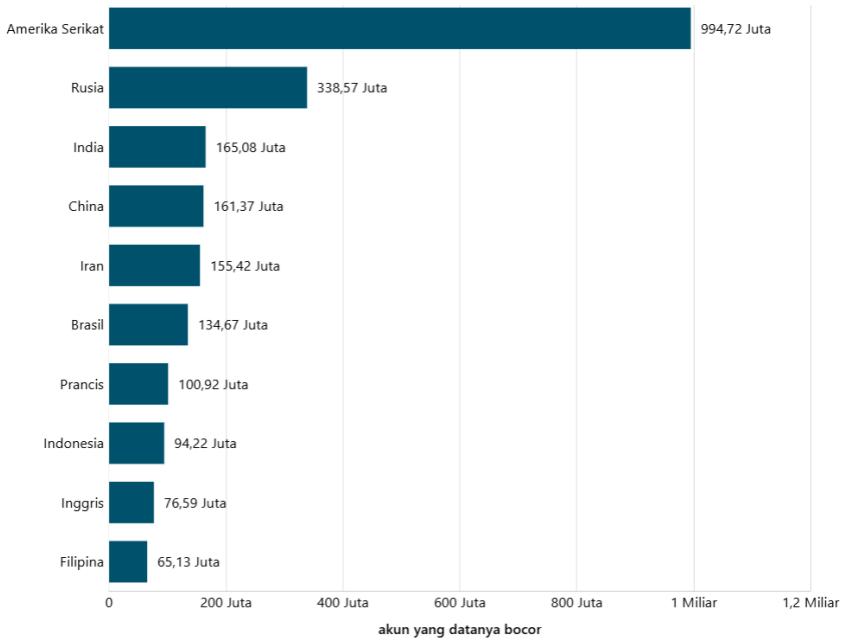
BAB I
PENDAHULUAN

1.1 Latar Belakang

Kemudahan dalam membagikan dan mendapatkan media digital seperti gambar, audio, video dan teks semakin pesat. Karena adanya perkembangan teknologi ini membuat sebuah informasi menjadi kebutuhan pokok bagi masyarakat atau organisasi. Informasi merupakan suatu hal yang penting bagi masyarakat modern saat ini maupun sebuah perusahaan, karena dengan adanya informasi ini kehidupan manusia modern dapat berjalan dengan baik. Dengan pesatnya perkembangan teknologi informasi, terutama internet, terjadi peningkatan signifikan dalam kasus *cybercrime*. Salah satu tantangan utama yang dihadapi dalam berbagi dan mentransmisikan berbagai jenis informasi melalui saluran publik adalah masalah keamanan data. Ancaman seperti penyadapan, pencurian, dan pemalsuan informasi melalui jaringan komputer dapat memberikan kerugian besar bagi pemilik informasi.[1].

Menurut laporan dari *Surfshark*, perusahaan *virtual private network* (*VPN*) asal Belanda, selama Januari 2020 - Januari 2024 ada sekitar 3,96 miliar akun digital yang mengalami kebocoran data[2]. Angka tersebut merupakan estimasi berdasarkan riset *Surfshark* terhadap kasus kebocoran data di 250 negara. Kebocoran data atau *data breach* merupakan keadaan dimana data suatu akun digital dapat diakses secara illegal oleh pihak selain pemilik. Data yang bocor tersebut berupa data pribadi, seperti nama lengkap, jenis kelamin, lokasi geografis, alamat *email*, kata sandi akun, nomor telepon dsb.



Gambar 1. 1 Kasus Kebocoran Data Tertinggi di Dunia

Berdasarkan hasil survei yang dilakukan oleh *Surfshark* dalam periode tersebut Indonesia menjadi negara dengan kebocoran data terbanyak ke-8 di dunia, dengan estimasi 94,22 juta akun bocor. *Cybercrime* tidak hanya mengancam individu tetapi juga organisasi dan negara, sehingga keamanan data menjadi prioritas utama. Pemerintah Indonesia pun tak luput dari sorotan kasus *cybercrime*. Menurut Badan Siber dan Sandi Negara (BSSN) sepanjang 2023 ada sekitar 1.67 juta data kredensial dari instansi Indonesia terekspos di *Darknet*[3]. *Darknet* merupakan jaringan internet yang tidak bisa dengan mudah diakses lewat peramban konvensional legal hukum seperti *google*. *Darknet* hanya bisa diakses melalui perangkat lunak khusus dengan menggunakan protokol komunikasi komputer yang tidak umum.

REKAPITULASI DARKNET EXPOSURE 2023

Sektor	Jumlah Data Exposure	Jumlah Instansi
Adm. Pemerintahan	665.916	134
Lainnya	586.597	56
Keuangan	165.085	58
TIK	161.282	29
Transportasi	56.925	63
ESDM	29.350	19
Kesehatan	3.785	45
Pangan	3.287	17
Pertahanan	1.958	8

Gambar 1. 2 Data Rekapitulasi Kasus *Darknet Exposure* 2023

Berdasarkan Gambar 1.2 BSSN menginformasikan sebanyak 1.674.185 data exposure yang mempengaruhi 429 instansi. Data nasional tersebut pada 2023 paling banyak berada pada sektor administrasi pemerintahan, yaitu sekitar 665 ribu data (39.9%). Kemudian diikuti oleh sektor Keuangan dengan 165 ribu data (9,86%), sektor Teknologi Informasi dan Komunikasi (TIK) dengan 161 ribu data (9,63%), sektor Transportasi dengan 56 ribu data (3,40%), Energi dan Sumber Daya Mineral (ESDM) dengan 29 ribu data (1,75%), Kesehatan dengan 3.7 ribu data (0,23%), Pangan dengan 3.2 ribu data (0,2%), Pertahanan dengan 1.9 ribu data (0,12%), dan sektor lainnya sebesar 586 ribu data (35,04%).

Kasus pencurian data telah beberapa kali terjadi di Indonesia seperti kasus pencurian data oleh seseorang yang mengidentifkasikan dirinya dengan nama “Bjorka” pada Mei 2023 lalu telah mencuri 19,56 juta data pengguna BPJS Ketenagakerjaan[4]. BPJS

Ketenagakerjaan ini merupakan salah satu instansi Kesehatan negara yang membantu masyarakat dalam memproses pembayaran pengobatan masyarakat. Dengan produk dari BPJS ini yaitu berupa kartu yang nantinya pada saat pembayaran pengobatan masyarakat akan mendapat gratifikasi. Bjorka mengunggah hasil curiannya dengan judul "BPJS Ketenagakerjaan Indonesia 19Million" pada *Breach Forums* yang merupakan situs terlarang atau dikenal (dark web). Tidak cukup hanya mengunggah sebesar 100.000 data, Bjorka menjual data-data tersebut bagi siapapun yang tertarik dengan nominal sebesar US$10.000 atau dalam rupiah setara Rp.154 juta.

Oleh karena itu, upaya untuk melindungi informasi yang dikirimkan terhadap seorang penyadap dan pihak yang tidak bertanggungjawab menjadi sebuah kebutuhan. Seperti Kriptografi dan Steganografi sangat disarankan sebagai bentuk upaya keamanan tersebut. Kriptografi adalah seni dan ilmu menjaga kerahasiaan data. Pada kriptografi, data asli diubah menjadi bentuk lain yang tidak dapat dibaca menggunakan suatu algoritma yang menghasilkan suatu key. Steganografi adalah seni dan ilmu menyembunyikan data pada media lain sebagai cover (misalnya citra) sehingga terlihat samar. Steganografi membutuhkan dua properti, yaitu pesan dan media penampung. Media penampung yang umumnya digunakan sekarang dapat berupa teks, suara, gambar, atau video. Sedangkan pesan yang disembunyikan dapat berupa teks, gambar, atau pesan lainnya. Penggabungan steganografi dan kriptografi secara bersamaan dapat meningkatkan pengamanan data. Metode penggabungan steganografi dan kriptografi banyak dikembangkan.

Salah satu penerapan penggabungan algoritma kriptografi RSA dan *El-Gamal* pada suatu penelitian yang dilakukan oleh Ahmad Miftah Fajrin, Jeremy Richard Benedict dan Henri Jayanata Kusuma pada Februari 2023[5]. Pada penelitiannya diterapkan algoritma RSA dan *El-Gamal* dengan mengenkripsi suatu pesan rahasia berformat

teks yang bertujuan untuk menganalisis performa kedua algoritma kriptografi tersebut. Kemudian menghasilkan kesimpulan bahwasan nya algoritma RSA melakukan proses enkripsi dan dekripsi unggul dalam kecepatannya dibandingkan algoritma *El-Gamal*. Serta kedua algoritma kriptografi RSA dan *El-Gamal* memiliki masing-masing kelebihan yaitu proses generate kunci yang kompleks pada RSA yaitu tingkat kesulitan dalam pemfaktoran bilangan non prima menjadi factor primanya sedangkan *El-Gamal* terletak pada kesulitan perhitungan modulus logaritmik diskrit dari bilangan prima besar dan pada pesan teks yang sama mampu menghasilkan pesan teks rahasia unik yaitu pesan rahasia akan selalu berbeda setiap di-enkripsi.

Penerapan metode *Least Significant Bit (LSB)* dalam proses pengamanan data dengan menyembunyikan keberadaan pesan asli pada suatu media penampung juga pernah diterapkan pada suatu penelitian yang dilakukan oleh Indra Gunawan dan Sumarno pada tahun 2018[6]. Pada penelitian tersebut berfokus pada pengimplementasian kombinasi dari kriptografi dan steganografi pada pesan teks dan media berupa video. Dimana diawal dilakukan proses input media penampung berupa file video berformat *MPEG*. Kemudian dilanjutkan dengan memasukkan *password* pada proses penyisipannya yang nantinya juga digunakan untuk mengekstraksi file video untuk mengeluarkan pesan yang disembunyikan. Sementara penelitian tersebut menghasilkan suatu kesimpulan bahwasannya metode *LSB* bisa dijadikan suatu upaya untuk memberikan pengamanan terhadap pesan yang ingin dikirimkan pada penerima dalam bentuk video.

Untuk mendukung penelitian ini diperlukan suatu pengujian guna meningkatkan validitas pada hasil yang didapatkan, yaitu pengujian dengan *blacbox testing. Blackbox testing* merupakan suatu metode pengujian software tanpa harus memperhatikan detail software. Pengujian ini berfokus pada output yang dihasilkan dari

masing-masing inputan yang diberikan. Kelebihan penerapan *blackbox testing* yaitu penguji tidak perlu memiliki pengetahuan mendalam tentang bahasa pemrograman tertentu, sehingga pengujian dilakukan dari sudut pandang pengguna guna membantu menunjukkan inkonsistensi pada persyaratan sistem[7].

Dari uraian tersebut, penulis mencoba memberikan judul pada penelitian ini yaitu "ANALISIS PENGEMBANGAN APLIKASI MENGGUNAKAN ALGORITMA RSA DAN *EL-GAMAL* PADA TEKNIK STEGANOGRAFI DENGAN METODE *LEAST SIGNIFICANT BIT (LSB)* sehingga diharapkan dari penelitian ini dapat memberikan dampak positif bagi banyak kalangan terutama pada upaya pengamanan data.

1.2 Rumusan Masalah

Tingkat kejadian pencurian data yang semakin marak bahkan merambah pada institusi negara menjadikan suatu ancaman dimana dalam kegiatan hidup saat ini yang serba digital. Berdasarkan uraian dari latar belakang diatas, ditetapkan rumusan masalah pada penelitian ini yaitu:

1. Bagaimana merancang suatu sistem keamanan yang menerapkan teknik kombinasi kriptografi dan steganografi menggunakan algoritma RSA dan *El-Gamal* serta metode LSB sebagai bentuk upaya pengamanan data.
2. Bagaimana proses pengujian keefektifan sistem yang menerapkan teknik kombinasi kriptografi dan steganografi menggunakan algoritma RSA dan *El-Gamal* serta metode *LSB* dengan metode *blackbox testing*.

1.3 Pertanyaan Penelitian

Berdasarkan keterangan pada rumusan masalah diatas, maka timbul beberapa pertanyaan peneliti dalam melakukan penelitian ini yaitu:

1. Bagaimana penerapan algoritma RSA (River, Shamir, Alderman) dan algoritma *El-Gamal* pada sistem pengamanan data?
2. Bagaimana penerapan Steganografi dengan menggunakan metode *Least Significant Bit* pada sistem pengamanan data?

3. Bagaimana cara menganalisis kinerja algoritma RSA (*River, Shamir, Alderman*) dan algoritma *El-Gamal* dengan menerapakan pengujian *blackbox testing*?

1.4 Batasan Masalah

Berdasarkan keterangan yang terdapat pada bagian rumusan masalah dan tujuan penelitian, maka untuk mewujudkan penelitian yang sesuai dengan masalah yang ada terdapat batasan masalah penelitian sebagai berikut:

1. Pesan yang digunakan merupakan file format *(*docx)*.
2. Penerapan algoritma yang digunakan pada enkripsi dan dekripsi pesan ini menggunakan Algoritma Nirsimetris/Asimetris yaitu Algoritma RSA (River, Shamir, Alderman) dan Algoritma *El-Gamal*.
3. Metode steganografi yang digunakan pada penelitian kali ini yaitu *Least Significant Bit* dengan media file berupa format file audio *(*wav)*.
4. Pengujian sistem dilakukan dengan menerapkan metode *blackbox testing*

1.5 Tujuan Penelitian

Berdasarkan penjelasan rumusan masalah, dapat ditelaah tujuan penelitian sebagai berikut:

1. Merancang dan mengimplementasikan algoritma RSA dan *El-Gamal* serta metode *Least Significant Bit* pada sistem pengamanan data.
2. Mengetahui kelayakan algoritma RSA dan *El-Gamal* serta metode *Least Significant Bit* pada sebuah aplikasi sistem pengamanan data dengan pengujian *blacbox testing.*

1.6 Manfaat Penelitian

Setelah penjabaran dari uraian rumusan masalah, batasan masalah dan tujuan penelitian diatas, maka dapat diketahui manfaat dari penelitian ini yaitu:

1. Manfaat bagi peneliti

   Sebagai tambahan wawasan dan pengalaman dalam tahap pengembangan diri dan diharapkan dapat bermanfaat sebagai pedoman untuk penelitian selanjutnya.

2. Manfaat praktis bagi ilmu pengetahuan

   Memberikan pemahaman terkait pengembangan aplikasi dengan menerapkan algoritma RSA dan *El-Gamal* serta metode *LSB* sebagai upaya dalam pengamanan data. Sehingga dapat mengetahui algoritma mana yang efektif untuk tujuan dapat diimplementasikan.