tersebut sejauh nilai kunci pada deret *alphabet.* Vigenere cipher adalah salah satu algoritma klasik yang menggunakan metode subsitusi abjad-majemuk. Subsitusi abjad-majemuk mengenkripsikan setiap huruf abjad-tunggal yang semua huruf di suatu pesan dienkripsi menggunakan kunci yang sama[2].

Sandi caesar merupakan sistem persandian klasik berbasis subtitusi yang sederhana. Enkrpsi dan dekripsi pada sistem persandian caesar menggunakan operasi *shift.* Operasi *shift* adalah mensubtituasikan suatu huruf menjadi huruf pada daftar alfabet berada di-*k (key)* = 3 (ganti dengan huruf ke-3 sebelah kanan) maka “A” menjadi “D”, “B” menjadi “E” dan seterusnya. Bagaimana dengan “X”, “Y” dan “Z”. Supaya semuanya memiliki subtitusi, huruf “A” dianggap disebelah kanan huruf “Z” sehingga “X” menjadi “A”, “Y” menjadi “B” dan “Z” menjadi “C”.

Untuk dapat mengolah teks asli yang merupakan deretan simbol huruf diperlukan pemetaan dari huruf menjadi angka dapat diapilikasi operasi matematika. Misalnya huruf “A” sampai “Z” dipetakan ke angka integer dari “0” sampai “25”. Perhatikan nilai yang mungkin bagi teks asli dan teks sandi adalah 0 sampai 25 dan apabila hasil pergeseran (penjumlahan) melebihi 26 angka tersebut dibagi 26 dan nilai yang dipakai adalah sisa bagi. Oleh karena itu sritmatika modular Z_{26} digunakan pada persandian caesar[5].

Sebagai contoh caesar cipher jika terjadi plaintks :

MAKALAH KRIPTOGRAFI

Maka jika dienkripsikan dengan nilai kunci 2 akan didapatkan cipherteks :

OCMCNCJ MTKRVQITCHK