PROPOSAL PROYEK AKHIR SKRIPSI

STMIK LPKIA

PROGRAM STUDI TEKNIK INFORMATIKA

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Nama | : | Afif Farakhan | NRP | : | 161014039 |
| Program Studi | : | Teknik Informatika | Kelas | : | 4IF-01 |
| Konsentrasi | : | Teknik Informatika | Diperiksa Tanggal | : |  |
| Pembimbing | : | Charel Samuel M., S.T., M.Kom. | Presentasi | : |  |
| (Charel Samuel M., S.T., M.Kom.)  Pembimbing | | | ( )  Penilai Seminar | | |

**1. JUDUL**

Penerapan Sistem Kriptografi Hybrid Menggunakan Algoritma RSA Dan AES Pada Aplikasi Email Berbasis Web

1. **LATAR BELAKANG**

Di zaman modern saat ini, komunikasi melalui internet merupakan kegiatan yang kita lakukan sehari-hari baik itu untuk keperluan sekolah, pekerjaan sampai kegiatan bisnis sekalipun . Dalam berkomunikasi di internet kita biasanya menggunakan layanan-layanan seperti email, aplikasi chatting dll. Dan terkadang kita pun perlu menyampaikan suatu informasi yang penting atau rahasia yang tidak boleh diketahui oleh pihak-pihak yang tidak berhak untuk mengetahuinya. Namun sayangnya internet bukanlah tempat yang aman bagi kita untuk berbagi informasi rahasia seperti ini dikarenakan adanya pihak-pihak yang mungkin dapat mengambil, membaca bahkan mensabotase pesan kita sehingga dalam berkomunikasi di internet kita butuh yang namanya keamanan.

Kriptografi merupakan ilmu untuk menjaga kerahasiaan suatu pesan ,berita atau informasi dimana pesan diubah atau dienkripsi menjadi suatu rangkaian yang tidak dapat dimengerti sampai pesan yang dienkripsi itu didekripsi sehingga isi pesan asli nya dapat dibaca oleh orang-orang yang berhak atau memiliki kunci untuk mendekrpsi pesan tersebut. Dari dua jenis kriptografi yang ada yaitu simetris dan asimetris ternyata kedua-dua nya memiliki kelebihan dan kelemahan masing-masing. Namun kelemahan ini dapat diatasi dengan adanya kriptografi jenis hybrid atau hybrid cryptography yang mana menggabungkan keunggulan kedua jenis kriptografi tersebut.

1. **RUMUSAN MASALAH**

Berdasarkan uraian dari latar belakang diatas, maka dapat dirumuskan duatu pokok permasalahan sebagai berikut:

1. Bagaimana penerapan kriptografi hybrid dengan algoritma RSA dan AES pada aplikasi email berbasis web.
2. Bagaimana proses enkripsi dan dekripsi pada sebuah pesan teks menggunakan sistem kriptografi hybrid..
3. Bagaimana tingkat keamanan kriptografi hybrid dibandingkan dengan kriptografi simetris dan asimetris saja.
4. Berapa lama waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pada sebuah pesan teks menggunakan kriptografi hybrid dengan algoritma RSA dan AES.
5. **TUJUAN DAN KEGUNAAN**

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan kriptografi hybrid pada aplikasi email berbasis web dengan menggunakan alogirtma kriptografi RSA dan AES.
2. Mengetahui proses enkripsi dan dekripsi pada sebuah pesan teks dengan menggunakan sistem kriptografi hybrid.
3. **METODOLOGI PENYELESAIAN MASALAH**
4. **KAJIAN PUSTAKA**

**7. TEMPAT PRAKTIK KERJA** \*Jika belum mendapatkan tempat PKL maka dapat dikosongkan terlebih dahulu

1. Nama Perusahaan :
2. Alamat Perusahaan :
3. Telepon :
4. Nama Pimpinan :
5. Praktik di Bagian :
6. Nama Pembimbing :
7. Jabatan Pembimbing :
8. Mulai PKL Tanggal :