

Kriptografi

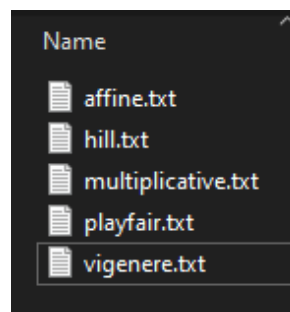
Kriptografi Klasik (Decipher)

Tugas Kelompok

- Arief Saferman (1806148656)
- Kevin Darmawan (1806148744)
- Ramadhan K.S (1806148826)
- Yogie Wisesa (1806148851)

Terdapat script Matlab bernama 'Source.m' yang kami buat untuk memudahkan cara penggunaan program ini. Program akan melihat kepada folder 'Decode' yang didalamnya terdapat file teks yang namanya telah ditentukan sebagai masukan (input) bagi program. Kunci pada setiap algoritma cipher telah di pre-defined dalam sebuah script, kita tinggal ubah kunci ini sesuai dengan kebutuhan. Program akan melakukan loop, membaca kesetiap file yang ada dalam list **FILE_DEC**. Apabila terdapat sebuah teks, maka program akan menganggap teks sebagai masukan yang telah di cipher. Kemudian program akan memanggil fungsi decipher yang sesuai dengan urutan nama file yang telah di-defined pada program.

```
1 - AFFINE = 1;  
2 - MULTIP = 2;  
3 - PLAYFAIR = 3;  
4 - HILL = 4;  
5 - VIGENERE = 5;
```



```
13 - FILE_DEC = {'Decode\affine.txt';  
14             'Decode\multiplicative.txt';  
15             'Decode\playfair.txt';  
16             'Decode\hill.txt';  
17             'Decode\vigenere.txt'};
```

```

19 -     viginereKey = 'KUNCI';
20 -     multipKey   = 11;
21 -     hillKey     = [3  7  11 13;
22 -                   4  7  5  6;
23 -                   2  21 14 9;
24 -                   3  23 21 8];
25 -     affineKey1  = 11;
26 -     affineKey2  = 13;
27 -     playfairKey = ['l', 'g', 'd', 'b', 'a';
28 -                   'q', 'm', 'h', 'e', 'c';
29 -                   'u', 'r', 'n', 'i', 'f';
30 -                   'x', 'v', 's', 'o', 'k';
31 -                   'j', 'y', 'w', 't', 'p'];

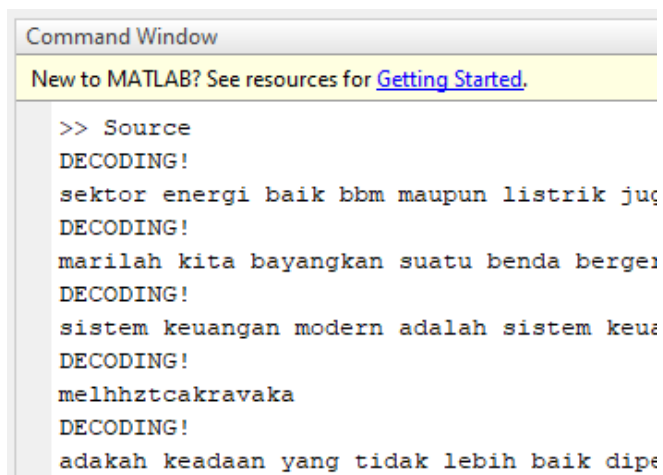
```

```

58 -     % Decoding using Decipher
59 -     for i = 1:size(FILE_DEC)
60 -         file = char(FILE_DEC(i));
61 -         text = importdata(file);
62 -         if ~(isempty(text))
63 -             fprintf('DECODING!\n');
64 -             for j = 1:size(text)
65 -                 string = char(text(j));
66 -                 switch (i)
67 -                     case AFFINE
68 -                         decipher = DecipherAffine(string, affineKey1, affineKey2);
69 -                     case MULTIP
70 -                         decipher = DecipherMultiplicative(string, multipKey);
71 -                     case PLAYFAIR
72 -                         decipher = DecipherPlayFair(string, playfairKey);
73 -                     case HILL
74 -                         decipher = DecipherHill(string, hillKey);
75 -                     case VIGENERE
76 -                         decipher = DecipherVigenere(string, viginereKey);
77 -                     end
78 -                 fprintf('%s\n', decipher);
79 -             end
80 -         end
81 -     end

```

Output:

A screenshot of the MATLAB Command Window. At the top, there is a yellow banner that says "New to MATLAB? See resources for [Getting Started](#)." Below this, the command prompt shows the user has entered the command ">> Source". The output of this command is a series of lines: "DECODING!", "sektor energi baik bbm maupun listrik juga", "DECODING!", "marilah kita bayangkan suatu benda bergerak", "DECODING!", "sistem keuangan modern adalah sistem keuangan", "DECODING!", "melihat cakrawala", "DECODING!", and "adakah keadaan yang tidak lebih baik daripada".

```
Command Window
New to MATLAB? See resources for Getting Started.
>> Source
DECODING!
sektor energi baik bbm maupun listrik juga
DECODING!
marilah kita bayangkan suatu benda bergerak
DECODING!
sistem keuangan modern adalah sistem keuangan
DECODING!
melihat cakrawala
DECODING!
adakah keadaan yang tidak lebih baik daripada
```

- Affine:

sektor energi baik bbm maupun listrik juga melakukan hal yang sama di tengah meningkatnya pemakaian bbm karena digunakan untuk transportasi mudik Pertamina tidak meminta kenaikan harga bbm masih tetap seperti sebelum Lebaran begitu juga dengan listrik meskipun banyak warga yang menyalakan TV saat Lebaran PLN tidak menaikkan harga mereka menjawab lonjakan permintaan dengan mengeluarkan stok tambahan dan juga orang-orang yang standby siap menangani gangguan

- Multiplicative:

marilah kita bayangkan suatu benda bergerak dalam galaksi Bima Sakti yang mungkin bergerak menjauhi pusat alam semesta dengan kecepatan sangat cepat apa yang terjadi dengan sinkronisasi waktu antara kita dan bintang-bintang dalam galaksi Bima Sakti atau dengan sinkronisasi waktu antara kita dengan benda-benda di sekitar ruangan kita yang relatif diam terhadap kita

- Playfair:

sistem keuangan modern adalah sistem keuangan yang didasarkan pada catatan otoritas keuangan atas nilai barang atau jasa pada transaksi yang terjadi dalam hal ini uang tidak diwakili oleh salah satu barang atau jasa itu sendiri uang juga tidak diwakili oleh nilai salah satu barang atau jasa tersebut uang adalah sekedar catatan otoritas keuangan atas nilai barang atau jasa yang ditransaksikan sistem ini dimulai saat uang dalam sistem perbankan tidak lagi dibackup dengan emas era ini dimulai pada saat Presiden AS Nixon mengambil keputusan untuk melepaskan backup emas terhadap dolar bagaimana sistem keuangan modern dan bagaimana perkembangannya akan dibahas dalam tulisan ini

- Hill:

melhhztcakravaka

- Vigenere:

adakah keadaan yang tidak lebih baik diperkenalkan oleh kehidupan agar kita menghargai keadaan lebih baik boleh jadi jawabannya adalah iya dengan cara apalagi kita bisa benarbenar mengerti keadaan lebih baik tanpa ada keadaan yang lebih buruk seandainya saja kehidupan tidak memperkenalkan keadaan lebih buruk adakah kita bisa menghargai keadaan yang lebih baik seandainya saja kehidupan tidak memperkenalkan keterbatasan bagaimanakah caranya kita memahami keagungan saat dalam peperangan justru keinginan untuk damai semakin menggebu-gebu saat kita laparlah kita akan lebih menghargai makna kenyang begitupun keberadaan suatu hal lebih buruk membuat alasan perlunya keadaan yang lebih baik

Dengan mengadopsi fungsi dari Cipher, berikut merupakan perubahan yang kami lakukan untuk membentuk fungsi Decipher.

a) Affine

Fungsi affine sebenarnya mirip dengan multiplicative yaitu hanya dikalikan namun hanya memiliki perbedaan pada rumusnya saja. Afinenya memiliki rumus cipher $f(x) = ax + b \bmod 26$ dengan kombinasi pada nilai a dan b nya sedangkan untuk deciphernya sendiri dia memiliki reverse yaitu dengan mengurangi ascii dari cipher teks dengan nilai b lalu dikalikan dengan invers dari a dan dimodulokan 26 $f(x) = (C-b) * a^{-1} \bmod 26$. Affine cipher merupakan algoritma yang sederhana digunakan pada zaman klasik (zaman enigma).

b) Multiplicative

Fungsi yang digunakan pada multiplicative cipher dan decipher sebetulnya sama. Hanya saja pada decipher kita perlu mencari inverse dari key pada modulo 26. Pada matlab kita dapat mencarinya dengan menggunakan fungsi $\text{gcd}(\text{key}, 26)$. Output kedua dari fungsi tersebut merupakan hasil inversenya dan kita cukup mengganti fungsi yang tadinya menggunakan key menjadi menggunakan inverse tersebut.

c) PlayFair

Hal yang dilakukan sama persis dengan fungsi ciphernya. Namun ini menggunakan nilai geser (shift) yang berbeda. Pada cipher, karakter jika memiliki row yang sama akan digeser kolomnya ke kanan sebanyak satu langkah. Pada decipher jika karakter memiliki row sama, kita geser kolomnya ke kiri sebanyak satu langkah. Hal ini berlaku juga pada karakter yang memiliki kolom sama.

d) Hill

Pada fungsi ini kami melakukan pengecekan yang sama seperti pada fungsi cipher. Kami harus memastikan bahwa teks memenuhi ruang matrix. Dalam penyesuaian ini, kami perlu membuat kolom matriks teks sama dengan jumlah baris matriks key. Kemudian kami memastikan bahwa matriks key dapat di inverse dengan mengecek nilai determinannya tidak sama dengan 0. Kemudian kami mencari nilai kongruen dari determinan matriks. Nilai kongruen ditandai dengan simbol 'S'.

$$\text{Det}(\text{key}) \times S = 1 \bmod 26$$

Tahap tersebut diperlukan dalam mencari inverse matriks modulo 26. Berikut merupakan cara melakukan inverse tersebut: (1) Cari nilai adjoint dari matriks key, (2)

modulo hasilnya dengan 26, (3) kalikan hasilnya dengan nilai kongruen, dan (4) modulo lagi hasilnya dengan 26. Setelah itu kami lakukan langkah seperti yang dilakukan dengan cipher yaitu mengalikan matriks teks dengan key.

e) Vigenere

Pada fungsi decipher untuk vigenere, proses yang dilakukan adalah kebalikan cipher. Pertama, cipher key dikonversi ke lowercase dan diubah ke indeks alfabet dengan -97. Lalu key akan direpetisi membentuk string sepanjang dari cipher text. Lalu algoritma akan memeriksa setiap huruf dari cipher dan key, mendekripsikan menjadi plaintext dengan mengurangi cipher dengan key dan mengoperasikan dengan modulus 26. Setelah didapatkan indeks alfabet plaintext maka hasilnya + 97 untuk mengembalikan menjadi plaintext terdekripsi.