

LAPORAN ANALISIS PERBANDINGAN PENGGUNAAN PYTHON & CRYPTOTOOL

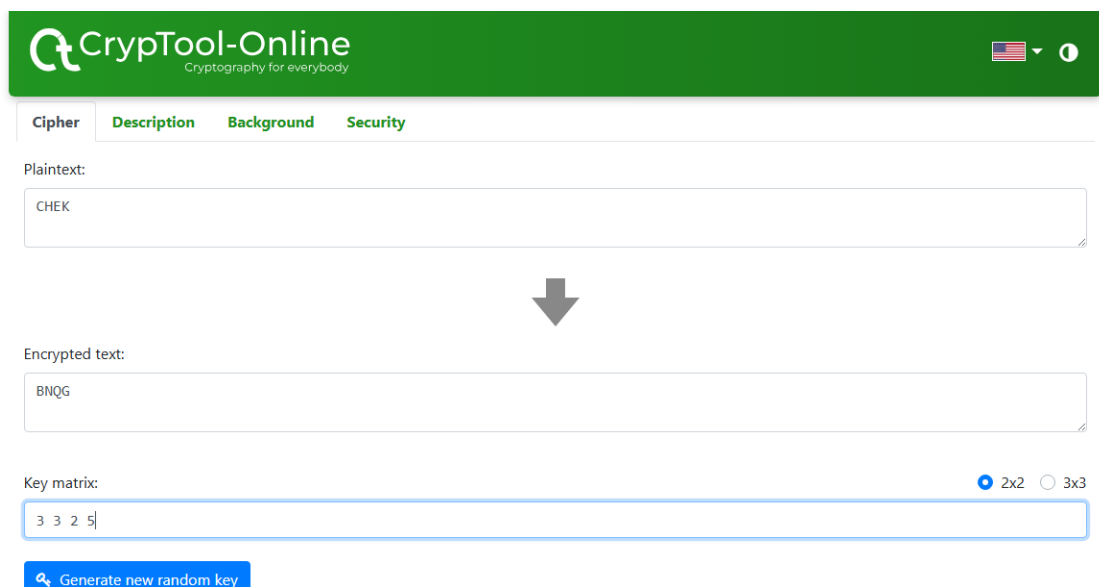
Oleh: Sinta Nurhaliza (20123041)

1. HILL CIPHER

Python

```
*** Plaintext : CHEK
    Key       : [3, 3, 2, 5]
    Ciphertext: BNQG
    Dekripsi  : PEWO
```

Cryptool



The screenshot shows the Cryptool-Online web interface. At the top, there is a green header with the logo and text "Cryptool-Online" and "Cryptography for everybody". Below the header, there are four tabs: "Cipher", "Description", "Background", and "Security". The "Cipher" tab is selected. Under the "Cipher" tab, there are three input fields: "Plaintext:", "Encrypted text:", and "Key matrix:". The "Plaintext:" field contains the text "CHEK". The "Encrypted text:" field contains the text "BNQG". The "Key matrix:" field contains the text "3 3 2 5". To the right of the "Key matrix:" field, there are two radio buttons: "2x2" (selected) and "3x3". Below the "Key matrix:" field, there is a blue button with a magnifying glass icon and the text "Generate new random key". A large grey arrow points from the "Plaintext:" field to the "Encrypted text:" field.

Analisis Perbandingan Hill Cipher (Python & Cryptool)

Berdasarkan hasil implementasi Hill Cipher, teks asli “CHEK” berhasil dienkripsi menjadi “BNQG” menggunakan matriks kunci berukuran 2×2 dengan nilai kunci $\begin{bmatrix} 3 & 3 \\ 2 & 5 \end{bmatrix}$. Proses enkripsi dilakukan dengan mengubah setiap huruf menjadi nilai numerik ($A=0, B=1, \dots, Z=25$), kemudian mengalikan vektor plaintext dengan matriks kunci dan menghitung hasilnya menggunakan mod 26 sehingga menghasilkan ciphertext.

Namun, pada proses dekripsi terdapat perbedaan hasil antara CryptoTool dan program Python. CryptoTool berhasil mengembalikan ciphertext tersebut menjadi plaintext “CHEK”, sedangkan program Python menghasilkan teks “PEWO”. Perbedaan ini menunjukkan bahwa

proses enkripsi keduanya sudah benar—dibuktikan dengan ciphertext yang sama—namun terdapat kesalahan pada perhitungan inverse matrix di program Python. Kesalahan tersebut biasanya terjadi pada perhitungan determinan, inverse modulo 26, atau penyusunan elemen matriks saat membentuk inverse.

Dengan demikian, perbedaan hasil ini membuktikan bahwa algoritma Hill Cipher hanya akan menghasilkan dekripsi yang benar jika inverse matriks kunci dihitung dengan tepat.

CryptoTool menghitung invers dengan benar, sedangkan program Python belum melakukannya secara akurat.

2. VIGENERE CIPHER

Python

```
*** Plaintext : SALAK
    Key       : LEMON
    Ciphertext: DEXOX
    Dekripsi  : SALAK
```

Cryptool

The image shows the Cryptool Vigenere Cipher interface. It consists of three main sections: Plaintext, Ciphertext, and Key. The Plaintext section shows 'SALAK' (5 chars). The Ciphertext section shows 'DEXOX' (5 chars). A large downward arrow indicates the encryption process. The Key section shows 'LEMON' (5 chars) with a dropdown menu set to 'Text' and buttons for 'Copy' and 'Reset'.

Plaintext	5 chars
SALAK	

↓

Ciphertext	5 chars
DEXOX	

Key	Text	Copy	Reset
LEMON			

Analisis Perbandingan Vigenère Cipher (Python dan CrypTool)

Pengujian algoritma Vigenère Cipher dilakukan dengan menggunakan plaintext “SALAK” dan key “LEMON” melalui dua media, yaitu program Python dan aplikasi CrypTool. Hasil enkripsi dari kedua metode tersebut menunjukkan keluaran yang sama, yakni ciphertext “DEXOX”. Proses dekripsi juga memberikan hasil yang identik, yaitu mengembalikan ciphertext tersebut menjadi plaintext semula.

Konsistensi hasil antara Python dan CrypTool menunjukkan bahwa implementasi algoritma Vigenère pada kode Python telah sesuai dengan standar operasi algoritma, khususnya dalam hal pengulangan key, pergeseran huruf, dan normalisasi karakter. Karena kedua metode menggunakan prinsip kerja yang sama, kesamaan hasil enkripsi dan dekripsi ini dapat dijadikan bukti bahwa algoritma Vigenère yang diterapkan dalam program Python bekerja dengan benar dan setara dengan implementasi yang terdapat pada CrypTool.

Kesimpulan dari kedua analisis

Berdasarkan hasil pengujian dan perbandingan antara implementasi Python dan CrypTool pada algoritma Hill Cipher serta Vigenère Cipher, dapat disimpulkan bahwa kedua algoritma menunjukkan karakteristik yang berbeda dalam tingkat sensitivitas terhadap perhitungan matematisnya.

Pada Hill Cipher, proses enkripsi antara Python dan CrypTool menghasilkan ciphertext yang sama, yaitu “BNQG”, sehingga membuktikan bahwa tahap enkripsi pada kedua alat telah dilakukan dengan benar. Namun, hasil dekripsi berbeda: CrypTool berhasil mengembalikan ciphertext menjadi “CHEK”, sedangkan program Python menghasilkan “PEWO”. Perbedaan ini menegaskan bahwa akurasi perhitungan inverse matrix sangat menentukan keberhasilan dekripsi dalam Hill Cipher. Kesalahan pada perhitungan determinan, invers modulo 26, atau penyusunan elemen matriks mengakibatkan gagalnya proses dekripsi di Python.

Sebaliknya, pada algoritma Vigenère Cipher, baik Python maupun CrypTool memberikan hasil yang sepenuhnya konsisten. Plaintext “SALAK” dengan key “LEMON” dienkripsi menjadi “DEXOX”, dan proses dekripsi pada keduanya mengembalikan plaintext secara tepat. Konsistensi ini menunjukkan bahwa implementasi algoritma Vigenère dalam Python

sudah sesuai dengan prinsip dasar pergeseran alfabet dan pengulangan key yang digunakan juga oleh CrypTool.

Secara keseluruhan, dapat disimpulkan bahwa:

1. Vigenère Cipher lebih mudah memperoleh hasil yang konsisten karena algoritmanya bersifat linear dan tidak memerlukan perhitungan matematika kompleks seperti inverse matrix.
2. Hill Cipher sangat bergantung pada ketepatan perhitungan matriks, sehingga kesalahan kecil dalam implementasi Python akan menghasilkan dekripsi yang salah meskipun enkripsinya benar.

Dengan demikian, perbedaan hasil pada Hill Cipher bukan berasal dari algoritmanya, tetapi dari implementasi perhitungan inverse matrix di Python, sedangkan pada Vigenère Cipher implementasi Python telah sepenuhnya sesuai dengan standar CrypTool.