Abstrak

Perkembangan teknologi dalam hal keamanan data pada sistem telah berkembang sangat pesat. Terdapat 2 aspek penting yakni keamanan dan kerahasiaan pada data informasi, maka dari itu sebelum dikirim harus melakukan enkripsi terlebih dahulu. Dalam hal ini penerapan pengamanan data informasi tidak hanya dilakukan dengan 1 teknik keamanan saja, melainkan dapat dengan cara kombinasi. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan yang dapat digunakan untuk meningkatkan keamanan data informasi. Dalam hal ini mengimplementasikan kriptografi berbasis lattice yakni NTRU yang akan dikombinasikan dengan algoritma AES. Kriptografi berbasis lattice yang digunakan pada penelitian ini NTRU karena NTRU melakukan enkripsi *scheme* sedangkan untuk berbasis *lattice* lainnya menggunakan *mix key encaps* dan *signature.* Selain itu, algoritma NTRU dapat bertahan pada NIST *round* 3. Algoritma NTRU juga merupakan kriptografi simetri yang dapat digunakan untuk membangkitkan bilangan acak. Kombinasi algoritma tersebut akan dilakukan pada FTP (*file transfer protocol*) yang dirancang untuk membuat sambungan antara server dan client, dimana nantinya dapat mengirimkan *file* dari client ke server. *File Transfer Protocol* yang telah dibuat akan diterapkan pada protokol TLS versi 1.2 dikarenakan hingga saat ini di bulan Agustus 2020 terdapat 98,4% yang menggunakan *support* TLS versi 1.2, sumber data diambil dari SSL Pulse. SSL Pulse yakni dasbor yang memantau kualitas dukungan SSL/TLS. Disisi lain sebelumnya juga sering ditemui serangan pada protokol TLS versi 1.2. Sehingga penelitian ini menegaskan bahwa implementasi dari algoritma kriptografi NTRU pada protokol versi TLS 1.2 agar dapat digunakan untuk meningkatkan keamanan.

Kata kunci: Random Polinomial, Kriptografi NTRU, Berbasis Lattice