INTISARI

Serangan Reduksi Latis LLL (Lenstra-Lenstra-Lovasz) pada Sistem Kriptografi NTRU (*Nth Degree Truncated Polynomial Ring*)

Oleh

SAIFULLAH ALI

17/414656/PA/18156

Telah diketahui bahwa sistem kriptografi berdasar pada permasalahan matematika. Salah satu kriptografi yang sedang berkembang saat ini adalah kriptografi latis. Kriptografi latis menggunakan permasalahan latis dalam menentukan vektor terpendek dan terdekat. Di sisi lain, salah satu serangan pada kriptografi latis menggunakan reduksi latis. Kriptografi latis dimulai ketika Hoffstein, Pipher, dan Silverman memperkenalkan sistem kriptografi NTRU (*Nth Degree Truncated Polynomial Ring*). Pada tulisan ini, akan diperlihatkan keamanan sistem kriptografi NTRU terhadap serangan reduksi latis LLL (Lenstra-Lenstra-Lovasz). Untuk itu, tulisan ini dimulai dengan mendeskripsikan sistem kriptografi NTRU dan dilanjutkan dengan mendeskripsikan reduksi latis LLL serta penerepan dalam penyerangan sistem kriptografi NTRU. Dari sini, dilakukan simulasi untuk melihat waktu pemecahan kunci privat pada latis NTRU. Selain itu, diberikan satu contoh parameter sistem kriptografi NTRU yang dinilai aman dari serangan LLL dengan asumsi yang diberikan yaitu sistem kriptografi NTRU 251 dengan estimasi waktu pemecahannya.

ABSTRACT

LLL (Lenstra-Lenstra-Lovasz) Lattice Reduction Attack On NTRU (Nth Degree Truncated Polynomial Ring) Cryptosystem

By

SAIFULLAH ALI

17/414656/PA/18156

It has been known that cryptosystems are based on mathematical problems. One of them that currently being developed is lattice-based cryptosystem. Lattice-based cryptosystem is based on lattice problems in accord to determine the shortest vectors and closest vectors. On the other hand, lattice cryptosystem has a flaw that can be penetrated by lattice reduction. Lattice-based cryptograpy began when Hoffstein, Pipher, and Silverman introduce the NTRU (Nth Degree Truncated Polynomial Ring) cryptosystem. In this final project, we demonstrated how secure the NTRU cryptosystem againts LLL (Lenstra-Lenstra-Lovasz) lattice reduction. Hence, this paper begins by desribing the NTRU cryptosystem and LLL lattice reduction. After that, the application of penetration attempt to the NTRU Cryptosystem would be shown. In this section, we performed real time simulation to examine the breaking time of private key on NTRU cryptosystem. In addition, we provided an example of the NTRU cryptosystem parameter (namely the NTRU 251 with an estimated breaking time) which is, with the given assumption, considered safe from LLL reduction lattice attack.