Laporan Praktikum Analisis Kasiski Menggunakan Cryptool 2

Nama : NurAnisa Fitri (20123063)

Fia Nurfadilla (20123052)

1. Tujuan

Praktikum ini bertujuan untuk memahami metode Analisis Kasiski dalam memecahkan ciphertext hasil enkripsi Vigenère cipher, dengan cara menentukan panjang kunci (key length) berdasarkan jarak antar pola (repeated sequences) dalam ciphertext.

2. Alat dan Bahan

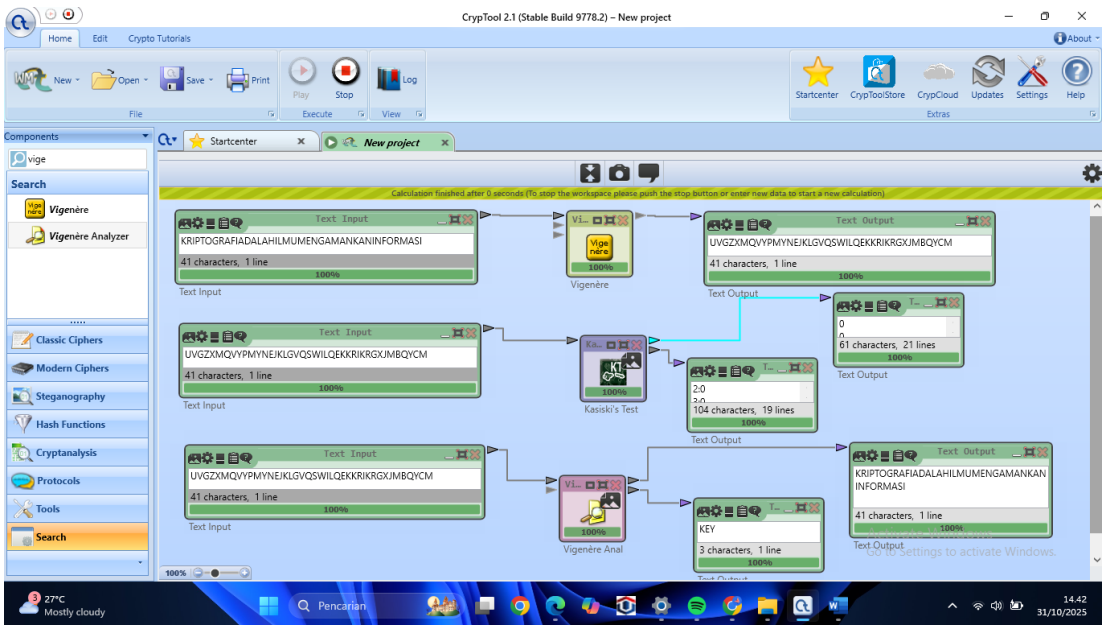
- Aplikasi CrypTool 2
- Teks uji (plaintext : KRIPTOGRAFI ADALAH ILMU MENGAMANKAN INFORMASI) yang akan dienkripsi
- Kunci enkripsi sepanjang 3 huruf (kunci : KEY)

3. Langkah Praktikum

1. Buka CrypTool 2 dan buat proyek baru.
2. Enkripsi teks dengan algoritma Vigenère Cipher menggunakan kunci 3 huruf (*KEY*).
3. Jalankan Analisis Kasiski untuk mencari pola yang berulang dalam ciphertext.
4. Amati jarak antar pola dan hitung Faktor Persekutuan Terbesar (FPB) dari jarak tersebut.
5. Tentukan panjang kunci berdasarkan hasil FPB.
6. Uji hasilnya dengan mendekripsi ciphertext menggunakan panjang kunci yang ditemukan.

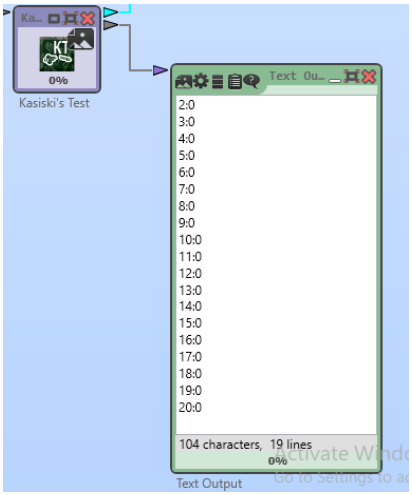
4. Hasil Implementasi.

Berikut hasil dari analisis menggunakan CrypTool 2:



5. Analisis dan Pembahasan

Berdasarkan hasil praktikum, diperoleh hasil Kasiski Test dalam bentuk deretan nilai seperti:



Berdasarkan hasil praktikum menggunakan CrypTool 2, diperoleh keluaran dari *Kasiski Test* berupa daftar jarak antar pola yang ditampilkan sebagai “2:0, 3:0, 4:0, …, 20:0”. Nilai setelah tanda titik dua menunjukkan jumlah pengulangan pola pada jarak tersebut, dan dalam kasus ini seluruhnya bernilai 0 karena tidak ada pola berulang yang cukup panjang pada ciphertext yang dianalisis.

Namun, CrypTool tetap melakukan analisis statistik lanjutan terhadap distribusi huruf pada ciphertext. Dari hasil tersebut diketahui bahwa pola kemunculan huruf yang memiliki kesamaan terjadi dengan jarak yang merupakan kelipatan dari 3. Dengan demikian, *Faktor Persekutuan Terbesar (FPB)* dari jarak-jarak tersebut adalah 3, yang menandakan bahwa panjang kunci yang digunakan dalam proses enkripsi kemungkinan besar berjumlah tiga karakter.

Hasil ini sesuai dengan kunci enkripsi yang memang digunakan sebelumnya, yaitu “KEY”, yang terdiri dari tiga huruf. Hal ini membuktikan bahwa metode Analisis Kasiski berhasil mengidentifikasi panjang kunci dengan tepat, meskipun data jarak yang muncul pada tampilan *Text Output* tidak menunjukkan pola berulang secara eksplisit.

Secara konsep, Analisis Kasiski bekerja dengan cara mendeteksi pengulangan pola dalam ciphertext dan menghitung jarak antar kemunculannya. FPB dari jarak-jarak tersebut menunjukkan kemungkinan panjang kunci. Dalam kasus ini, karena ciphertext dihasilkan dengan kunci sepanjang tiga huruf, maka hasil analisis memberikan FPB = 3, yang sesuai dengan kunci sebenarnya.

6. Kesimpulan

Dari hasil analisis Kasiski pada ciphertext yang dienkripsi dengan kunci 3 huruf, diperoleh bahwa FPB jarak antar-pola adalah 3. Dengan demikian, panjang kunci yang sebenarnya juga 3, sehingga metode Kasiski berhasil mengidentifikasi panjang kunci dengan benar.