BAB 1
PENDAHULUAN

1.1 Latar Belakang

Kriptografi merupakan istilah yang berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* (*Crypto*) dan *graphia* (*graph*y). *Kript*o artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Jadi Kriptografi adalah ilmu sekaligus seni untuk menjaga keamanan pesan ataupun data tertentu. Jika dilihat lebih spesifik kriptografi merupakan suatu metode membangun skema atau protokol yang bertujuan membuat suatu data dan privasi dari pengguna lebih aman dan terlindungi. Terdapat beberapa metode yang digunakan dalam membuat kriptografi diantaranya kriptografi berbasis lattice. [1,2,3,4]

Lattice jika diakumulasikan merupakan suatu kotak yang memiliki pola tertentu. Lattice sendiri biasanya digabungkan dengan metode - metode tertentu seperti kriptografi berbasis lattice dan metode - metode lainnya dengan ilmu matematika. Kriptografi berbasis lattice sendiri merupakan sebuah istilah umum konstruksi primitif kriptografi yang melibatkan suatu lattice *(*aljabar abstract*)* baik itu dalam konstruksi itu sendiri maupun keamanan data lainnya. Kriptografi berbasis lattice merupakan hal penting dalam metode kriptografi kuantum. Tidak seperti skema kunci lainnya yang banyak digunakan seperti *RSA, Diffie-Hellman* ataupun *elliptic-curve cryptosystem* yang mudah diserang menggunakan komputer kuantum, kriptografi berbasis lattice lebih aman, dikarenakan metode yang digunakan dalam pembentukan kunci lebih kompleks. Kriptografi berbasis lattice biasanya dapat disebut juga NTRU berbasis lattice. Hal tersebut terjadi karena NTRU atau *N-th degree Truncated polynomial Ring Units* merupakan satu - satunya jenis enkripsi berbasis lattice untuk saat ini, Kriptografi yang menggunakan lattice untuk proses enkripsi dan dekripsi data. NTRU berbasis lattice sendiri menggunakan metode polinomial abstrak, algoritma *euclidean* dan algoritma *karatsuba* dalam proses pembentukan kunci, enkripsi maupun dekripsi data. Kunci yang di dapat dari hasil NTRU berbasis lattice akan disimpan di setiap database pengguna. Kunci publik akan digunakan untuk enkripsi dan kunci private akan di gunakan untuk dekripsi teks, sehingga teks yang tersimpan di database akan teracak. Hal tersebut akan menyebabkan, jika terdapat seseorang yang ingin meretas menggunakan cara MITM (*Man In The Middle*) *attack* ataupun menggunakan *Pegasus Attack,* maka teks yang terlihat di database akan bersifat acak. [5,6]

Melihat perkembangan zaman sekarang, dimana mengirim pesan antar perangkat sudah tidak asing lagi. Pengguna biasanya menggunakan alat-alat canggih seperti *smartphone* dan komputer untuk berkomunikasi dengan pengguna lainnya. Namun banyak aplikasi yang digunakan *smartphone* ataupun komputer yang belum cukup aman untuk merahasiakan teks yang dikirimkan oleh pengguna. Sebagai contoh aplikasi obrolan berbasis Android yaitu WhatsApp menggunakan metodologi

algoritma AES 256 sebagai alat untuk melindungi privasi obrolan para penggunanya. Menurut sebuah laporan di Financial Times pada hari Selasa (14/5/2019), *spyware* yang mengeksploitasi kerentanan adalah pegasus, yang dibuat oleh perusahaan Israel NSO. AES 256 yang di gunakan WhatsApp memiliki kunci yang lebih pendek sehingga ketika data dari database dapat diakses oleh penyadap. Penyadap dapat lebih gampang dalam penerjemahan data. [7][8]

Untuk menyelesaikan permasalahan di atas dibuat sebuah aplikasi berbasis android dimana dalam aplikasi tersebut di design dengan UI (*user interface*) yang lebih sederhana sehingga lebih mempermudah pengguna dalam proses penggunaannya. Selain itu aplikasi juga akan dilengkapi dengan metode kriptografi NTRU berbasis lattice yang akan sangat berguna dalam proses pengamanan data pribadi, obrolan dan lain lain terkait pengguna.

Dari penjelasan diatas kami dapat melihat bahwa setiap aplikasi yang di bangun selalu memiliki kekurangan baik itu dari keamanan pengguna dan lain - lainnya. Namun dengan menerapkan metode Kriptografi NTRU berbasis lattice dalam aplikasi obrolan berbasis android yang akan dibuat , harapan kedepannya aplikasi dapat membuat pengguna lebih merasa aman dalam penggunaan aplikasi khususnya dalam bidang komunikasi. [9]

1.2 Perumusan Masalah

Berdasarkan latar belakang diatas, maka rumusan masalah yang akan dibahas adalah:

a. Bagaimana membuat sistem komunikasi berbasis teks yang lebih aman untuk digunakan oleh pengguna?
b. Bagaimana cara membuat kriptografi NTRU berbasis lattice yang akan diterapkan pada sebuah aplikasi obrolan berbasis android?

1.3 Batasan Masalah

Batasan masalah dari pembangunan aplikasi ini adalah :

a. Aplikasi yang di buat menggunakan metode kriptografi NTRU berbasis lattice pada proses enkripsi pesan teks.
b. Aplikasi dibuat berbasis *mobile* android.
c. Aplikasi digunakan paling rendah pada usia 14 tahun (dianjurkan, kurang dari itu tidak dianjurkan).
d. Hanya terdapat 3 fitur obrolan yaitu obrolan pribadi, obrolan siaran baru dan obrolan grup yang masing – masing percakapan teks sudah di enkripsi dengan metode kriptografi berbasis lattice.

e. Setiap obrolan hanya dapat mengirimkan 3 jenis bentuk pesan yaitu pesan teks, pesan gambar, dan pesan *file* dokumen. Hanya percakapan teks yang di enkripsi oleh kriptografi berbasis lattice.

f. Beberapa fungsi yang akan di enkripsi adalah obrolan berupa teks, url pesan gambar, url pesan file dan password pengguna

g. Aplikasi ini hanya bisa digunakan pada *smartphone* android dengan versi sistem operasi minimal *Lolipop* 5.0 (API level : 21).

h. Aplikasi akan mendukung pembuatan UI (*User Interface*) yang sederhana.

i. Aplikasi akan bekerja secara normal jika didukung dengan koneksi internet pada perangkat *smartphone* android.

j. Aplikasi didukung oleh beberapa aplikasi pihak ketiga yang dibutuhkan

1.4 Tujuan

Tujuan dari pembangunan aplikasi ini :

a. Membangun Aplikasi obrolan berbasis android dengan memanfaatkan media kriptografi NTRU berbasis lattice sebagai metode dalam proses pengamanan data pengguna

b. Mempermudah pengguna dalam berkomunikasi jarak jauh yang dapat meminimalisir masalah dari pengamanan data

c. Mempermudah pengguna dalam menyebarkan informasi yang dapat berguna untuk semua pengguna.

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang dilakukan dalam pembangunan aplikasi ini adalah

a. Tahap Studi literatur

   Mencari referensi di internet dan pustaka yang berhubungan dengan topik proyek akhir, seperti kriptografi berbasis lattice, UI/UX design, aplikasi obrolan menggunakan firebase, kriptografi NTRU asimetri .

b. Tahap pencarian dan pengumpulan data

   Pencarian dan pengumpulan data dilakukan dengan cara survei kepada masyarakat umum dan bertanya kepada sumber ahli.

c. Tahap perancangan sistem

   Perencanaan aplikasi dilakukan sesuai dengan standar pembuatan aplikasi. Mulai dari *mock-up*, design database, *workflow*, dan lain - lainnya.

d. Tahap implementasi

Melakukan implementasi terhadap aplikasi yang telah dirancang sebelumnya.

e. Tahap pengujian dan analisis

   Melakukan pengujian terhadap aplikasi yang telah dibuat dan melakukan analisis hasil pengujian tersebut.

f. Tahap evaluasi dan perbaikan

   Melakukan perbaikan aplikasi setelah aplikasi dilakukan pengujian kepada pengguna. Sehingga tampilan dan fungsi aplikasi sesuai dengan keinginan pengguna.

g. Tahap Pengujian Akhir

   Melakukan pengujian kembali setelah diperbaiki dan disesuaikan dengan keinginan pengguna

h. Tahap pembuatan laporan

   Membuat laporan proyek akhir yang berisi dokumentasi dalam proses menyelesaikan proyek akhir beserta hasil analisis.

1.6 Pembagian Tugas Anggota

Berikut pembagian tugas anggota tim proyek :

a. I Kadek Sumendra

Peran : Project Manager dan Programmer

Tanggung Jawab:

- Pembuatan aplikasi
- Pembuatan buku
- Pembuatan jurnal
- Pembuatan panduan pengguna
- Pembuatan poster

b. Yoga Afrizal Riandika

Peran : *Designer* dan *Programmer*

Tanggung Jawab:

- Pembuatan aplikasi
- Pembuatan buku
- Pembuatan video promosi
- Pembuatan video presentasi.