BAB V

Penutup

5.1 Kesimpulan

Kriptografi Vigènere Cipher ini dapat diterapkan untuk pengamanan aplikasi rekam medis pasien ,Data yang ada pada rekam medis pasien menjadi lebih aman dengan menggunakan enkripsi yang dikustomisasi.

Ciphertext Vigenère adalah kombinasi dari pergeseran Caesar yang dikombinasikan dengan kata kunci. Panjang kata kunci menentukan jumlah enkripsi berbeda yang diterapkan pada plaintext. Kekuatan dari cipher Vigenère adalah bahwa ia tidak rentan terhadap analisis frekuensi karena fakta bahwa cipher berputar melalui perubahan yang berbeda, sehingga huruf plaintext yang sama tidak akan selalu dienkripsi ke huruf ciphertext yang sama.

Cipher Vigenère sulit dipecahkan menggunakan brute-force karena setiap huruf dalam pesan dapat dikodekan sebagai salah satu dari 26 surat. Karena penyandian pesan tergantung pada kata kunci yang digunakan, pesan yang diberikan dapat disandikan 26 cara, dimana k adalah panjang kata kunci. Misalnya, jika kita hanya tahu bahwa pesan dikodekan dengan kata 7 huruf, maka itu bisa dikodekan dalam 26^7=8miliar cara!

5.2 Saran

Saran-saran yang dapat diberikan dari hasil penelitian ini adalah :

Penambahan String lain bisa membantu untuk memecah masalah dari metode kasiski yang mampu memecahkan metode enkripsi vigenere cipher,atau mengubah urutan dari teks plain tersebut hal ini juga dapat mempersulit bagi meotode kasiski memecah emkripsi tersebut.Penggunaan metode enkripsi terbaru seperti AES 256,karena vigenere cipher hanya mengakomodasi input text(aphlabetical).