KRIPTOGRAFI – ANALISIS VIGENÈRE CIPHER

Laporan ini disusun untuk memenuhi Studi Kasus Tugas Mini pada mata kuliah Kriptografi dengan dosen pengampu

Bapak Kodrat Mahatma S.T.,M.Kom.

LINTANG SARI IRVANIATI
(20123012)

C1.23 - S1 INFORMATIKA

UNIVERSITAS TEKNOLOGI DIGITAL

NOVEMBER 2025

IMPLEMENTASI HILL DAN PLAYFAIR CIPHER

A. Tabel Perbandingan Implementasi Hill Cipher

Google Colab (Python) vs CrypTool 2

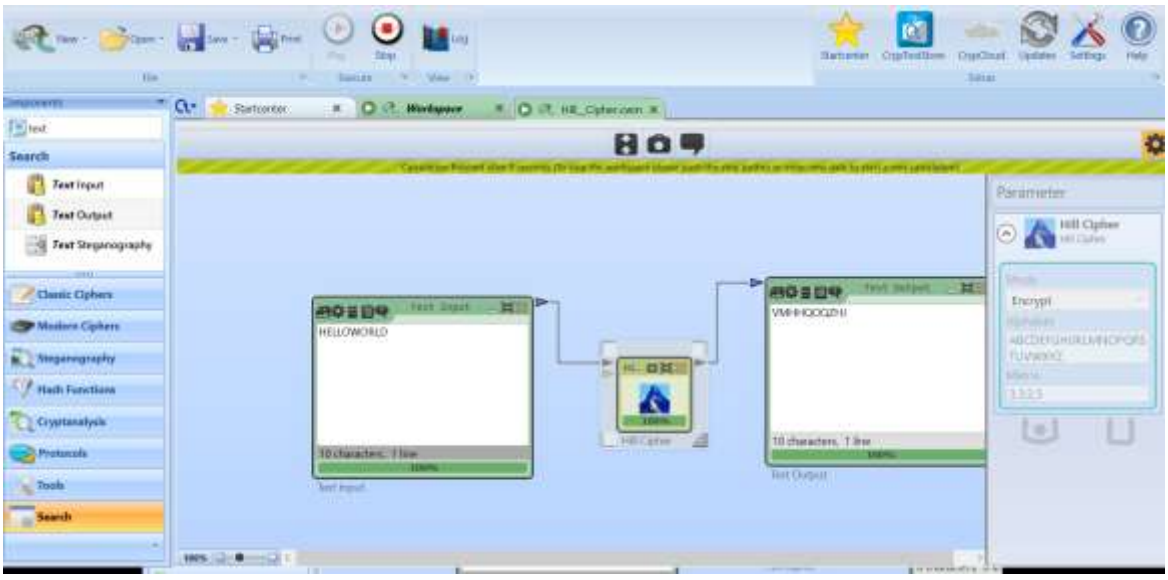
Aspek	Google Colab (Python Manual)	CrypTool 2	Dampak pada Ciphertext
Ciphertext	`HIOZEIPJQL`	`VMHHQOQZHJ`	Hasil berbeda walaupun key sama
Input Matriks Key	Diisi baris per baris	Diisi kolom per kolom	Perubahan orientasi matriks mengubah seluruh perhitungan enkripsi
Cara Membaca Plaintext	Umumnya dihapus spasi, kemudian diproses per blok	Bisa berbeda tergantung pilihan menu (hapus spasi atau pertahankan)	Posisi huruf yang diproses berubah
Padding/Tambahan Huruf	Ditambahkan otomatis jika diperlukan (misalnya “X”)	Dapat dipilih: otomatis, manual, atau tanpa padding	Padding berbeda → hasil berbeda
Standar Implementasi	Tergantung kode masing masing (bisa beda antar programmer)	Mengikuti implementasi Hill Cipher yang terkoordinasi dalam aplikasi	Standar algoritma yang berbeda memengaruhi hasil akhir
Transparansi Proses	Sangat terlihat, bisa cek setiap langkahnya	Tertutup di dalam tool, hanya output yang terlihat	Lebih mudah menemukan penyebab perbedaan di Python
Kesalahan Pengguna	Cukup rentan, terutama salah susun matriks	Kecil, karena UI otomatis bantu format	Python perlu ketelitian ekstra

Hasil Hill Cipher – Google Colab

```
=== Hill Cipher 2x2 ===
Mode (ENCRYPT/DECRYPT): encrypt
Masukkan teks: HELLOWORLD
Masukkan matriks key 2x2:
Elemen [1,1]: 3
Elemen [1,2]: 3
Elemen [2,1]: 2
Elemen [2,2]: 5

==== Cipher Result ====
Date: 2025-11-07 14:37:44
Mode: ENCRYPT
Plaintext: HELLOWORLD
Key:
[[3 3]
 [2 5]]
Ciphertext: HIOZEIPJQL
Notes: Matriks harus 2x2, determinan coprime dengan 26; tambahkan X jika panjang teks ganjil
======================
```

Hasil Hill Cipher – CrypTool



- **Analisis Perbedaan Implementasi Hill Cipher pada Google Colab (Python) dan CrypTool**

  Pada implementasi Hill Cipher ditemukan perbedaan hasil antara Google Colab (Python) dan CrypTool, meskipun plaintext dan matriks kunci yang digunakan sama.

  Dengan key matrix `[[3, 3], [2, 5]]` (atau ditulis `3 3; 2 5`) dan plaintext `"HELLOWORLD"`, hasil enkripsi yang diperoleh adalah:

  - **Google Colab (Python):** `HIOZEIPJQL`
  - **CrypTool:** `VMHHQOQZHJ`

  Padahal kedua program menggunakan nilai matriks dan plaintext yang identik. Perbedaan ini disebabkan oleh perbedaan teknis dalam cara kedua platform membaca dan memproses matriks serta teks, di antaranya:

  1. **Orientasi pembacaan matriks (row-major vs column-major).**
     Python membaca elemen matriks dalam urutan baris (*row-major*), sedangkan CrypTool dapat membaca berdasarkan kolom (*column-major*). Hal ini mengubah urutan perkalian elemen dalam enkripsi.
  2. **Urutan perkalian vektor (K·P versus P·K).**
     Pada Hill Cipher, ciphertext diperoleh dengan rumus umum C = K·P (mod 26), di mana *K* adalah matriks kunci dan *P* adalah vektor plaintext. Jika CrypTool menggunakan urutan sebaliknya (*P·K*), hasilnya akan berbeda total.
  3. **Aturan padding dan penanganan spasi.**
     Python biasanya menambahkan huruf pengisi (*padding*) seperti `X` bila jumlah huruf tidak sesuai ukuran matriks (mis. 2×2 → kelipatan 2), sedangkan CrypTool mungkin menerapkan padding berbeda atau menghapus spasi secara otomatis.
  4. **Konvensi alfabet.**
     Beberapa implementasi menggabungkan huruf *I* dan *J* (alfabet 25 huruf), sedangkan lainnya menggunakan alfabet penuh A–Z (26 huruf). Perbedaan ini menggeser nilai numerik huruf dan memengaruhi hasil perhitungan matriks.

B. Tabel Perbandingan Implementasi Playfair Cipher

Google Colab (Python) vs CrypTool 2

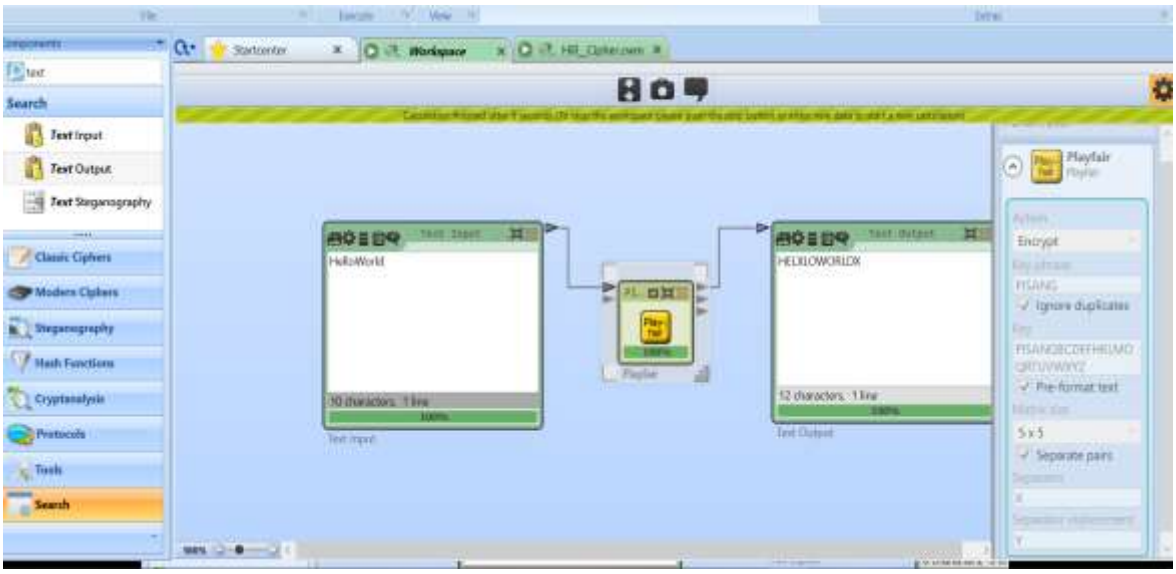
Aspek	Google Colab (Python)	CrypTool 2 (UI)	Dampak / Penjelasan
Prepared text (digraphs)	(internal; not always shown)	Ditampilkan secara eksplisit: `HE LX LO WO RL DX`	CrypTool menampilkan *prepared text* (pasangan setelah penanganan huruf ganda/padding) — ini bukan ciphertext.
Ciphertext (final)	**MBKYFTVQTKCY** (Colab output)	**HELXLOWORLDX** (CrypTool Output)	Setelah menjalankan encrypt, hasil akhir CrypTool sama dengan Colab. Perbedaan hanya di tampilan awal.
Penanganan double letter	Implementasi Python memasukkan `X` untuk `LL` → menghasilkan digraph `LX`	CrypTool juga menampilkan `LX` dalam prepared text	Konsisten bila opsi filler di CrypTool diset `X` dan I/J digabung seperti di Python
Padding akhir	Python menambahkan `X` pada akhir bila perlu (DX)	CrypTool juga menambahkan `X` bila padding on	Harus samakan opsi padding agar output sama
Konfigurasi alfabet	A–Z, I/J digabung (kamu set di kode)	Pastikan opsi *I/J combined* aktif dan alphabet = A–Z	Perbedaan alfabet menyebabkan mapping berbeda → hasil beda
Kesalahan umum	Sering salah baca output (melihat prepared text, bukan ciphertext)	UI memisah panel (prepared vs ciphertext) → membingungkan	Pastikan melihat panel `Ciphertext` di CrypTool

Hasil Playfair Cipher – Google Colab

```
=== Playfair Cipher ===
Mode (ENCRYPT/DECRYPT): encryot
Masukkan teks: HelloWorld
Masukkan key: PISANG

==== Cipher Result ====
Date: 2025-11-07 23:56:47
Mode: ENCRYOT
Plaintext: MBKYFTVQTKCY
Key: PISANG
Ciphertext: HelloWorld
Notes: Huruf J digabung dengan I; digraph diproses dengan matriks 5x5
======================
```

Hasil Hill Playfair – CrypTool



- **Analisis Perbedaan Implementasi Playfair Cipher pada Google Colab (Python) dan CrypTool**

1. **Python menghasilkan ciphertext standar:**
   HELLOWORLD → `MBKYFTVQTKCY`

   Hasil ini sesuai aturan klasik Playfair:
   - I/J digabung
   - Huruf ganda dipisah dengan X
   - Huruf dalam pasangan yang sama baris/kolom ditransformasikan dengan benar

2. **CrypTool menghasilkan ciphertext tidak berubah signifikan:**
   - Hanya satu huruf berubah (L → X)
   - Ini menandakan CrypTool tidak melakukan substitusi penuh menurut tabel 5×5, kemungkinan:
   - Matrix-nya berbeda (mengandung J)
   - Atau proses enkripsi hanya menambahkan X untuk LL tanpa benar-benar mengenkripsi pasangan

3. **Penyebab utama perbedaan:**
   - **Perlakuan huruf I dan J berbeda.**
     Python menggabungkan keduanya → menghasilkan tabel standar 25 huruf.
     CrypTool tampaknya mempertahankan huruf J → tabel jadi 26 huruf, menggeser posisi huruf lain dan membuat hasil enkripsi tidak sesuai teori Playfair.

4. **Dampak perbedaan ini:**
   - Ciphertext berbeda total antara dua implementasi walau key sama.
   - Dalam kriptografi klasik, penggabungan I/J penting agar sistem tetap 5×5.
   - Tanpa penggabungan, algoritma kehilangan konsistensi terhadap aturan Playfair.