BAB I
PENDAHULUAN

1.1 Latar Belakang Masalah

Berdasarkan data yang dirilis oleh Kementerian Komunikasi dan Informatika (Kominfo), jumlah pengguna internet di Indonesia pada tahun 2021 meningkat sebanyak 11% dibandingkan tahun sebelumnya, dari 175,4 juta meningkat menjadi 202,6 juta pengguna[1]. Data dari [2] jumlah pengguna internet di Indonesia tahun 2022 meningkat sebanyak 1,03% dibandingkan tahun sebelumnya dengan jumlah 204,7 juta pengguna internet. Salah satu keuntungan yang dapat diperoleh yaitu memberikan kemudahan pada proses komunikasi jarak jauh yang dilakukan melalui media telepon, sms, email, dan sebagainya. Dengan media tersebut, para pengguna dapat berbagi pesan dalam bentuk teks, foto, video, audio, bahkan dapat melampirkan file.

Disisi lain, kemajuan dalam bidang teknologi informasi dan komunikasi juga memiliki ancaman keamanan, diantaranya penyadapan jaringan dengan serangan *Man In The Middle* menggunakan teknik *sniffing* yang memiliki tujuan untuk mendapatkan data penting atau sensitif. Data tersebut didapatkan melalui media komunikasi yang terhubung pada jaringan yang tidak aman atau sudah terkena serangan *Man In The Middle*. Sehingga besar kemungkinan terjadi penyalahgunaan data yang sifatnya merugikan seperti yang terjadi pada kasus kebocoran data pribadi pengguna BPJS kesehatan pada bulan Mei 2021 dimana 279 juta data pengguna yang berisi NIK, nama, alamat rumah, nomor telepon, alamat e-mail, dan foto pengguna dijualbelikan di Raid Forums [3]. Untuk mencegah terjadinya penyalahgunaan data seperti pada kasus tersebut, dibutuhkan mekanisme keamanan untuk menjaga kerahasiaan informasi dari pesan yang dikirimkan. Tindakan pencegahan yang dapat dilakukan yaitu menerapkan teknik *hybrid* kriptosistem untuk mengenkripsi pesan dan diperkuat dengan teknik steganografi untuk menyembunyikan pesan tersebut ke dalam media *image* (citra).

Steganografi merupakan sebuah seni yang dapat digunakan untuk melakukan penyembunyian pesan ke dalam media file yang terdiri dari foto, audio, video, maupun dokumen yang memiliki tujuan agar isi pesan tidak mudah diketahui

oleh pihak yang tidak memiliki hak akses. Sedangkan enkripsi merupakan teknik yang digunakan untuk mengamankan data dengan cara mengubah *plaintext* menjadi kode rahasia yang tujuannya agar pesan atau file hasil enkripsi hanya dapat dibuka dan dibaca oleh orang yang berhak mengaksesnya menggunakan cara khusus yaitu deskripsi [4]. Sehingga pada penelitian ini menerapkan metode enkripsi simetris yang memiliki kunci enkripsi dan deskripsi yang sama dalam proses pengamanan pesan. Pada penelitian ini menerapkan *hybrid* kriptosistem yang memadukan metode enkripsi *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) kemudian diperkuat dengan teknik steganografi *Pixel Value Differencing* (PVD).

Hybrid kriptosistem dalam penelitian ini merupakan hasil perpaduan algoritma kriptografi klasik dan modern yang bersifat simetris. *Vigenere Cipher* merupakan metode kriptografi klasik yang dituliskan pada buku terbitan tahun 1553 berjudul *La Citra del. Sig Giovan Battista Bellaso*. Algoritma ini dinamakan *Vigenere* karena terinspirasi dari seorang peneliti bernama Blaise de Viggenere yang berhasil menemukan metode *autokey cipher* yang lebih aman dalam menghasilkan *keystream*. Metode ini merupakan hasil pengembangan dari algoritma dasar yang telah ditemukan oleh Givan Battista Bellaso [5]. Oleh karena itu, *Vigenere Cipher* tahan terhadap analisis frekuensi cipher karena algoritma ini berputar melalui pergeseran yang berbeda. Algoritma *Vigenere Cipher* dipadukan dengan *Advanced Encryption Standard* 128 bit (AES) yang ditemukan pada November 2001 oleh Rijmen dan Daemen. Saat itu, AES berhasil memenangkan kompetisi kriptografi yang diadakan oleh NIST dengan menyisihkan empat usulan algoritma lain, diantaranya RC6, *Twofish*, MARS, dan *Serpent*. Algoritma AES masuk ke dalam kategori *iteratedblock cipher* yang dapat mengubah ukuran blok *ciphertext* melalui komputasi yang dilakukan secara berulang. AES memiliki tiga variasi ukuran kunci yaitu 128 bit, 192 bit, dan 256 bit dapat dipilih secara independen. Kekuatan enkripsi AES [6] dibuktikan dalam bentuk pengukuran desimal yaitu 2^{128} kemungkinan kunci pada AES 128 bit atau sebanding dengan 3.4 x 10^{38} kombinasi kunci. Sedangkan untuk AES 192 bit memiliki 2^{192} kemungkinan kunci yang sebanding dengan 6.2 x 10^{57} kombinasi kunci, dan AES 256 bit

memiliki 2^{256} kemungkinan kunci yang sebanding dengan 1.1×10^{77} kombinasi kunci. Metode steganografi *Pixel Value Differencing* (PVD) pertama kali diusulkan pada tahun 2003 oleh Wu-Tsai. Adapun skema penyisipan pesan yang dilakukan pada metode ini [7] adalah dengan melakukan perhitungan nilai selisih antara dua piksel yang berdekatan dalam blok yang sama. Pemilihan metode ini didasarkan pada kelebihan dari *Pixel Value Differencing* yang dapat membuat peningkatan daya tampung pesan serta memiliki kemampuan untuk mengurangi distorsi pada teknik steganografi.

Pemilihan teknik kriptografi *Advanced Encryption Standard* (AES) didasarkan pada masalah kerentanan pada teknik kriptografi *Data Encryption Standard* (DES) yang mudah dipecahkan dengan serangan *brute force* [8]. Untuk menambah keamanan pesan yang dikirim, maka algoritma kriptografi *Advanced Encryption Standard* 128 bit ini dikombinasikan dengan algoritma *Vigenere Cipher*. Sedangkan teknik steganografi *Pixel Value Differencing* (PVD) dipilih karena algoritma steganografi sebelumnya seperti *Least Significat Bit* (LSB) sudah berhasil dilakukan proses steganalisis menggunakan teknik *Chi Square* yang dapat mendeteksi pesan yang disisipkan pada image secara sequensial [9] dan untuk teknik *Most Significant Bit* (MSB) memiliki tingkat distorsi yang tinggi karena pesan disisipkan pada bit paling awal yang berpengaruh, sehingga mudah untuk dideteksi. Berdasarkan pemaparan tersebut, maka pada penelitian ini dibuat sebuah sistem *Stego-Kripto* untuk mengamankan pesan menggunakan *hybrid* kriptosistem *Vigerene Cipher* dan *Advanced Encryption Standard* 128 bit (AES) yang dipadukan dengan teknik steganografi *Pixel Value Differencing* (PVD). Setelah pesan berhasil diamankan menggunakan mekanisme tersebut, maka dilakukan pengujian yang terdiri dari pengujian validitas, performansi, serta pengujian MSE dan PSNR yang berfungsi untuk mengukur dan mengetahui pengaruh *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 (AES) yang dipadukan dengan *Pixel Value Differencing* dalam pengamanan pesan.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dipaparkan, diperoleh rumusan permasalahan yaitu: "Bagaimana pengaruh penerapan *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) yang dipadukan dengan *Pixel Value Differencing* (PVD) dalam pengamanan pesan"?

1.3 Batasan Masalah

Adapun batasan masalah dalam penelitian ini meliputi :

a. Teknik steganografi yang digunakan yaitu *Pixel Value Differencing* (PVD).
b. Enkripsi yang diterapkan yaitu *hybrid* kriptosistem menggunakan *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES).
c. Media *cover* yang digunakan untuk menyisipkan pesan adalah file *image grayscale* dengan format 8 bit *depth* yang berekstensi .PNG.
d. Kunci yang digunakan untuk enkripsi AES 128 bit memiliki ukuran 16 karakter.
e. Bahasa pemrograman yang digunakan untuk pembuatan *project* yaitu *Python3* dan *library* yang diterapkan meliputi *Pillow* (untuk memanipulasi file gambar), dan *Math* (untuk menghitung fungsi matematika).
f. Penelitian ini membahas mengenai konsep matematis dan penerapannya pada *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) serta mengenai konsep penyisipan pesan pada media *image* (citra) menggunakan teknik *Pixel Value Differencing* (PVD).

1.4 Tujuan Penelitian

Penelitian ini memiliki tujuan untuk mengetahui pengaruh penerapan *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) yang dipadukan dengan *Pixel Value Differencing* (PVD) dalam pengamanan pesan.

1.5 Manfaat Penelitian

Manfaat yang diharapkan dari adanya penelitian ini adalah :

1. Manfaat teoritis

   Hasil penelitian ini diharapkan dapat memberikan kontribusi dan manfaat bagi pengetahuan (*contribution to knowledge*) dalam terciptanya mekanisme keamanan data yang diperoleh dari adanya kombinasi antara metode steganografi *Pixel Value Differencing* (PVD) dengan *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Standard* 128 bit (AES).

2. Manfaat praktis

   Luaran penelitian ini diharapkan mampu memberikan manfaat bagi semua pihak, khususnya pengguna internet dan media digital dalam mengamankan data dan file penting lainnya dengan metode *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES) serta dapat menyisipkan hasil enkripsi tersebut pada media *image* (citra) menggunakan teknik *Pixel Value Differencing* (PVD).

1.6 Sistematika Penulisan

Dalam mewujudkan tujuan penelitian ini, maka sistematika penulisan yang disajikan dalam skripsi ini meliputi :

BAB I Pendahuluan

Pada bab ini membahas mengenai latar belakang permasalahan yang diselesaikan dalam skripsi. Untuk memudahkan penyelesaian masalah, maka penulis membuat rumusan masalah yang dibahas dalam skripsi disertai dengan adanya batasan penelitian beserta tujuan dan manfaat yang ingin dicapai dari penelitian. Selain itu, penulis juga menyajikan sistematika penulisan skripsi yang menjadi tahapan dalam tercapainya tujuan penelitian.

BAB II Landasan Teori

Pada bab ini membahas mengenai kajian pustaka yang berasal dari penelitian terkait yang telah dilakukan sebelumnya serta teori-teori pendukung yang berkaitan dengan *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced*

Encryption Standard 128 bit (AES) yang dipadukan dengan steganografi *Pixel Value Differencing* (PVD).

BAB III Metodologi Penelitian

Pada bab ini memuat metode penelitian yang diterapkan dalam menyelesaikan masalah penelitian yang terdiri dari jenis penelitian, identifikasi variabel penelitian, metode pengumpulan data, metode ekperimental, pengujian dan analisis.

BAB IV Pembahasan

Bab ini membahas mengenai alur perhitungan pada *hybrid* kriptosistem *Vigenere Cipher* dan *Advanced Encryption Standard* 128 bit (AES), validasi terhadap hasil enkripsi file menggunakan *hybrid* kriptosistem, mekanisme penyisipan pesan ke dalam media citra (*image*) menggunakan teknik steganografi *Pixel Value Differencing* (PVD), dan melakukan analisis terhadap kualitas citra hasil dari proses steganografi.

BAB V Penutup

Pada bagian penutup berisi kesimpulan dari penelitian yang telah dilakukan dan saran untuk penelitian kedepannya yang bersifat membangun.