**Laporan Implementasi Lima Algoritma Kriptografi Klasik**

Dosen pengampu: Kodrat Mahatma

A blue and red logo

AI-generated content may be incorrect.

Disusun oleh :

Kelompok 8

Khabibah Wiendie Zahra (20123073)

Marshelindo Rizkina Ardhyansyah (20123080)

**PROGRAM STUDI INDFORMATIKA**

**UNIVERSITAS TEKNOLOGI DIGITAL BANDUNG**

**2025**

1. **Mekanisme dan Implementasi kode**
2. **Affine Cipher**

* **Mekanisme :** Menggunakan dua kunci dalam fungsi linier. Ini secara signifikan meningkatkan keragaman pemetaan awal dibandingkan Caesar.
* **Fungsi Kunci** : Pasangan kunci (a, b), di mana a adalah pengali dan b adalah pergeseran.

Syarat Mutlak: a harus koprima (GCD(a, 26) = 1) agar invers perkalian modular a{-1} ada. Ini menjamin dekripsi dapat dibalik.

* **Rumus matematis :**



* **Implementasi kode :**

A screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of text

AI-generated content may be incorrect.

* **Hasil Output :**

A black screen with white text

AI-generated content may be incorrect.

1. **Caesar Cipher**

* **Mekanisme :** Sandi ini adalah kasus khusus dari substitusi monoalfabetik. Setiap huruf digeser sejauh n posisi.
* **Fungsi Kunci** : shift (geseran tunggal, 1 < shift > 25).
* **Rumus matematis :**
* ****
* **Implentasi kode :**

A screen shot of a computer program

AI-generated content may be incorrect.

* **Hasil Output :**

A black background with white text

AI-generated content may be incorrect.

1. **Vigenere Chiper (sandi kunci berulang)**

* **Mekanisme :** Sandi ini menggunakan *banyak alfabet* pengganti yang berbeda, ditentukan oleh huruf pada kata kunci ($K$) yang diulang-ulang (perluasan kunci). Ini berhasil menyembunyikan pola frekuensi huruf secara langsung.
* **Fungsi Kunci** : Kata kunci K = k1, k2, …, kL.
* **Rumus matematis :**



* **Implentasi kode :**

A screen shot of a computer program

AI-generated content may be incorrect.

A computer screen shot of text

AI-generated content may be incorrect.

* **Hasil Output :**

A screen shot of a computer

AI-generated content may be incorrect.

1. **Playfair Cipher**

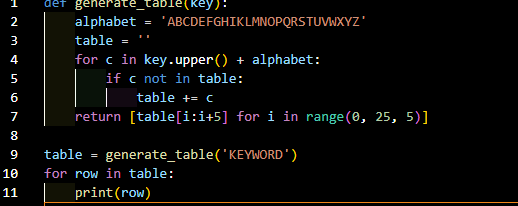
* **Mekanisme:** Playfair Cipher merupakan **cipher digraph substitusi**, artinya mengenkripsi **dua huruf sekaligus (pasangan huruf)** menggunakan **matriks kunci berukuran 5×5**.

Langkah-langkah utama:

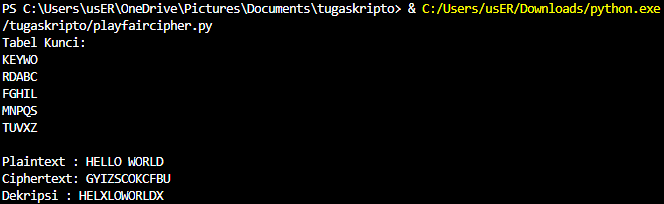
* Membentuk tabel kunci (key table) berukuran 5×5 dari kata kunci (key).
  + Huruf “J” digabung dengan “I” (jadi hanya 25 huruf).
  + Huruf yang berulang diabaikan.
* Membagi plaintext menjadi pasangan dua huruf (bigram).
  + Jika ada huruf ganda (seperti “LL”), sisipkan huruf X di antara mereka.
  + Jika jumlah huruf ganjil, tambahkan X di akhir.
* Mengenkripsi setiap pasangan berdasarkan posisi kedua huruf di tabel.
* **Aturan Enkripsi:**

| **Kondisi Huruf** | **Aturan Enkripsi** | **Penjelasan** |
| --- | --- | --- |
| **Sebaris** | Geser ke kanan satu kolom | Jika di ujung kanan, kembali ke awal baris |
| **Sekolom** | Geser ke bawah satu baris | Jika di bawah, kembali ke atas kolom |
| **Membentuk persegi** | Tukar kolom antar huruf | Bentuk persegi imajiner, ambil huruf di sudut lainnya |

* **Implementasi kode:**



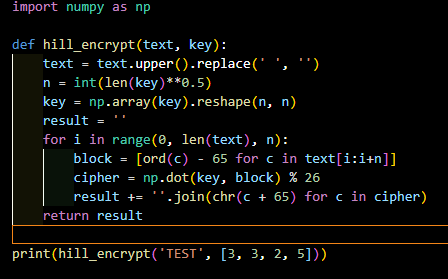
* Hasil Output:



1. **Hill Cipher**

* **Mekanisme**: Hill Cipher adalah algoritma **cipher polialfabetik blok**, yang mengenkripsi plaintext dalam bentuk **kelompok huruf (blok)** menggunakan **operasi matriks linear** di bawah **modulo 26**.
* Kunci pada Hill Cipher berbentuk **matriks bujur sangkar (n × n)** yang berisi bilangan bulat (biasanya hasil konversi dari huruf A–Z → 0–25).
* Fungsi key: Kunci (key) direpresentasikan dalam bentuk **matriks persegi**, contohnya untuk kunci 2×2:
* **Rumus matematis:**



* **Implementasi kode:**
* 
* Hasil Output:



**II. Analisis kuantitatif dan keamanan**

Tingkat keamanan sandi klasik berbanding lurus dengan ruang kunci (keyspace) dan kerentenannya terhadap metode serangan statistika

| **Sandi** | **Ruang Kunci (K)** | **Dasar Kerentanan** | **Keamanan Relatif** |
| --- | --- | --- | --- |
| Caesar | 25 | Jumlah alfabet & K kecil | Sangat Rendah (Pecah Instan) |
| Affine | 312 | K kecil & mudah ditebak | Rendah (Cepat Pecah) |
| Vigenère | Bergantung panjang kunci (misal 26^L) | Kunci pendek & pengulangan | Sedang dengan Kriptanalisis Lanjutan |
| Playfair | 25! (faktor dari 25 huruf unik) | Digram berulang & analisis frekuensi | Sedang (Sulit dipecahkan tanpa konteks) |
| Hill | Bergantung ukuran matriks (misal 2×2: 26⁴) | Matriks dapat dibalik & rentan terhadap analisis linear | Sedang–Tinggi (Tergantung ukuran matriks) |

**III. Analisis Kelemhan**

| **Cipher** | **Kelemahan Utama** |
| --- | --- |
| Caesar | Mudah dipecahkan dengan brute-force (hanya 25 kemungkinan). |
| Vigenère | Masih rentan terhadap analisis frekuensi jika panjang kunci diketahui. |
| Affine | Jika nilai a diketahui atau salah pilih, cipher dapat terpecahkan. |
| Playfair | Tidak cocok untuk komputerisasi modern karena hanya bekerja pada huruf. |
| Hill | Membutuhkan matriks invers untuk dekripsi; sulit jika determinan tidak relatif prima terhadap 26. |

**IV. Kesimpulan**

Lima algoritma cipher klasik memiliki prinsip enkripsi yang berbeda namun bertujuan sama, yaitu menjaga kerahasiaan pesan.

 Caesar: sederhana, cepat, mudah dipecahkan.

 Vigenère: lebih aman, polialfabetik, tapi rentan Kasiski.

 Affine: dua kunci, masih bisa frekuensi.

 Playfair: digraph, lebih aman, analisis digraph tetap memungkinkan.

 Hill: matriks blok, paling aman diantara yang lain, tapi perhitungan lebih rumit.

Link github:

<https://github.com/marshelindo/TugasKriptografi.git>

<https://github.com/khabibah/tugaskriptografi>