Dari cipherteks yang didapat kita dapat lihat bahwa huruf M dienkripsikan menjadi O, huruf A dienkripsikan menjadi huruf C, dan seterusnya dimana huruf pada pesan digeser sejauh nilai kunci. Algoritma caesar cipher sangat sederhana sehingga sangat berisiko untuk dipecahkan karena hanya dibutuhkan pengetahuan satu huruf dari plainteks untuk mengetahui kunci yang digunakan. Vigenere cipher yang menerapkan metode subtitusi abjad-majemuk tidak memiliki permasalah tersebut karena tergantung dengan kunci yang diberikan. Kunci yang digunakan vigenere cipher berbeda dengan yang digunakan caesar cipher. Jika pada caesar kuncinya hanya satu nilai saja, maka pada vigenere cipher kunci yang digunakan berbentuk deretan huruf. Kunci yang berbentuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk di enkripsikan dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang plainteks maka kunci akan diulang sampai panjang kunci sama dengan panjang plainteks. Algoritma ini akan meminimalkan kemungkinan dipecahkannya cipherteks jika satu huruf plainteks diketahui.

Model matematika dari enkripsi pada algoritma vigenere cipher ini adalah seperti berikut:

$C_i = E_k (M_i) = (M_i + K_i) \bmod 26$

Dan model matematika untuk dekripsinya adalah :

$M_i = D_k (C_i) = (C_i - K_i) \bmod 26$

Dengan C memodelkan cipherteks, M memodelkan plainteks, dan K memodelkan kunci.