x5**

char extractChar[5][5]= {{'q', 'u', 'a', 't', 'e'},

{'r', 'v', 'o', 'i', 's'},

{'b', 'c', 'd', 'f', 'g'},

{'h', 'k', 'l', 'm', 'n'},

{'p', 'w', 'x', 'y', 'z'}};

Struktur data ini bertujuan untuk mengambil karakter pada posisi yang ditentukan setelah diproses dalam encrypt dan decrypt. Dalam proses encrypt dan decrypt, terjadi perubahan posisi berdasarkan aturan yang telah ditentukan. Contoh perubahan posisi yang dilakukan pada proses encrypt dan decrypt:

encrypted\_i1 = i1;

encrypted\_j1 = (j1 + 1)%5;

encrypted\_i2 = i2;

encrypted\_j2 = (j2 + 1)%5;

Setelah melakukan proses demikian, maka perlu mengambil karakter yang sesuai dengan posisi setelah diubah. Sehingga struktur data ini akan langsung mengambil kontain dari extractChar[i][j]

1. **Struktur data map**

void generateExtractIndex(){

for(int i=0; i<5; i++)

{

for(int j=0; j<5; j++)

{

extractIndex.insert(pair<char, int>(extractChar[i][j], (i+1)\*10+(j+1)));

}

}

}

Struktur data ini memudahkan untuk mencari index dari karakter yang akan diubah, sehingga tidak diperlukan pencarian secara linear terus menerus. Untuk mendapatkan indexnya maka kita butuh memanggil index dengan karakter seperti berikut

i1 = extractIndex[buffer1]/10 - 1;

j1 = extractIndex[buffer1]%10 - 1;

Buffer1 merupakan variabel char yang berisi karakter yang akan diganti. Karena dalam struktur data map, kita diizinkan untuk menggunakan variabel non integer untuk menjadi index.

Dalam fair.cpp, terdapat tiga fungsi yang paling utama, yaitu:

1. **Enkripsi dan Dekripsi**

Fungsi ini berjalan untuk mengenkripsikan ataupun mendekripsikan dua karakter yang dipassing.

1. **setPathFile**

Fungsi ini untuk setting path file yang akan diencrypt ataupun didekripsi, dan juga file yang dihasilkan setelah proses enkripsi selesai

1. **readFile**

Fungsi ini membaca semua karakter yang ada pada file yang akan diencrypt ataupun didecrypt. Dalam fungsi ini akan memanggil fungsi enkripsi dan dekripsi sesuai mode yang dipilih dengan mempassing dua karakter kedalam fungsi itu.

Ketiga fungsi ini berada dalam suatu class. Alasan kita menggunakan class, karena kita ingin sekadar berlatih apa yang sudah kita dapatkan di semester lalu.

**Menjalankan Program**

Untuk melakukan build (sudah kami build) bisa menggunakan syntax:

**g++ -o playFair fair.cpp**

Fungsinya adalah untuk membuat playFair.exe yang nantinya akan dirun untuk menjalankan program

Kemudian untuk melakukan running program bisa menggunakan:

**./playFair -mode path**

Path adalah path dari file yang ingin di enkripsi / dekripsi Mode yang bisa dipilih adalah:

**-h atau --help**  
Mode ini digunakan untuk melihat manual penggunaan program ini

**-e atau --Enkripsi**  
Mode untuk mengenkripsikan sebuah teks sesuai dengan path file yang telah ditentukan

**-d atau --Dekripsi**  
Mode untuk mendekripsikan sebuah teks sesuai dengan path file yang telah ditentukan