

## Latar Belakang

- Terdapat dua buah string yaitu plaintext dan ciphertext dan satu buah bilangan bulat yaitu batas atas panjang kunci enkripsi yang di berikan
- Plaintext dan ciphertext yang ada dalam kondisi yang tidak lengkap
- Metode enkripsi yang digunakan Vigenere Cipher dengan aturan:
$$y_i = x_i + k_{1+(i-1) \bmod M} \bmod 26$$
- Diminta untuk mendapatkan plaintext dari yang telah di ketahui

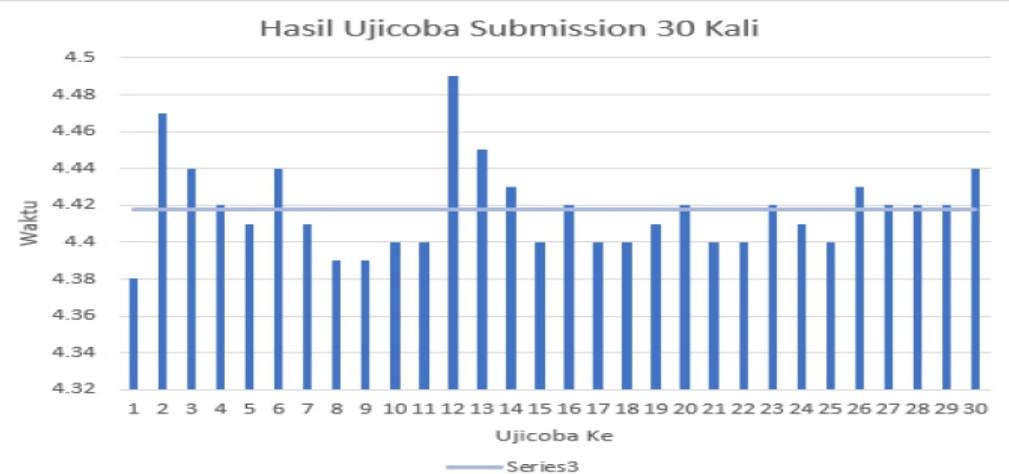
## Metodologi

### Kasiski Examination



### Intersection

## Hasil



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

## Saran

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