**PROPOSAL PROYEK AKHIR SKRIPSI**

**STMIK LPKIA**

**PROGRAM STUDI TEKNIK INFORMATIKA**

|  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- | --- |
| |  |  |  |  |  |  | | --- | --- | --- | --- | --- | --- | | Nama Mahasiswa | : | Afif Farakhan | NRP | : | 161014039 | | Program Studi (PS) | : | 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.

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 kriptografi hybrid dapat menangani kelemahan kriptografi simetris dan asimetris.
2. Bagaimana penerapan sistem kriptografi hybrid dengan algoritma RSA dan AES pada sebuah pesan teks.
3. **TUJUAN DAN KEGUNAAN**

Adapun tujuan dari penelitian ini adalah sebagai berikut:

1. Untuk mengimplementasikan sistem kriptografi hybrid pada sebuah pesan teks dengan menggunakan algoritma kriptografi RSA dan AES.
2. Mengetahui proses enkripsi dan dekripsi pada sebuah pesan teks dengan menggunakan sistem kriptografi hybrid.
3. **METODOLOGI PENYELESAIAN MASALAH**

Kriptografi simetris merupakan kriptografi yang cepat untuk digunakan namun, kriptografi ini memiliki tingkat keamanan yang kurang baik dikarenakan kunci untuk mengenkripsi dan mendekripsi merupakan satu kunci yang sama sehingga siapapun yang mengetahui kunci tersebut dapat mendekrip dan mengetahui isi pesan nya. Sedangkan krptografi asimetris merupkana kriptografi yang kuat karena memiliki dua kunci yaitu kunci publik dan kunci privat namun, kriptografi ini memerlukan waktu yang lebih lama sehingga dalam mengenkripsi pesan yang banyak akan memakan waktu yang sangat lama.

Untuk mengatasi masalah ini maka digunakanlah sistem kriptografi hybrid. Algoritma-algoritma kriptografi yang digunakan adalah penggabungan algoritma RSA dan AES. Untuk Kriptografi simetris nya digunakan algoritma kriptografi AES (Advanced Encryption Standard) sedanagkan untuk kriptografi asimetris nya digunakan algoritma RSA (Rivest-Shamir-Adleman). Dengan menggunakan sistem kriptografi hybrid ini maka tujuan nya yaitu kelemahan-kelemahan dari sistem kriptografi simetris dan asimetris dapat diatasi sehingga menghasilkan sistem kriptografi yang cepat seperti sistem kriptografi simetris dan aman seperti sistem kriptografi asimetris.

1. **KAJIAN PUSTAKA**

[1] Albert Ginting. Implementasi Algoritma Kriptografi RSA Untuk Enkripsi dan Dekripsi Email, Jurnal Teknologi dan Sistem Komputer, Vol.3 No.2, April 2015.

[2] Asri Prameshwari. Implementasi Algoritma Advanced Encryption Standard (AES) 128 Untuk Enkripsi dan Dekripsi File Dokumen, Eksplora Informatika Vol. 8, No 2, September 2018.

[3] Ahmad Pudoli. Penggunaan Hybrid Cryptosystem Untuk Enkripsi dan Dekripsi Pesan Messanger Menggunakan Algoritma Rivest Shamir Adleman (RSA) Dan Advanced Encryption Standard (AES) Dengan Firebase Pada Android, Jurnal Telematika MKOM Vol. 9 No 3, November 2017.

[4] Jamaludin. Rancang Bangun Kombinasi Hill Cipher dan RSA Menggunakan Metode Hybrid Cryptosystem, Publikasi Jurnal & Penelitian Teknik Informatika Vol. 2 No 2, April 2018.

[5] Oris Krianto Sulaiman. Hybrid Cryptosystem Menggunakan XOR Cipher dan Merkle-Hellman Knapsack Untuk Menjaga Kerahasiaan Pesan Digital, Jurnal Teknologi Informasi Vol. 3, No 2, Desember 2019.

[6] Sebastian Suhandinata. Analisis Performa Kriptografi Hybrid Algoritma Blowfish dan Algoritma RSA, Jurnal Teknologi dan Informasi Vol. 6, No 1, Desember 2019.

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

1. Nama Perusahaan : Digital Oasis
2. Alamat Perusahaan : Jl. Unoar III No. 13, Sukawarna, Kec. Sukajadi, Kota Bandung, Jawa Barat 40164
3. Telepon : (022) 88888989
4. Nama Pimpinan :
5. Praktik di Bagian :
6. Nama Pembimbing :
7. Jabatan Pembimbing :
8. Mulai PKL Tanggal : 2 Maret 2020