

## **LAPORAN STUDI KASUS MINI**

Laporan ini dibuat untuk memenuhi tugas Studi Kasus Mini pada Mata Kuliah  
Kriptografi dengan Dosen Pengampu Kodrat Mahatma, S.T., M.Kom



Disusun Oleh :  
Amanda Aulia Nurani (20123043)

**C1.23 S1 INFORMATIKA**  
**UNIVERSITAS TEKNOLOGI DIGITAL**  
**2025**

## SOAL

### Studi Kasus Mini

- Gunakan teks 'HELLO WORLD' untuk uji Hill + Playfair.
- Boleh juga kata yang lain. Kalau bisa interaktif, sehingga teks bisa diubah
- Bandingkan dengan hasil dari CrypTool atau CyberChef

#### Praktikum Mandiri

1. Jalankan Hill Cipher di CrypTool
2. Bandingkan hasil dengan hasil di Python
3. Catat perbedaan jika ada

### ANALISIS HASIL HILL CIPHER (PYTHON DAN CRYPTOTool)

#### 1. Deskripsi Percobaan

Percobaan dilakukan menggunakan algoritma Hill Cipher dengan ukuran matriks kunci **2x2** dan nilai **key matrix (3, 3, 2, 5)**. Teks yang digunakan sebagai plaintext adalah "**HELLO WORD**".

Percobaan dilakukan dengan dua alat, yaitu :

- 1) Program Python hasil implementasi manual Hill Cipher.
- 2) Aplikasi Cryptool 2 sebagai pembanding hasil.

#### 2. Hasil dari Program Python

Karena pada program Python terdapat perintah untuk menghapus spasi (`replace(" ", "")`), maka teks yang digunakan dalam proses enkripsi menjadi "**HELLOWORD**".

```
PROBLEMS OUTPUT DEBUG CONSOLE TERMINAL PORTS

PS D:\SEMESTER 5\KRIPTOGRAFI\TUGAS\TUGAS BESAR 1> & C:/Users/Lenovo/AppData/Roaming/Microsoft/Windows/Start Menu/Programs/Python 3.8/Hill Cipher.py
Masukkan teks: HELLOWORLD
Masukkan ukuran matriks key (contoh: 2 untuk 2x2, 3 untuk 3x3): 2
Masukkan 4 elemen key matrix (pisahkan dengan spasi): 3 3 2 5

 Key valid! Lanjut ke proses enkripsi & dekripsi...

===== HASIL =====
Plaintext : HELLOWORLD
Key Matrix:
[[3 3]
 [2 5]]
Encrypt : HIOZEIPJAR
Decrypt : HELLOWORDX
```

Huruf ‘X’ pada hasil deskripsi ditambahkan secara otomatis sebagai padding karena Panjang teks tidak genap dengan ukuran matriks kunci (2 karakter per blok).

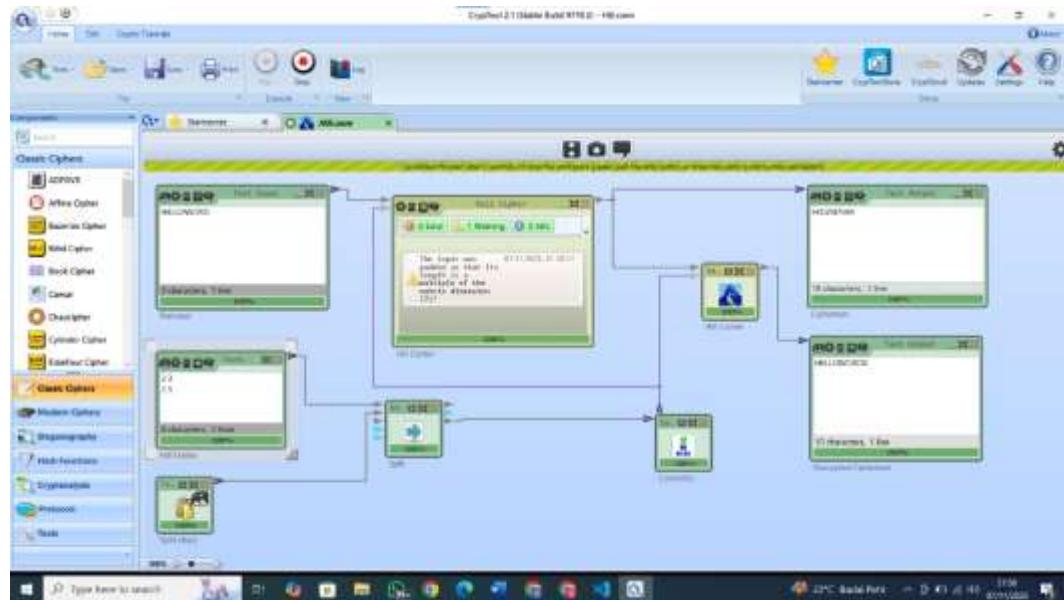
### 3. Hasil dari Cryptool

Pada Cryptool, Ketika plaintext dimasukan dengan spasi “HELLO WORD”, proses enkripsi menampilkan error dan tidak menghasilkan keluaran (output).



Hal ini disebabkan karena Cryptool menganggap spasi bukan bagian dari alfabet yang valid untuk perhitungan matriks, sedangkan Hill Cipher hanya mendukung huruf A-Z (tanpa spasi, angka, dan symbol).

Namun, Ketika spasi dihapus dan teks diubah menjadi “HELLOWORD”, hasil yang diperoleh sama dengan program Python.



#### 4. Analisis Perbedaan

Aspek	Program Python	Cryptool
Penanganan Spasi	Spasi dihapus otomatis oleh program	Tidak dapat memproses spasi (error)
Padding (penambahan huruf X)	Otomatis ditambahkan jika panjang teks ganjil	Ditambahkan otomatis oleh system Cryptool
Alfabet yang digunakan	A-Z (dikonversi ke angka 0-25)	A-Z (tidak mendukung karakter lain)
Hasil Enkripsi	Sama (HIOZEIPJAR)	Sama (HIOZEIPJAR)
Hasil Deskripsi	HELLOWORDX	HELLOWORDX

#### 5. Kesimpulan

Berdasarkan hasil percobaan, dapat disimpulkan bahwa :

- 1) Hill Cipher tidak mendukung karakter spasi, sehingga plaintext harus berupa huruf kapital tanpa pemisah.
- 2) Perbedaan utama antara Python dan Cryptool terletak pada penanganan input dengan spasi, Python menghapusnya otomatis, sedangkan Cryptool menolak input tersebut.
- 3) Proses enkripsi dan deskripsi menghasilkan output yang identik jika plaintext dan key matrix sama.

- 4) Penambahan huruf padding seperti “X” merupakan hal wajar untuk menyesuaikan Panjang teks dengan ukuran blok Hill Cipher.

## **ANALISIS HASIL PLAYFAIR CIPHER (PYTHON DAN CRYPTOOL)**

### **1. Deskripsi Algoritma**

Playfair Cipher merupakan salah satu algoritma klasik berbasis substitusi digraf (dua huruf sekaligus).

Berbeda dengan Caesar atau Vigenère yang mengenkripsi satu huruf per langkah, Playfair Cipher bekerja dengan cara membagi teks menjadi pasangan huruf (digraph).

Langkah umumnya adalah sebagai berikut:

- 1) Membuat matriks 5x5 berdasarkan keyword (huruf tidak boleh duplikat).
  - Huruf J digabungkan dengan I.
  - Huruf alfabet selain itu diisi secara berurutan.
- 2) Plaintext diubah menjadi huruf kapital dan dibersihkan dari spasi.
- 3) Jika ada dua huruf yang sama dalam satu pasangan, maka huruf kedua diganti X.
- 4) Jika jumlah huruf ganjil, maka ditambahkan huruf X di akhir.
- 5) Enkripsi dilakukan berdasarkan posisi huruf di matriks:
  - Jika satu baris, geser ke kanan.
  - Jika satu kolom, geser ke bawah.
  - Jika berbeda baris dan kolom, ambil huruf di sudut persegi panjang yang dibentuk.
- 6) Dekripsi dilakukan dengan arah berlawanan dari proses enkripsi.

## 2. Hasil dari Python

```
PS D:\SEMESTER 5\KRIPTOGRAFI\TUGAS\TUGAS BESAR 1> & C:/Users/Lenovo/ARAFI/TUGAS/TUGAS BESAR 1/Playfair Cipher.py"
Masukkan teks: HELLO WORD
Masukkan key: KEYWORD

MATRIX KEY      : KEYWORD

K E Y W O
R D A B C
F G H I L
M N P Q S
T U V X Z

===== HASIL =====
Plaintext       : HELXLOWORD
Key             : KEYWORD
Encrypt         : GYIZSCOKDA
Decrypt         : HELXLOWORD
```

Penjelasan hasil :

- 1) Teks asli “HELLO WORD” diubah menjadi HELXLOWORD karena terdapat huruf ganda LL menjadi LX.
- 2) Huruf “J” (jika ada) otomatis diganti dengan “I”, namun pada teks ini tidak terdapat huruf J.
- 3) Enkripsi menghasilkan ciphertext GYIZSCOKDA.
- 4) Hasil deskripsi mengembalikan plaintext yang sama yaitu HELXLOWORD.

### 3. Hasil dari Cryptool



Penjelasan hasil :

- 1) Cryptool juga otomatis mengonversi plaintext menjadi HELXLOWORD, sama seperti Python.
- 2) Ciphertext yang dihasilkan identic GYIZSCOKDA
- 3) Struktur cipher key yang terbentuk pun sama (25 huruf unik, tanpa J)

### 4. Analisis Perbedaan

Aspek	Python	Cryptool
Plaintext Input	HELLOWORLD	HELLOWORLD
Plaintext Terformat	HELXLOWORD	HELXLOWORD
Key	KEYWORD	KEYWORD
Ciphertext	GYIZSCOKDA	GYIZSCOKDA
Decrypt Result	HELXLOWORD	HELXLOWORD
Penanganan Spasi	Diabaikan (bisa tanpa error)	Diabaikan (bisa tanpa error)
Huruf Ganda	LX (X disisipkan)	LX (X disisipkan)
Huruf "J"	Diganti "I"	Diganti "I"

### 5. Kesimpulan

Berdasarkan hasil percobaan, dapat disimpulkan bahwa :

- 1) Implementasi Playfair Cipher di Python dan Cryptool menghasilkan hasil enkripsi dan deskripsi yang identik.

- 2) Keduanya mampu memproses teks yang mengandung spasi tanpa error, karena spasi diabaikan sebelum proses enkripsi.
- 3) Mekanisme pengolahan teks (penggantian huruf J, penyisipan X, dan pembentukan matriks kunci) sama persis di kedua system.