

#### Optimasi Kasiski Examination pada Studi Kasus SPOJ The Bytelandian Cryptographer (Act IV)

#### Algoritma Pemograman | Departemen Informatika | FTIK | ITS

## Latar Belakang

- -Terdapat dua buah string yaitu plaintext dan ciphertext dan satu buah bilangan bulat yaitu batas atas panjang kunci enskripsi yang di berikan
- Plaintext dan ciphertext yang ada dalam kondisi yang tidak lengkap
- Metode enskripsi yang digunakan Vigenere Cipher dengan aturan:

$$y_i = x_i + k_{1+(i-1)modM} mod 26$$

- Diminta untuk mendapatkan plaintext dari yang telah di ketahui

# Metodologi

#### **Kasiski Examination**



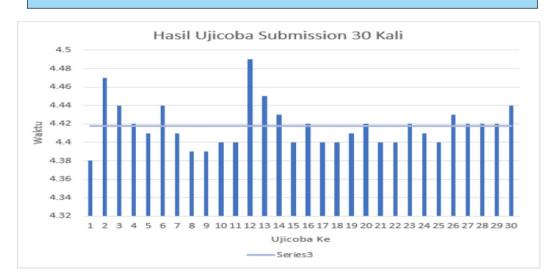
Intersection

# Kesimpulan

Implementasi Kasiski Examination terhadap studi kasus ini tidak cukup. Dibutuhkan metode intersection sehingga dapat menyelesaikan studi kasus ini dengan benar.

Kompleksitas waktu yang dibutuhkan O(T\*(M/2)\*(N+S)), dimana T adalah testcase, M adalah batas atas panjang kunci, N jumlah karakter tidak '\*' pada keduanya dan S yang '\*' pada ciphertext

## Hasil



## Saran

Mencari metode baru dalam pencarian panjang kunci atau optimisasi metode ini.

Freddy Hermawan Y Rully Soelaiman, S. Kom, M. Kom Wijayanti Nurul Khotimah, S.Kom, M.Sc NIP 19860312201212004

NRP 511310040 NIP 19700213199402001



