HACKING VIGÈNERE CIPHERS

Muhammad Zabbar Falihin - 222112225
3SI2

Penjelasan

Vigenère Cipher memperluas konsep dari Substitution Cipher dengan menggunakan kunci yang terdiri dari beberapa huruf, di mana setiap huruf menentukan pergeseran untuk huruf-huruf dalam teks asli. Ini menciptakan pola enkripsi yang lebih kompleks dan sulit ditebak dibandingkan dengan Caesar Cipher. Untuk *meng-hack* Vigenère Cipher tanpa mengetahui kunci, salah satu metode yang digunakan adalah analisis frekuensi dan Kasiski Examination.

Algoritma

1. IDENTIFIKASI SEKUENS YANG BERULANG

Algoritma

1. Identifikasi Sekuens yang Berulang

Cari sekuens huruf yang berulang dalam teks terenkripsi. Jarak antara sekuens-sekuens yang sama ini bisa memberikan petunjuk tentang panjang kunci. Sekuens berulang merujuk pada pola huruf atau grup huruf yang muncul lebih dari satu kali dalam teks terenkripsi. Pencarian sekuens berulang ini merupakan bagian penting dari Kasiski Examination, sebuah metode untuk membantu menentukan panjang kunci dalam Vigenère Cipher.

Algoritma

2. KASISKI EXAMINATION

Algoritma

2. Kasiski Examination

Kasiski Examination adalah metode yang lebih spesifik untuk meng-hack Vigenère Cipher. Kasiski Examination menggunakan jarak antar sekuens berulang untuk menentukan panjang kunci yang mungkin. Ide dasarnya adalah bahwa jarak tersebut seringkali merupakan kelipatan dari panjang kunci. Kasiski Examination membantu menentukan panjang kunci, yang merupakan informasi kritikal untuk memecahkan Vigenère Cipher.

Algoritma

3. ANALISIS FREKUENSI

Algoritma

3. Analisis Frekuensi

Setelah panjang kunci diduga, teks terenkripsi dapat dibagi menjadi beberapa bagian berdasarkan panjang kunci, dan analisis frekuensi dapat diterapkan pada setiap bagian untuk menebak huruf kunci.

Algoritma

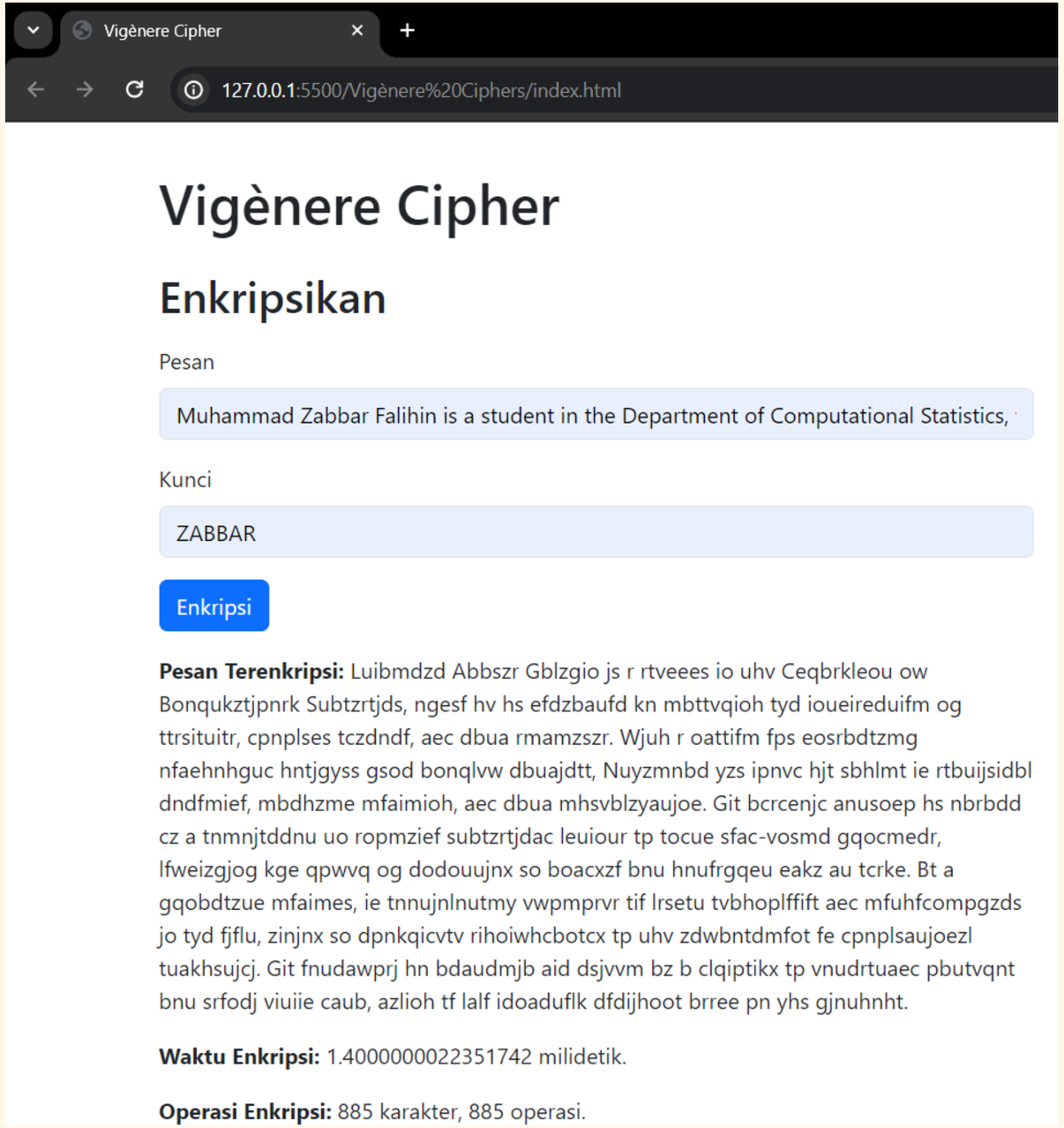
4. PERCOBAAN DAN KESALAHAN

Algoritma

4. Percobaan dan Kesalahan

Dengan menggunakan huruf-huruf kunci yang ditebak, dilakukan percobaan untuk mendekripsi teks. Ulangi proses dengan menyesuaikan tebakan sampai teks terdekripsi dengan benar terbaca.

Penggunaan


Vigènere Cipher
127.0.0.1:5500/Vigènere%20Ciphers/index.html
Vigènere Cipher
Enkripsikan
Pesan
Muhammad Zabbar Falihin is a student in the Department of Computational Statistics,
Kunci
ZABBAR
Enkripsi
Pesan Terenkripsi: Luibmdzd Abbszr Gblzgio js r rtveees io uhv Ceqbrkleou ow Bonqukztjpnrk Subtzrtjds, ngesf hv hs efdzbaufd kn mbttvqioh tyd ioueireduifm og ttrsituitr, cpnplses tczdndf, aec dbua rmamzszr. Wjuh r oattifm fps eosrbdtzmg nfaehnhguc hntjgyss gsod bonqlvw dbuajdtt, Nuyzmnbd yzs ipnvc hjt sbhlmt ie rtbuijsidbl dndfmief, mbdhzme mfaimioh, aec dbua mhsvblzyaujoe. Git bcrcenjc anusoep hs nbrbdd cz a tnmnjtddnu uo ropmzief subtzrtjdac leuiour tp tocue sfac-vosmd gqocmedr, lfweizgjog kge qpwvq og dodouujnx so boacxzf bnu hnufrgqeu eakz au tcrke. Bt a gqobdtzue mfaimes, ie tnnujnlnutmy vwpmprvr tif lrsetu tvbhoplffift aec mfuhfcompgzds jo tyd fjflu, zinjnx so dpnkqicvtv rihoiwhcbotcx tp uhv zdwbntdmfot fe cpnplsaujoezl tuakhsujcj. Git fnudawprj hn bdaudmjb aid dsjvvm bz b clqiptikx tp vnudrtuaec pbutvqnt bnu srfodj viuiie caub, azlioh tf lalf idoaduflk dfdijhoot brree pn yhs gjnuhnht.
Waktu Enkripsi: 1.4000000022351742 milidetik.
Operasi Enkripsi: 885 karakter, 885 operasi.

Penggunaan

```
def main():
    ciphertext = """Luibmdzd Abbszr Gblzgio js r rtveees io uhv Ceqbrkleou ow Bonqukztjpnrk
    Subtzrtjds, ngesf hv hs efdzbaufd kn mbttvqioh tyd ioueireduifm og ttrsituitr, cpnplses
    tczdndf, aec dbua rmamzszr. Wjuh r oattifm fps eosrbdtzmg nfaehnhguc hntjgyss gsod bonqlvw
    dbuajdtt, Nuyzmnbd yzs ipnvc hjt sbhlmt ie rtbuijsidbl dndfmief, mbdhzme mfaimioh, aec dbua
    mhsvblzyaujoe. Git bcrcenjc anusoep hs nbrbdd cz a tnmnjtddnu uo ropmzief subtzrtjdac
    leuiour tp tocue sfac-vosmd gqocmedr, lfweizgjog kge qpwvq og dodouujnx so boacxzf bnu
    hnufrgqeu eakz au tcrke. Bt a gqobdtzue mfaimes, ie tnnujnlnutmy vwpmprvr tif lrsetu
    tvbhoplffift aec mfuhfcompgzds jo tyd fjflu, zinjnx so dpnkqicvtv rihoiwhcbotcx tp uhv
    zdwbntdmfot fe cpnplsaujoezl tuakhsujcj. Git fnudawprj hn bdaudmjb aid dsjvvm bz b
    clqiptikx tp vnudrtuaec pbutvqnt bnu srfodj viuiie caub, azlioh tf lalf idoaduflk dfdijhoot
    brree pn yhs gjnuhnht."""
    hackedMessage = hackVigenere(ciphertext)

    if hackedMessage != None:
        print('Menyalin pesan yang dipecahkan ke clipboard:')
        print(hackedMessage)
        pyperclip.copy(hackedMessage)
    else:
        print('Gagal memecahkan pesan.')
```

Penggunaan

```
PROBLEMS  OUTPUT  DEBUG CONSOLE  TERMINAL  PORTS                                                    Python

PS D:\STIS\Semester 6\KSI\P5> & C:/Users/jabarfalih/AppData/Local/Programs/Python/Python312/python.exe "d:/STIS/Semester 6/KSI/P5/Hacking Vigènere Ciphers/main.py"

Hasil periksa Kasiski Examination menunjukkan kemungkinan panjang kunci: 2 3 6 4 12 8 9 16 7 14 5 10 15 11 13

Mencoba peretasan dengan panjang kunci 2 (16 kunci yang mungkin)...
Kemungkinan huruf kunci 1: Z A F N
Kemungkinan huruf kunci 2: A B G H
Mencoba dengan kunci: ZA
Mencoba dengan kunci: ZB
Mencoba dengan kunci: ZG
Mencoba dengan kunci: ZH
Mencoba dengan kunci: AA
Mencoba dengan kunci: AB
Mencoba dengan kunci: AG
Mencoba dengan kunci: AH
Mencoba dengan kunci: FA
Mencoba dengan kunci: FB
Mencoba dengan kunci: FG
Mencoba dengan kunci: FH
Mencoba dengan kunci: NA
Mencoba dengan kunci: NB
Mencoba dengan kunci: NG
Mencoba dengan kunci: NH
Mencoba peretasan dengan panjang kunci 3 (64 kunci yang mungkin)...
Kemungkinan huruf kunci 1: B D N O
Kemungkinan huruf kunci 2: A N P G
Kemungkinan huruf kunci 3: B R G H
Mencoba dengan kunci: BAB
Mencoba dengan kunci: BAR
Mencoba dengan kunci: BAG
Mencoba dengan kunci: BAH
Mencoba dengan kunci: BNB
Mencoba dengan kunci: BNR
Mencoba dengan kunci: BNG
Mencoba dengan kunci: BNH
Mencoba dengan kunci: BPB
Mencoba dengan kunci: BPR
Mencoba dengan kunci: BPG
Mencoba dengan kunci: BPH
Mencoba dengan kunci: BGB
Mencoba dengan kunci: BGR
Mencoba dengan kunci: BGG
Mencoba dengan kunci: BGH
Mencoba dengan kunci: DAB
Mencoba dengan kunci: DAR
Mencoba dengan kunci: DAG
Mencoba dengan kunci: DAH
Mencoba dengan kunci: DNB
Mencoba dengan kunci: DNR
Mencoba dengan kunci: DNG
Mencoba dengan kunci: DNH
Mencoba dengan kunci: DPB
Mencoba dengan kunci: DPR
```

Penggunaan

PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS Python

```
Mencoba dengan kunci: NAR
Mencoba dengan kunci: NAG
Mencoba dengan kunci: NAH
Mencoba dengan kunci: NNB
Mencoba dengan kunci: NNR
Mencoba dengan kunci: NNG
Mencoba dengan kunci: NNH
Mencoba dengan kunci: NPB
Mencoba dengan kunci: NPR
Mencoba dengan kunci: NPG
Mencoba dengan kunci: NPH
Mencoba dengan kunci: NGB
Mencoba dengan kunci: NGR
Mencoba dengan kunci: NGG
Mencoba dengan kunci: NGH
Mencoba dengan kunci: OAB
Mencoba dengan kunci: OAR
Mencoba dengan kunci: OAG
Mencoba dengan kunci: OAH
Mencoba dengan kunci: ONB
Mencoba dengan kunci: ONR
Mencoba dengan kunci: ONG
Mencoba dengan kunci: ONH
Mencoba dengan kunci: OPB
Mencoba dengan kunci: OPR
Mencoba dengan kunci: OPG
Mencoba dengan kunci: OPH
Mencoba dengan kunci: OGB
Mencoba dengan kunci: OGR
Mencoba dengan kunci: OGG
Mencoba dengan kunci: OGH
Mencoba peretasan dengan panjang kunci 6 (4096 kunci yang mungkin)...
Kemungkinan huruf kunci 1: Z D K O
Kemungkinan huruf kunci 2: A O L P
Kemungkinan huruf kunci 3: B A O Q
Kemungkinan huruf kunci 4: B F H M
Kemungkinan huruf kunci 5: A N P G
Kemungkinan huruf kunci 6: R G H M
Mencoba dengan kunci: ZABBAR
Kemungkinan peretasan enkripsi dengan kunci ZABBAR:
Muhammad Zabbar Falihin is a student in the Department of Computational Statistics, where he is dedicated to mastering the intersection of statistics, computer scien
ce, and data analysis. With a passi

Tekan D untuk selesai, atau tekan Enter untuk melanjutkan peretasan:
> D
Menyalin pesan yang dipecahkan ke clipboard:
Muhammad Zabbar Falihin is a student in the Department of Computational Statistics, where he is dedicated to mastering the intersection of statistics, computer scien
ce, and data analysis. With a passion for extracting meaningful insights from complex datasets, Muhammad has honed his skills in statistical modeling, machine learni
ng, and data visualization. His academic journey is marked by a commitment to applying statistical methods to solve real-world problems, leveraging the power of comp
uting to analyze and interpret data at scale. As a proactive learner, he continuously explores the latest technologies and methodologies in the field, aiming to cont
ribute significantly to the advancement of computational statistics. His endeavors in academia are driven by a curiosity to understand patterns and trends within dat
a, aiming to make impactful decisions based on his findings.
PS D:\STIS\Semester 6\KSI\P5>
```

Penjelasan Kode Program

https://github.com/zabbarfalih/ksi-pertemuan5

TERIMA KASIH