Puguh Aji Prabowo
223200021

Vigenère Cipher

Kriptografi telah menjadi salah satu aspek penting dalam dunia komunikasi dan keamanan informasi. Salah satu teknik kriptografi klasik yang menarik untuk dibahas adalah Vigenère Cipher. Vigenère Cipher adalah sebuah algoritma kriptografi yang menggunakan teknik substitusi karakter untuk menyandikan pesan teks. Algoritma ini pertama kali ditemukan oleh seorang kriptografer Prancis, Blaise de Vigenère, pada abad ke-16. Vigenère Cipher adalah salah satu teknik kriptografi klasik yang sangat populer pada zamannya.

Prinsip Kerja Vigenère Cipher

Vigenère Cipher adalah bentuk kriptografi substitusi polialfabetik. Ini berarti bahwa algoritma ini menggunakan beberapa alfabet yang berbeda untuk mengenkripsi pesan teks, yang membuatnya lebih kuat daripada algoritma substitusi Caesar Cipher yang hanya menggunakan satu alfabet. Prinsip kerja Vigenère Cipher adalah sebagai berikut:

Kunci Enkripsi: Pengirim dan penerima pesan harus memiliki kunci yang sama, biasanya dalam bentuk kata atau frasa. Kunci ini digunakan sebagai referensi untuk mengenkripsi dan mendekripsi pesan.

Pesan Teks: Pesan yang akan dienkripsi harus berupa teks yang ingin disandikan.

Enkripsi: Setiap karakter dalam pesan teks dienkripsi menggunakan alfabet kunci yang sesuai. Proses ini melibatkan pergeseran karakter pesan dengan karakter kunci. Karakter kunci berulang terus menerus sampai semua karakter dalam pesan teks terenkripsi.

Dekripsi: Penerima pesan dapat mendekripsi pesan dengan menggunakan kunci yang sama untuk mengurangkan pergeseran karakter yang dilakukan pada pesan terenkripsi.

Contoh Vigenère Cipher

Mari kita lihat contoh sederhana bagaimana Vigenère Cipher berfungsi. Misalkan kita memiliki pesan teks "HELLO" dan kunci "KEY." Pertama, kita konversi pesan teks dan kunci menjadi angka, dengan "A" menjadi 0, "B" menjadi 1, dan seterusnya. Kemudian, kita melakukan operasi modulo 26 untuk menjaga agar nilai tetap dalam rentang alfabet (26 karakter).

Pesan Teks (HELLO): 7 4 11 11 14
Kunci (KEY): 10 4 24
Kemudian, kita enkripsi karakter demi karakter:

'H' dienkripsi dengan 'K' (7 + 10 = 17, yang setara dengan 'R')
'E' dienkripsi dengan 'E' (4 + 4 = 8, yang setara dengan 'I')
'L' dienkripsi dengan 'Y' (11 + 24 = 35, tetapi kita ambil modulo 26, yang setara dengan 'Y')
'L' dienkripsi dengan 'E' (11 + 4 = 15, yang setara dengan 'O')
'O' dienkripsi dengan 'Y' (14 + 24 = 38, tetapi kita ambil modulo 26, yang setara dengan 'Y')
Sehingga, pesan teks "HELLO" dienkripsi menjadi "RIEYO."

Saya juga sudah membuat program sederhana menggunakan js yang sudah saya lampirkan juga untuk contoh lebih realnya,

Kelemahan Vigenère Cipher

Meskipun Vigenère Cipher adalah salah satu algoritma kriptografi klasik yang kuat pada zamannya, ia memiliki kelemahan. Salah satu kelemahan utamanya adalah panjang kunci. Jika panjang kunci terlalu pendek, pesan dapat dengan mudah diretas dengan teknik analisis frekuensi.

Namun, Vigenère Cipher tetap menjadi tonggak penting dalam sejarah kriptografi dan memberikan inspirasi bagi perkembangan algoritma kriptografi modern yang lebih kompleks. Teknik-teknik kriptografi seperti Enigma machine yang digunakan selama Perang Dunia II juga terinspirasi oleh konsep dasar yang digunakan dalam Vigenère Cipher.

Saat ini, Vigenère Cipher telah digantikan oleh algoritma kriptografi yang lebih kuat dan canggih, seperti Advanced Encryption Standard (AES) yang menggunakan pendekatan kriptografi simetris yang jauh lebih kuat dan aman. Meskipun begitu, pemahaman tentang Vigenère Cipher masih penting dalam memahami sejarah kriptografi dan bagaimana algoritma kriptografi telah berevolusi hingga saat ini.