2.1.2 Aspek-aspek keamanan

Kriptografi tidak hanya memberikan kerahasiaan dalam telekomunikasi, namun juga memberikan komponen-komponen berikut ini:

a. *Authentication (*otentikasi), penerima pesan dapat memastikan keaslian pengirimnya.
b. *Integrity* (integritas), penerima harus dapat memeriksa apakah pesan telah dimodifikasi. Seorang penyusup seharusnya tidak dapat memasukkan tambahan ke dalam pesan, mengurangi atau mengubah pesan.
c. *Non-repudiation* (nir penyangkalan), pengirim seharusnya tidak dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya, tanpa kriptografi, seseorang dapat mengelak bahwa dialah pengirim pesan yang sesungguhnya[4].

2.1.3 Vigenere Cipher

Vigenere cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu *Blaise de Vigenere*, namun sebenarnya buku *La Cifra del Sig. Giovan Batista Belaso*, sebuah buku yang ditulis oleh *Giovan Batista Belaso* pada tahun 1553.

Cara kerja dari vigenere cipher ini mirip dengan caesar cipher, yaitu mengenkripsikan plainteks pada pesan dengan cara menggeser huruf pada pesan