INTISARI

Kriptosistem Kunci-Publik GTRU dan Aplikasinya Pada Grup $\mathbb{Z}^n$ dan Grup Poli-$\mathbb{Z}$

Oleh

Rifky Manuel Satyana

18/427682/PA/18642

Kriptosistem kunci-publik telah digunakan di sebagian besar transmisi data di internet dan didasarkan pada perhitungan matematis. NTRU adalah salah satu kriptosistem kunci-publik pasca komputasi kuantum yang bekerja pada ring polinomial terpotong derajat N. Lebih lanjut, NTRU dikenal dengan ragam variannya dan salah satunya adalah GTRU. Pada tahun 2019, Xu dkk membuat kriptosistem GTRU atau *Group-based NTRU-like* yang bekerja pada grup yang diperoleh dengan menggeneralisasi NTRU ke dalam struktur grup. Mereka mengaplikasikan GTRU pada grup poli-$\mathbb{Z}$ khusus dan mengklaim bahwa GTRU memiliki performa yang lebih baik dibandingkan dengan RSA. Dengan demikian skripsi ini ditujukan untuk mencari nilai kebeneran klaim tersebut yang kemudian ditemukan tidak benar. Perlu diketahui bahwa definisi performa suatu kriptosistem pada penulisan skripsi ini adalah seberapa cepat kriptosistem tersebut dapat menyelesaikan proses pembangunan kunci, enkripsi dan dekripsi yang diukur oleh waktu.

ABSTRACT

GTRU Public-Key Cryptosystem and its Application on $\mathbb{Z}^n$ and Poly-$\mathbb{Z}$ Group

By

Rifky Manuel Satyana

18/427682/PA/18642

Public-key cryptosystems have been used in most data transmission across the internet and are based on mathematical computations. NTRU is one of public-key cryptosystem post-quantum computing era working on truncated ring polynomials of degree N. Furthermore, NTRU is known for its variety of variance and one of it is GTRU. In 2019, Xu and friends created GTRU or *Group-based NTRU-like* cryptosystem working on groups that is achieved by generalizing NTRU into the group structure. They also applied GTRU on a special poly-$\mathbb{Z}$ group and claimed that GTRU has better performance than RSA. Thus this undergraduate thesis is written to prove the latter statement and it is found to be invalid. It should be noted that the definition of the performance of a cryptosystem in the writing of this undergraduate thesis is how fast the cryptosystem can complete the key generation, encryption, and decryption processes as measured by time.