INTISARI

MATRU : SISTEM KRIPTOGRAFI BERBASIS NTRU

Oleh

FISZEDTA PUTRI KINANTY

18/424263/PA/18368

Sistem kriptografi NTRU (*Nth Degree Truncated Polynomial Ring*) merupakan sistem kriptografi berbasis permasalahan latis yang beroperasi pada ring polinomial $\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1\rangle$. Pada tugas akhir ini, akan dikaji mengenai salah satu sistem kriptografi perkembangan dari sistem kriptografi NTRU, yakni sistem kriptografi MaTRU. Secara umum, cara kerja MaTRU sama dengan prinsip umum dari NTRU, namun MaTRU beroperasi pada jenis ring yang berbeda. Sistem kriptografi MaTRU beroperasi pada ring matriks berukuran $k \times k$ atas ring polinomial $\mathcal{R}$. Selain membahas mengenai cara kerja sistem kriptografi MaTRU, tugas akhir ini juga berisi mengenai analisis keberhasilan sistem kriptografi MaTRU dengan memberikan beberapa parameter yang dapat digunakan dalam menjalankan sistem kriptografi MaTRU. Selanjutnya, diberikan pula modifikasi sistem kriptografi MaTRU agar tingkat keberhasilannya meningkat.

ABSTRACT

MATRU : AN NTRU - BASED CRYPTOSYSTEM

By

FISZEDTA PUTRI KINANTY

18/424263/PA/18368

NTRU (*Nth Degree Truncated Polynomial Ring*) cryptosystem is one of the lattice-based cryptosystem and operates in the ring $\mathcal{R} = \mathbb{Z}[x]/\langle x^n - 1\rangle$. In this final project, we introduce one of the new variant of the NTRU public key cryptosystem, the MaTRU cryptosystem. MaTRU cryptosystem works under the same principle as the NTRU cryptosystem, but it operates in a different ring. MaTRU cryptosystem operates in the ring of $k \times k$ matrices of polynimial ring in $\mathcal{R}$. In addition to a description of how the MaTRU cryptosystem works, this final project also contains some analysis of the success rate of the MaTRU cryptosystem by providing several parameters that can be used in running the MaTRU cryptosystem. Furthermore, there are also some modifications of the MaTRU cryptosystem to increase success rate of MaTRU cryptosystem.