

BAB I

PENDAHULUAN

1.1.Latar Belakang

Pesatnya perkembangan teknologi informasi saat ini, khususnya internet. Sangat mungkin sekali untuk saat ini lembaga pendidikan dapat memberikan layanan informasi yang baik. Perkembangan teknologi informasi khususnya dalam dunia pendidikan ini berkembang dengan cepat terutama pada pandemi, kurang lebih selama 2 tahun ke belakang ini. Hampir seluruh kegiatan yang biasa dilakukan disekolah berubah sangat drastis menjadi online. Selain pandemi kemarin ternyata sudah diterapkan proses pengiriman data secara online dari satu sekolah ke dinas pendidikan atau ke suatu lembaga untuk keperluan tertentu, sebagai contoh proses SNMPTN dimana setiap siswa terpilih dapat mengirimkan data pribadi khususnya nilai rapor untuk keperluan daftar perguruan tinggi.

Penggunaan teknologi dalam proses pengiriman data secara *online* tersebut tentu diharapkan dapat berjalan sesuai yang direncanakan. Namun, tidak dapat disangkal bahwa orang yang tidak bertanggung jawab dapat melakukan kejahatan dunia maya untuk mencuri, mengubah, atau hal lain yang dapat merugikan. Berdasarkan artikel berita (cyberthreat.id) tercatat kurang lebih 12 kasus kebocoran data terjadi sejak 2019 di Indonesia, ini menjadi sebuah peringatan bahwa kebocoran data di Indonesia sangat rentan terjadi.

Sebuah data menjadi hal penting pada saat ini terutama pada bidang akademik maka diperlukan suatu keamanan yang cukup pada sebuah *database*. Untuk menjamin keamanan sebuah data tersebut kita memerlukan keamanan data. Keamanan data adalah upaya untuk melindungi data dari hal-hal yang tidak diinginkan. Ada beberapa metode untuk keamanan data salah satunya adalah dengan teknik penyandian atau biasa kita sebut dengan kriptografi.

Kriptografi berperan penting dalam menjaga informasi sehingga menyulitkan pengguna atau pihak yang tidak bertanggung jawab untuk memperoleh informasi tersebut. Pada penelitian ini dilakukan pengamanan data menggunakan dua metode dari *Symmetric Key Cryptography* atau Kriptografi Kunci Simetris dan *Asymmetric Key Cryptography* atau Kriptografi Kunci asimetris yaitu *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA) pada data siswa. Hal ini bertujuan agar dapat memaksimalkan proses enkripsi dan dekripsi data siswa agar dapat menghasilkan suatu keamanan data yang bisa dibilang cukup aman karena menggunakan 2 metode dari kriptografi kunci simetris dan asimetris.

Pemilihan 2 jenis algoritma tersebut dipilih dengan pertimbangan yang cukup. Pemilihan 2 algoritma tersebut dipilih karena dinilai dapat menutupi kekurangan dari satu algoritma dan diharapkan dapat memberikan keuntungan dan keunggulan untuk suatu keamanan data.

Berdasarkan latar belakang, penelitian ini mengusulkan untuk menggunakan 2 metode *Symmetrics Key Cryptography* atau Kriptografi Kunci Simetris dan *Asymmetrics Keys Cryptography* atau Kriptografi Kunci asimetris yaitu *International Data Encryption Algorithmad* (IDEA) dan *Rivest Shamir Adleman* (RSA) sebagai solusi dalam pengamanan pada database. Sehingga penelitian ini mengambil judul **“PENERAPAN KEAMANAN DATA SISWA MENGGUNAKAN INTERNATIONAL DATA ENCRYPTION ALGORITHM (IDEA) DAN RIVEST SHAMIR ADLEMAN (RSA)”**.

1.2.Rumusan Masalah

Agar berfokus terhadap permasalahan tertentu berdasarkan latar belakang diatas maka Rumusan Masalah pada penelitian ini yaitu :

- a. Apakah proses penerapan keamanan data menggunakan algoritma IDEA dapat mengamankan data siswa?
- b. Apakah dengan menambahkan algoritma RSA dapat mengamankan kunci dari algoritma IDEA?

- c. Apakah terdapat penambahan karakter pada penerapan algoritma IDEA dan RSA?

1.3. Batasan Penelitian

Agar penelitian ini tetap berada dalam batasan yang diinginkan dan dapat mencapai hasil yang optimal, maka pada penelitian ini dibatasi sebagai berikut :

- a. Algoritma yang digunakan dalam proses enkripsi dan dekripsi untuk pengamanan data menggunakan algoritma kriptografi simetris IDEA dan algoritma asimetris RSA.
- b. Penggunaan data dalam penelitian ini menggunakan data siswa yang merupakan siswa eligible dari SMAN 99 Jakarta yang terdiri dari NIS, NISN, kelas, nama, nilai semester 1 – 5 yang terdiri dari (Bahasa Indonesia, Matematika, Bahasa Inggris, Biologi, Fisika, Kimia).
- c. Parameter hasil penelitian dalam penelitian ini adalah keberhasilan pada penerapan enkripsi dan dekripsi menggunakan algoritma simetris IDEA dan penerapan enkripsi dan dekripsi kunci menggunakan algoritma asimetris RSA, selain itu dapat mengetahui efisiensi waktu yang dibutuhkan pada proses tersebut.
- d. Program yang dibuat dalam penelitian ini dibuat dalam bentuk *website* yang dapat melakukan penerapan enkripsi dan dekripsi pada proses input data siswa ke database.

1.4. Tujuan Penelitian

Berdasarkan latar belakang, rumusan masalah, dan batasan penelitian yang dilakukan pada penelitian ini maka tujuan dari penelitian ini adalah:

- a. Menerapkan algoritma kriptografi simetris IDEA dan algoritma kriptografi asimetris RSA dalam penerapan enkripsi dan dekripsi untuk menjaga

kerahasiaan data dari kejahatan oleh seseorang yang tidak bertanggung jawab.

- b. Proses enkripsi dan dekripsi menggunakan algoritma kriptografi kunci simetris IDEA dan algoritma kriptografi kunci asimetris RSA menjadi pilihan dalam sistem penerapan enkripsi dan dekripsi yang lebih baik

1.5 Manfaat Penelitian

Agar memberikan informasi dan pengetahuan yang dibutuhkan untuk memecahkan permasalahan diatas, manfaat yang diperoleh dari penelitian ini sebagai berikut :

- a. Pada penelitian ini dapat memberi pengetahuan dan pengalaman yang baru sebagai penulis dalam keamanan data menggunakan algoritma kriptografi.
- b. Hasil dari penelitian bisa dijadikan suatu bahan pertimbangan atau bisa dikembangkan, dan dapat menjadi bahan referensi terkait penerapan pengamanan data menggunakan *International Data Encryption Algorithm* (IDEA) dan *Rivest Shamir Adleman* (RSA)
- c. Hasil dari penelitian ini bermanfaat untuk meningkatkan keamanan dan bermanfaat untuk menjaga kerahasiaan pada data dari seseorang yang tidak berkepentingan dalam mengetahui data dan informasi tersebut.

1.6.Luaran yang Diharapkan

Hasil dari penelitian ini diharapkan dapat menghasilkan keberhasilan dalam penerapan enkripsi dan dekripsi menggunakan algoritma kriptografi simetris IDEA dan algoritma kriptografi asimetris RSA.

1.7.Sistematika Penulisan

Penataan penulisan pada penelitian ini disusun dalam 5 bab yang didalamnya terdiri beberapa sub bab dan daftar pustaka yang saling terkait antara satu dengan yang lainnya. Melalui sistematika penulisan ini diharapkan dapat mempermudah dalam memahami materi secara ringkas. Isi setiap bab dalam penelitian ini meliputi:

BAB I PENDAHULUAN

Bagian ini menjelaskan tentang latar belakang penulisan, rumusan masalah, batasan penelitian, tujuan penulisan, manfaat penelitian, luaran yang diharapkan dan sistematika penulisan.

BAB II LANDASAN TEORI

Bagian ini membahas beberapa teori yang mendukung atau menunjang dengan pokok pembahasan yang mendasari penulisan pada penelitian ini.

BAB III METODOLOGI PENELITIAN

Bagian ini menjelaskan tentang metode yang digunakan dalam penelitian ini. Yang terdiri dari kerangka pikir untuk menggambarkan tahapan pada penelitian ini, serta tahapan perancangan perangkat lunak, alat bantu yang digunakan pada penelitian serta jadwal penelitian.

BAB IV HASIL DAN PEMBAHASAN

Bagian ini menjelaskan perancangan dan hasil yang sudah direncanakan pada bab sebelumnya, Serta menganalisis hasil dari proses tersebut.

BAB V KESIMPULAN DAN SARAN

Bagian ini menjelaskan hasil yang dapat disimpulkan dalam penelitian ini, seta saran untuk proses pengembangan selanjutnya.

DAFTAR PUSTAKA