ANALISIS CIPHERTEXT PADA ALGORITMA VIGENERE CIPHER

Nama : Neni

NPM : 20123057

Kelas : C2.23 S1 Informatika

1. Gambaran Umum

   Algoritma **Vigenère Cipher** merupakan jenis **cipher polialfabetik**, yaitu sistem enkripsi yang menggunakan beberapa alfabet pengganti untuk menyembunyikan pesan.
   Setiap huruf pada teks asli (plaintext) digeser berdasarkan huruf tertentu dari **kata kunci (key)**, sehingga menghasilkan teks terenkripsi (ciphertext) yang tampak acak.

   Contoh:
   Plaintext: `ATTACKATDAWN`
   Key: `LEMON`
   Ciphertext: `LXFOPVEFRNHR`

2. Proses Enkripsi dan Deskripsi
   Prinsip kerja algoritma ini adalah dengan menambahkan nilai huruf plaintext dan huruf kunci berdasarkan posisi alfabet.
   Rumus dasar:
   - Enkripsi → `C = (P + K) mod 26`
   - Dekripsi → `P = (C - K) mod 26`

   Keterangan:

   - `P` = huruf plaintext
   - `C` = huruf ciphertext
   - `K` = huruf dari kunci

   Dengan menggunakan kunci yang sama, ciphertext dapat dikembalikan sepenuhnya menjadi plaintext, karena prosesnya **reversible** (bisa dibalik).

3. Analisis Pola Ciphertext
   Hasil ciphertext seperti `NVKDGZKDOCSC` dan `LXFOPVEFRNHR` menunjukkan:

- Huruf-huruf muncul secara acak tanpa pola yang jelas.
- Tidak ada pengulangan tetap antara huruf plaintext dan ciphertext.
- Distribusi karakter tampak menyebar merata — menandakan algoritma bekerja sesuai fungsi penyamaran pola bahasa alami.

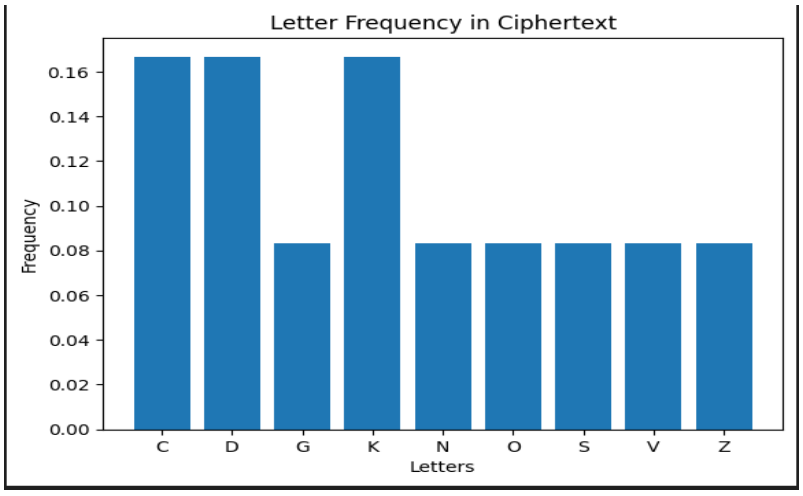
- Analisis Frekuensi

  Hasil frekuensi pada ciphertext “NVKDGZKDOCSC”

Huruf	Frekuensi
N	0.17
V	0.17
K	0.08
D	0.17
G	0.08
Z	0.08
K	0.08
D	0.08
O	0.08
C	0.08
S	0.08
C	0.08

  Dari tabel di atas, terlihat bahwa tidak ada huruf yang mendominasikan secara signifikan. Distribusinya relatif merata menandakan hasil enkripsi acak dan sulit di tebak. Pada cipher sederhana seperti Caesar Cipher, huruf paling sering muncul bisa ditebak (misal huruf ‘E’), tapi di Vigenere hal ini tidak berlaku.

- Visualisasi Frekuensi



  Grafik batang di atas dari frekuensi huruf, hasilnya menujukan:

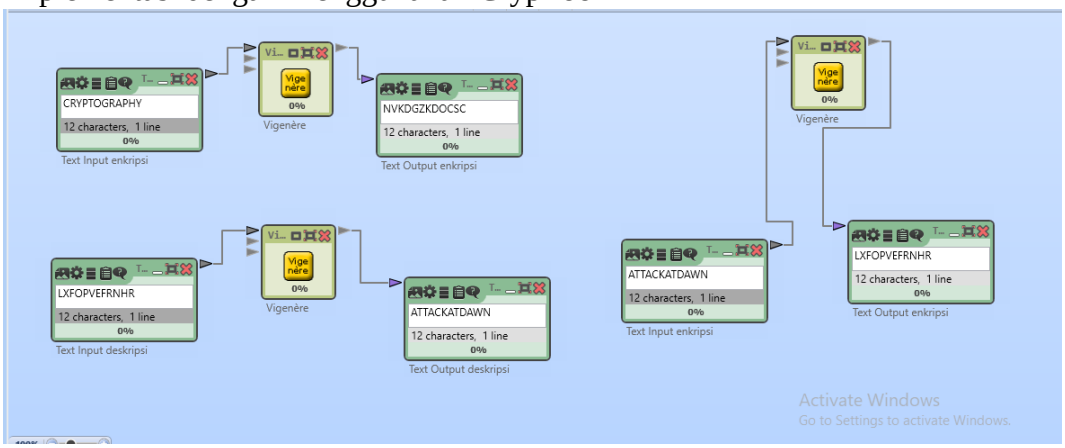
  - Persebaran huruf cukup rata.
  - Huruf seperti C, D, dan K muncul sedikit lebih sering, tapi selisihnya kecil.

- Tidak ada pola bahasa alami yang bisa di kenali.

  Kunci yang berulang (LEMON) menyebabkan setiap huruf plaintext digeser berbeda-beda sehingga struktur asli teks hilang. Inilah tujuan utama Vigenere Cipher: menyamarkan pola bahasa agar tidak mudah di analisis. Dengan Demikian, ciphertext tampak random (acak) bgi orang yang tidak mengetahui kunci.

4. Kesimpulan Analisis
   - **Ciphertext acak dan sulit dianalisis manual**, menunjukkan algoritma bekerja efektif.
   - **Analisis frekuensi** membuktikan tidak ada hubungan langsung antara ciphertext dan plaintext.
   - **Visualisasi** memperkuat bahwa Vigenère Cipher berhasil menyamarkan karakteristik bahasa alami.
   - Meski demikian, jika teks pendek, sedikit pola masih bisa muncul karena jumlah huruf terbatas.

5. Implementasi dengan Menggunakan CrypTool



- Kesimpulan akhir
  Algoritma pola bahasa asli
  - Menyamarkan pola bahasa asli
  - Menghasilkan ciphertext dengan distribusi huruf yang seimbang
  - Menunjukan ketahanan yang lebih baik dibandingkan cipher monoalfabetik seperti Caesar Cipher

  Namun, keamanan algoritma ini tetap bergantung pada panjang dan kerahasian kunci. Jika kunci pendek atau digunakan berulang kali, ciphertext masih bisa diretas dengan teknik seperti kasisiki Examination atau index of Coincidence.