

TUGAS MINI : PERBANDINGAN PENGGUNAAN PYTHON DAN CRYPTOOOL

Dini Magmun Hariri

20123058

CAESAR CIPHER

Python

```
=== Caesar Cipher ===  
Teks Asli      : DINNENG  
Shift          : 3  
Hasil Enkripsi: GLQQHQJ  
Hasil Dekripsi: DINNENG  
  
Hasil telah disimpan ke file 'hasil_caesar_cipher.txt'
```

Cryptool

The image displays two screenshots of the Cryptool application interface, demonstrating the Caesar Cipher encryption and decryption process.

Top Screenshot (Encryption):

- Input (plaintext):** DINNENG
- Key:** 3
- Output (ciphertext):** GLQQHQJ

Bottom Screenshot (Decryption):

- Input (ciphertext):** GLQQHQJ
- Key:** 3
- Output (plaintext):** DINNENG

Analisis Perbedaan

Berdasarkan hasil percobaan, proses enkripsi dan dekripsi pada program Python menghasilkan output yang sama dengan hasil pada aplikasi Cryptool, yaitu ciphertext *GLQQHQJ* dari plaintext *DINNENG* dengan shift 3. Hal ini membuktikan bahwa implementasi algoritma Caesar Cipher pada program Python sudah sesuai dengan teori dan aplikasi perbandingan Cryptool.

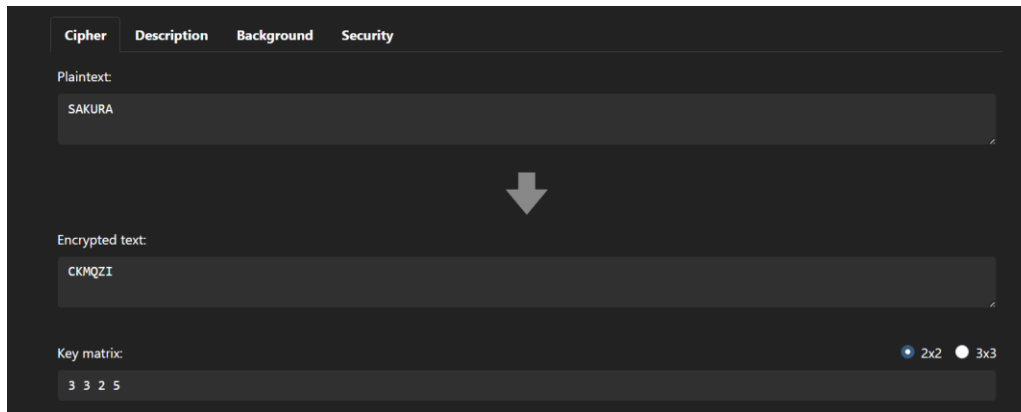
Perbedaan antara keduanya hanya terletak pada cara pelaksanaan, di mana Python membutuhkan penulisan kode dan logika pemrograman, sedangkan Cryptool menyediakan antarmuka visual yang mempermudah pengguna dalam melakukan enkripsi dan dekripsi tanpa harus menulis program. Dengan demikian, kesamaan hasil dari kedua implementasi ini membuktikan konsistensi dan validitas algoritma Caesar Cipher yang digunakan.

HILL CIPHER

Python

```
Plaintext : SAKURA  
Ciphertext: CKMQZI  
Dekripsi  : SAKURA
```

Cryptool



Analisis Perbedaan

Berdasarkan hasil implementasi Hill Cipher, teks asli “SAKURA” berhasil dienkripsi menjadi “CKMQZI” menggunakan matriks kunci berukuran 2x2 dengan nilai kunci [3 3; 2 5]. Proses enkripsi dilakukan dengan mengubah setiap huruf menjadi nilai numerik (A=0, B=1, ..., Z=25), kemudian dikalikan dengan matriks kunci dan dihitung menggunakan mod 26 untuk menghasilkan ciphertext.

Proses dekripsi dilakukan dengan menggunakan inverse matrix dari kunci yang sama, dan hasilnya menunjukkan bahwa ciphertext berhasil dikembalikan menjadi plaintext “SAKURA” secara utuh. Hal ini membuktikan bahwa algoritma Hill Cipher bekerja dengan baik dalam proses enkripsi dan dekripsi, asalkan matriks kunci yang digunakan memiliki invers modulo 26.

KESIMPULAN

Berdasarkan hasil percobaan yang dilakukan menggunakan Python dan CrypTool pada algoritma Caesar Cipher dan Hill Cipher, dapat disimpulkan bahwa kedua alat tersebut menghasilkan output yang sama dan konsisten sesuai dengan teori kriptografi klasik.

Pada Caesar Cipher, baik Python maupun CrypTool berhasil mengenkripsi plaintext *DINNENG* menjadi ciphertext *GLQQHQJ* dengan shift 3, serta mendekripsinya kembali tanpa kesalahan.

Sementara pada Hill Cipher, teks *SAKURA* berhasil dienkripsi menjadi *CKMQZI* dan didekripsi kembali dengan benar menggunakan matriks kunci $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$.

Perbedaan utama antara keduanya terletak pada cara penggunaan:

- Python memerlukan pemahaman logika pemrograman dan implementasi algoritma secara manual.
- CrypTool menyediakan antarmuka grafis yang memudahkan pengguna memahami konsep enkripsi dan dekripsi secara visual.

Dengan demikian, dapat disimpulkan bahwa kedua alat ini sama-sama valid dan akurat dalam menerapkan algoritma kriptografi klasik, namun memiliki perbedaan dalam pendekatan penggunaannya—Python unggul untuk otomasi dan pengembangan, sedangkan CrypTool lebih efektif untuk pembelajaran dan visualisasi konsep kriptografi.

Link Github

<https://github.com/dinimh/KRIPTOGRAFI>