LAPORAN PRAKTIKUM KRIPTOGRAFI

TUGAS 3

Disusun Oleh :

Muthia Azzahra

140810200066

UNIVERSITAS PADJADJARAN

FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM

PROGRAM STUDI TEKNIK INFORMATIKA

2022

Penjelasan Kode Program Hill Cipher

Pada program ini, terdapat beberapa fungsi yang memiliki kegunaannya masing-masing, antara lain sebagai berikut:

1. Fungsi cariDet untuk mencari determinan dari matriks, dicek terlebih dahulu jika matriks ordo 2x2 maka akan dihitung, jika != 2 maka akan invalid.
2. Fungsi cariDetInverse untuk mencari invers dari determinan matriks tersebut, dicek apakah R yang merupakan determinan != 0 jika iya maka akan di modulo dengan 26.
3. Fungsi mod untuk memodulokan rumusnya.
4. Fungsi cariInverse untuk mencari inverse matrik, menggunakan fungsi determinan dan inverse determinan lalu dicek ordo jika 2x2 maka akan dibentuk adjoin dari matrik tersebut. Lalu setelah itu akan di inverse pada rumus m_inverse[i][j] = mod26(adj[i][j] * detInverse) ;
5. Fungsi enkripsi untuk mengenkripsi plaintext, dicek dahulu apakah huruf%ordo matriks == 0 jika iya maka langsung diubah menjadi matriks dan dikalikan oleh key, jika kurang akan ditambahkan x pada bagian belakang plaintext. setelah itu di enkripsi dan ditambahkan ‘a’ agar sesuai dengan ASCII.
6. Fungsi dekripsi sama dengan enkripsi hanya menggunakan invers matriks.
7. Fungsi gcd untuk mengecek gcd harus = 1
8. Fungsi find key untuk menemukan kunci dari plaintext dicek dulu apakah gcd plaintext =1 jika tidak maka determinan tidak relatif kunci tidak dapat ditemukan.
9. Kekurangan pada program ini hanya dapat menggunakan matriks ber-ordo 2 x 2 dan huruf wajib kecil semua

Sebagai kunci global

```
int key[3][3] ;
```

Fungsi Mod

```
int mod26(int x) // fungsi untuk modulo

{
```

```
    return x >= 0 ? (x%26) : 26-(abs(x)%26) ;

}
```

Mencari determinan matriks

```
int cariDet(int m[3][3] , int n)

{

    int det;

    if(n == 2) // jika ordo matriks = 2

    {

        det = m[0][0] * m[1][1] - m[0][1]*m[1][0] ;

    }

    else det = 0 ; // invalid input

    return mod26(det);

}
```

Mencari invers matriks

```
int cariDetInverse(int R , int D = 26)
```