Ghimnastiar Al Abiyyuna 05311940000042

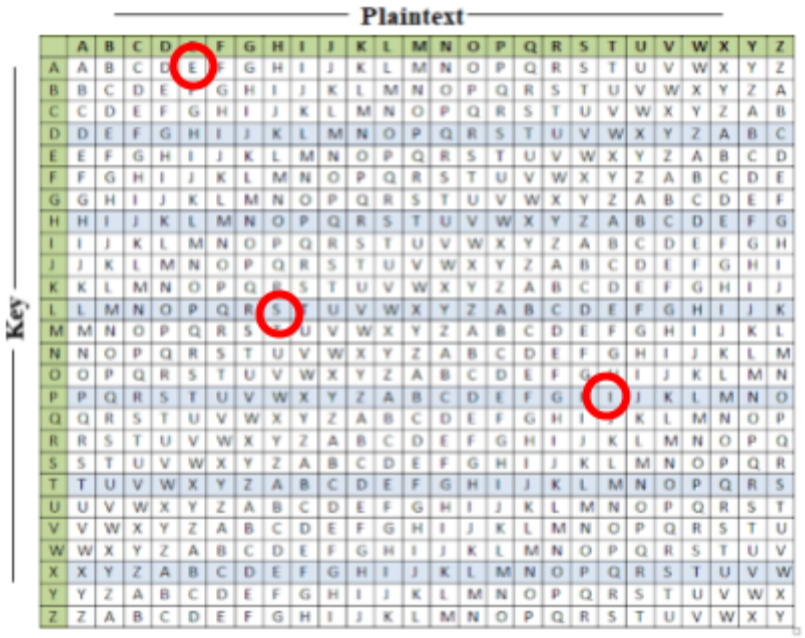
EAS
Teknologi Keamanan Komputer

Cyphertext

“ise sxcsg bptudo if ulr zdce qxqfvrflg”

Metode kasiski adalah salah satu cara mendekripsi sebuah sandi vigenere. Metode ini memanfaatkan perulangan huruf dalam penulisan sebuah kalimat. Namun, setelah diperhatikan, ternyata soal kali ini tidak memiliki potongan kata yang berulang sehingga saya saya mencoba sedikit menebak dan memanfaatkan pola penulisan kalimat dalam Bahasa Inggris. Singkat cerita, saya mengasumsikan kata **“ise”** dari kalimat chipertext soal memiliki plaintext sebuah kata Bahasa Inggris yang berjumlah tiga karakter/huruf. Berikut merupakan beberapa kata dalam Bahasa Inggris yang paling sering digunakan yang tersusun dari tiga karakter: **The, You, Any, But, New, And**. Karena kata **“ise”** berada di awal kalimat, oleh karena itu, kata pertama yang saya coba adalah **“The”**.

Karena saya sudah mengasumsikan sebuah kata dari plaintextnya, kita bisa menemukan sebagian atau bahkan seluruh key dari chipertext tadi. Di sini saya menggunakan tabel bujursangkar Vigenere yang berisi daftar pergeseran karakter dari plaintext menjadi chipertext.



Setelah melihat tabel di atas, didapatkan sebuah key “pla”.

Percobaan 1:

Pertama saya menggunakan dan mencoba key yaitu “plap”. Berikut merupakan hasil dari dekripsi ciphertext:

“the dirsr metfod iq far kore biffgculr”

ditemukan beberapa kata yang kembali berpotensi merupakan kata dalam Bahasa Inggris yaitu “metfod” dan juga “iq”.

Percobaan 2:

Untuk percobaan selanjutnya saya menggunakan key “plan”

“the first method is far more difficult”

Dalam percobaan kedua akhirnya ditemukan kalimat yang dapat diartikan.

Kesimpulan pada percobaan kali ini adalah metode kasiski sangat memanfaatkan pengulangan 2huruf dan 3huruf, jika contoh kasus yang kita miliki kebetulan tidak memiliki pengulangan maka kita harus mulai berasumsi dan mencoba satu satu kemungkinan yang bisa dijadikan kunci, **cara ini sangat memakan waktu dan tidak efektif ini juga menjadi kelemahan metode kasiski.**