1. Pendahuluan

Latar Belakang

Digital Signature atau tanda tangan digital merupakan bagian penting pada saat pengiriman dokumen digital. *Digital Signature* berfungsi untuk memvalidasi keabsahan dari pengirim dokumen dan integritas dari sebuah dokumen digital . Ada banyak jenis *Digital Signature* yang digunakan salah satunya adalah *Cryptonote Signature* [1]. *Cryptonote Signature* digunakan pada beberapa *Crypto currencies* seperti *Bitcoin*, *monero* dan *karbo*. Disamping itu *Cryptonote Signature* juga digunakan pada beberapa sistem informasi yang menggunakan *blockchain* misalnya sitem catatan kesehatan yang dibangun oleh Debasish Ray Chadwuri [2]. Walaupun demikian *Cryptonote Signature* masih memiliki kekurangan berupa kunci yang panjang sehingga waktu yang diperlukan untuk melakukan komputasi cukup lama. Oleh karena itu, perlu dicari jenis *Digital Signature* yang memiliki yang komputasi yang lebih rendah.

Pada tugas akhir ini, digunakan *Digital Signature* lain untuk diperbandingkan dengan *Cryptonote Signature*. *Digital Signature* tersebut adalah *Rank Quasi Cyclic Signature* atau RQCS [3]. RQCS dipilih karena memiliki panjang kunci yang pendek sehingga waktu yang perlukan untuk melakukan komputasi lebih singkat. Selain itu pada RQCS memiliki proses iterasi lebih sedikit dibandingkan dengan *Cryptonote Signature* karena menggunakan perkalian matriks, sementara pada *Cryptonote Signature* terdapat proses iterasi cukup banyak karena pada *Cryptonote Signature* menggunakan perkalian titik yang terdapat pada ecc. Percobaan dilakukan dengan menggunakan berbagai nilai panjang kunci, kemudian dihitung waktu proses untuk setiap panjang kunci baik menggunakan menggunakan *Cryptonote Signature* maupun RQCS.

Topik dan Batasannya

Topik yang diusulkan pada tugas akhir ini adalah perbandingan antara *Cryptonote Signature* dengan *Rank Quasi Cyclic Signature.* Perbandingan antara keduanya dilakukan dengan membandingkan panjang kunci, panjang pesan, dan waktu proses komputasi. Perbandingan ini dilakukan karena *Cryptonote dan RQCS* memiliki perbedaan pada panjang kunci dan mekanisme yang dilakukan. Adapun jumlah kunci yang dicoba adalah 25 kunci dengan panjang mulai dari 8 bit hingga 128 bit. Masing masing kunci memiliki pesan yang di uji cobakan sebanyak 16 pesan .

Tujuan

Percobaan ini memiliki tujuan mengatasi kekurangan *Cryptonote Signature* berupa waktu komputasi yang lama dengan RQCS