**EAS Teknologi Keamanan Komputer**

Soal:

Carilah plaintext dari ciphertext berikut menggunakan metode kasiski.Chipertext di bawah dienkripsi menggunakan metode Vigenere.

**“ise sxcsg bptudo if ulr zdce qxqfvrflg”**

Jawab:

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:**

Saya mencoba memasukkan key ke dalam chipertext untuk mendapatkan bagian plaintext yang lainnya, dan hasilnya adalah sebagai berikut:

**“the dmcdv baiuod iq jlc odnt qiffggfwv”**

Terlihat bahwa sepertinya tidak ada kata yang menunjukkan atau bahkan mendekati sebuah plaintext. Hal ini bisa terjadi karena beberapa hal, salah satunya karena jumlah key yang dimasukkan kurang atau tidak sesuai. Oleh karena itu, saya mencoba menambahkan sebuah huruf ke dalam key.

Saya kembali mengasumsikan bahwa key adalah sebuah kata dalam Bahasa Inggris. Setelah itu, saya mencari daftar kata dalam kamus Bahasa Inggris yang berawalan “pla” dan memiliki empat buah karakter. Berikut merupakan daftar kata yang saya temukan:



**Percobaan 2:**

Saya mencoba mendekripsi ciphertext awal namun kali ini saya menggunakan key yang berbeda yaitu “play”. Hasil yang saya dapatkan adalah sebagai berikut:

**“the uirsi metwod ih far bore siffxculi”**

Ternyata plaintext yang dihasilkan masih tidak terlalu berbentuk. Namun, dapat dilihat ada beberapa kata yang berpotensi merupakan sebuah kata dalam Bahasa Inggris seperti “metwod” dan “ih”. Walaupun kata “play” bukan merupakan key dari chipertext di atas, namun setidaknya ada petunjuk yang diperoleh yaitu jumlah karakter dari key sudah lebih benar dari sebelumnya.

**Percobaan 3:**

Sama seperti sebelumnya, saya melanjutkan percobaan menggunakan key yaitu “plap”. Berikut merupakan hasil dari dekripsi ciphertext:

**“the dirsr metfod iq far kore biffgculr”**

Terdapat kesamaan hasil seperti sebelumnya. Ada beberapa kata yang kembali berpotensi merupakan kata dalam Bahasa Inggris yaitu “metfod” dan juga “iq”.

**Percobaan 4:**

Sama seperti sebelumnya, saya melanjutkan percobaan menggunakan key yaitu “plan”. Berikut merupakan hasil dari dekripsi ciphertext:

**“the first method is far more difficult”**

Benar saja, akhirnya kita memperoleh sebuah plaintext berbahasa Inggris yang benar dengan menggunakan key “plan”. Dengan demikian, key dari ciphertext soal tadi adalah “plan”.

Kesimpulan dari pemecahan soal di atas adalah, dekripsi menggunakan metode Kasiski merupakan sebuah metode yang memanfaatkan perulangan bagian teks yang ada. Namun, dikarenakan soal di atas tidak memiliki bagian kata yang berulang, mau tidak mau kita harus mencoba menebak bagian teks dari ciphertext dan mencoba berbagai kemungkinan key sampai didapatkan hasil yang diinginkan. Cara ini cukup tidak efektif namun dapat berhasil.