BAB I
PENDAHULUAN

1.1 Latar Belakang

Dalam komunikasi modern, video telah menjadi salah satu media yang populer untuk berbagi informasi, baik dalam konteks pribadi maupun bisnis. Terkadang, ada kebutuhan untuk menyembunyikan pesan rahasia di dalam video tersebut tanpa diketahui oleh pihak yang tidak berwenang. Pesan-pesan penting yang disembunyikan di dalam video tersebut perlu dijaga keamanan dan kerahasiaannya agar tidak jatuh ke tangan yang salah. Jika dirunut dari Al-Quran terdapat suatu ayat yang menjelaskan tentang tindakan yang melanggar privasi, yaitu suatu tindakan yang dapat diartikan sebagai tindakan pengambilan, pengubahan, atau pengaksesan terhadap data pribadi seseorang tanpa izin terlebih dahulu dari pemiliknya.

Dalam Islam telah diatur dengan jelas tentang pentingnya menjaga privasi seseorang. Di dalam QS. An-Nur ayat 27 disebutkan :

يٰٓاَيُّهَا الَّذِيْنَ اٰمَنُوْا لَا تَدْخُلُوْا بُيُوْتًا غَيْرَ بُيُوْتِكُمْ حَتّٰى تَسْتَأْنِسُوْا وَتُسَلِّمُوْا عَلٰٓى اَهْلِهَاۗ ذٰلِكُمْ خَيْرٌ لَّكُمْ لَعَلَّكُمْ تَذَكَّرُوْنَ

Yang artinya : "*Wahai orang-orang yang beriman! Janganlah kamu memasuki rumah yang bukan rumahmu sebelum meminta izin dan memberi salam kepada penghuninya. Yang demikian itu lebih baik bagimu, agar kamu selalu ingat*".

Ayat tersebut menjelaskan pentingnya sebuah privasi dimana tidak diperbolehkan seseorang untuk mengetahui sebuah informasi pribadi orang lain. Pada penelitian ini privasi yang akan dijaga kerahasiaannya adalah berupa sebuah pesan yang berisi informasi rahasia. Salah satu metode yang umum digunakan untuk menjaga kerahasiaan pesan adalah kriptografi. Kriptografi adalah ilmu dan seni mengamankan informasi dengan mengubah pesan menjadi bentuk yang tidak terbaca, kecuali oleh pihak yang ditujukan. RSA (Rivest-Shamir-Adleman) adalah salah satu algoritma kriptografi yang sangat kuat yang digunakan dalam banyak

aplikasi keamanan. Di sisi lain, penyematan pesan adalah teknik yang digunakan untuk menyembunyikan pesan rahasia ke dalam media digital tanpa mengubah secara signifikan kontennya. Salah satu metode penyematan pesan yang umum digunakan adalah Least Significant Bit (LSB) dan algoritma LSB2BIT yang digunakan dalam konteks ini.

Di sebuah dunia yang semakin terhubung secara digital, pesan-pesan rahasia menjadi semakin rentan terhadap risiko keamanan. Perlunya mengamankan pesan sebelum distribusi menjadi sebuah keharusan mutlak untuk melindungi informasi yang bersifat rahasia dan sensitif. Sebagai kebijakan umum, banyak organisasi dan individu yang memahami pentingnya memastikan bahwa komunikasi mereka tidak jatuh ke tangan yang tidak berhak. Pertama-tama, melalui pengamanan pesan rahasia, kita dapat melindungi informasi pribadi dan bisnis dari upaya penyadapan atau serangan siber. Dalam era di mana teknologi informasi berkembang pesat, keberhasilan dalam mengamankan pesan menjadi kunci untuk mencegah akses ilegal dan pengungkapan informasi yang dapat merugikan.

Selain itu, melindungi pesan rahasia juga mendukung pembangunan dan pemeliharaan kepercayaan di antara pihak-pihak yang terlibat. Dalam konteks bisnis, rahasia perusahaan, rencana strategis, dan informasi kritis lainnya adalah aset yang sangat berharga. Keamanan yang kuat pada tahap distribusi pesan membantu memastikan bahwa informasi ini hanya dapat diakses oleh pihak yang sah, memperkuat kerjasama dan kepercayaan di antara para pemangku kepentingan. Perlunya mengamankan pesan sebelum distribusi juga berkaitan erat dengan perlindungan privasi individu. Pesan-pesan pribadi yang diungkapkan secara online atau melalui media digital harus dikelola dengan hati-hati untuk mencegah penyalahgunaan atau eksploitasi. Dengan menerapkan langkah-langkah keamanan yang efektif, kita dapat memastikan bahwa hak privasi individu tetap terlindungi. Secara keseluruhan, perlunya mengamankan pesan rahasia sebelum distribusi merupakan langkah proaktif untuk menghadapi tantangan keamanan modern. Dengan menerapkan teknologi enkripsi, protokol keamanan, dan praktik-praktik terbaik lainnya, kita dapat menjaga kerahasiaan informasi yang vital, mendukung

keberlanjutan operasional, dan membangun dasar kepercayaan di dalam komunikasi digital.

Berdasarkan penelitian terdahulu yang dilakukan oleh Paramita & Usman Sudibyo, 2021. Penelitian ini bertujuan untuk meneliti tentang pengamanan dari file mp3 dengan algoritma asimetris RSA dan simetris transposisi kolumnar. Hasilnya, dengan menggabungkan kedua algoritma tersebut, sistem aplikasi akan memiliki kemampuan untuk mengelola file mp3 dan mengenkripsi file mp3 dengan hasil data yang tidak dapat di putar layaknya file mp3 pada umumnya. Penelitian lainnya yang dilakukan oleh Wati et al., 2020. Penelitian ini bertujuan untuk mengamankan data dengan menggunakan Cipher Block Chaining (CBC) kemudian hasil enkripsi tersebut diamanakan melalui citra digital menggunakan algoritma LSB. Penelitian tersebut menghasilkan sebuah aplikasi yang dapat digunakan untuk melakukan enkripsi data menggunakan algoritma CBC dan menyisipkan hasil enkripsi ke dalam sebuah citra menggunakan algoritma LSB. Berdasarkan penelitian yang telah dilaksanakan tersebut, pada penelitian ini akan digunakan algoritma RSA dan LSB2bit untuk melakukan pengamanan dan penyematan pesan ke dalam sebuah video digital untuk menghasilkan tingkat keamanan yang lebih baik dalam melindungi sebuah pesan yang bersifat rahasia.

Algoritma RSA telah terbukti aman dan kuat dalam menjaga kerahasiaan data. Dengan menggunakan algoritma RSA, pesan dapat dienkripsi sebelum disisipkan ke dalam video. Algoritma ini menggunakan pasangan kunci publik dan kunci privat untuk melakukan enkripsi dan dekripsi data. Dengan demikian, hanya pihak yang memiliki kunci privat yang dapat membaca pesan yang disisipkan. Namun, algoritma RSA saja tidak cukup untuk menyisipkan pesan ke dalam video secara tidak terlihat. Oleh karena itu, algoritma LSB2bit digunakan sebagai pendekatan tambahan. Algoritma LSB2bit memanfaatkan bit paling tidak signifikan dalam piksel-piksel video yang dapat dimanipulasi tanpa mengganggu kualitas visual secara signifikan. Dengan menggunakan metode ini, pesan dapat disisipkan dengan cara yang tidak terlihat oleh mata manusia.

Berdasarkan latar belakang tersebut, pada penelitian ini akan dibangun sebuah aplikasi yang dapat digunakan untuk melakukan keamanan pesan dan

melakukan penyematan pesan yang telah diamankan ke dalam video digital menggunakan algoritma RSA dan LSB2bit. Maka pada penelitian ini akan ditarik sebuah judul berupa "**Implementasi Penyematan Pesan Ke Dalam Video Menggunakan Algoritma RSA Dan LSB2bit**".

1.2 Rumusan Masalah

Berikut rumusan masalah yang akan dicari pemecahannya melalui penelitian ini, antara lain :

1. Bagaimana mengimplementasikan algoritma RSA dan LSB2BIT dalam penyematan pesan ke dalam video ?
2. Bagaimana membangun sebuah aplikasi yang dapat digunakan untuk menyematkan pesan ke dalam video menggunakan algoritma RSA dan LSB2BIT ?

1.3 Batasan Masalah

Dalam penulisan penelitian ini dibatasi permasalahannya sebagai berikut :

1. Penelitian ini berfokus pada penyematan pesan ke dalam video menggunakan algoritma RSA dan LSB2BIT.
2. Pesan yang dapat disisipkan adalah berupa teks yang dapat di inputkan secara langsung melalui aplikasi serta dapat terdiri dari huruf, angka dan simbol.
3. Penyematan pesan hanya dilakukan pada format video MP4.
4. Durasi file video yang akan digunakan sebagai media uji coba adalah maksimal selama 2 menit.
5. Proses penyisipan akan gagal jika pesan yang di input lebih panjang dibanding ukuran file video yang digunakan.
6. Analisis keamanan akan difokuskan pada tingkat keamanan pesan yang disematkan dengan menggunakan algoritma RSA.
7. Proses penyematan pesan ke dalam video dilakukan menggunakan algoritma LSB2BIT.
8. Sistem pada penelitian ini akan dibangun menggunakan perangkat lunak Android Studio dengan bahasa pemrograman Java dan XML.
9. Sistem yang akan dihasilkan pada penelitian ini ditujukan penggunaannya pada perangkat mobile dengan sistem operasi Android.

1.4 Tujuan Penelitian

Tujuan dari pelaksanaan penelitian ini dapat disimpulkan menjadi poin sebagai berikut :

1. Menerapkan algoritma RSA dan metode LSB2BIT dalam penyematan pesan ke dalam video.
2. Membangun sebuah aplikasi yang dapat digunakan untuk menyematkan pesan ke dalam video menggunakan algoritma RSA dan LSB2BIT.

1.5 Manfaat Penelitian

Yang menjadi manfaat dari pelaksanaan penelitian ini dapat dilihat sebagai berikut :

1. Penelitian ini dapat memberikan sumbangan pengetahuan dan wawasan baru dalam bidang kriptografi, penyematan pesan, dan keamanan informasi.
2. Aplikasi yang dihasilkan dari penelitian ini dapat digunakan secara umum untuk dijadikan sebagai media untuk mengamankan pesan sebelum mengirimkannya ke penerima.
3. Hasil penelitian ini dapat digunakan sebagai referensi dan sumber pembelajaran dalam pengajaran mata kuliah yang berkaitan dengan keamanan informasi, kriptografi, dan pengolahan media digital.

UNIVERSITAS ISLAM NEGERI
SUMATERA UTARA MEDAN