BAB I
PENDAHULUAN

1.1 Latar Belakang

Di era informasi ini, komunikasi memainkan peran yang sangat penting dalam membantu pengembangan teknologi baru. Dalam buku yang ditulis oleh Pinaki Mitra (2018) yang berjudul "Introductory Chapter: Recent Advances In Cryptography and Network Security" disebutkan bahwa, dalam pengembangan teknologi yang pesat ini, bentuk dari perangkat komputer yaitu *processors* dan penyimpanan (*hard disk)* semakin kecil, namun dengan munculnya teknologi baru tersebut tentu kemampuan menghitung dan kapasitas penyimpanan meningkat. Hal ini memungkinkan informasi yang dikomunikasikan jauh lebih mudah, lebih cepat, dan lebih praktis baik dalam jaringan kabel maupun nirkabel. Seiring dengan perkembangan teknologi tersebut, timbul suatu masalah yaitu keamanan dan kerahasiaan dari pertukaran informasi.

Keamanan adalah hal yang penting untuk dipertimbangkan, terlebih jika informasi tersebut sangat rahasia. Oleh karena itu, sebuah mekanisme diperlukan untuk mengamankan informasi yang dikirim (Mitra, 2018). Proses dari mengubah informasi asli menjadi bentuk tersamar sebagai enkripsi. Proses mengkonversi informasi yang tersamar menjadi informasi asli dikenal sebagai dekripsi. Ilmu dari enkripsi dan dekripsi dikenal sebagai kriptografi. Kriptografi ini dapat menjamin bahwa informasi yang dikirimkan hanya diketahui oleh pengirim dan penerima saja. Kriptografi itu sendiri dapat mengenkripsi dan mendekripsi file berbentuk pesan teks, gambar, video dan juga audio.

Mansi dan Chawla (2015) mengemukakan bahwa "Selama bertahun-tahun beberapa teknik enkripsi telah diterapkan, tetapi sebagian besar teknik hanya mengenkripsi data teks, sangat sedikit teknik yang diusulkan untuk data multimedia seperti data audio". Data audio merupakan suatu kumpulan data yang memiliki nilai tertentu. Mengenkripsi data audio berarti mengamankan nilai-nilai di dalamnya sehingga membuat data audio terenkripsi menghasilkan suara yang tidak dapat

dimengerti oleh pihak ketiga. Hal ini memungkinkan pengirim mengirimkan data audio pada jaringan apapun dengan aman tanpa seseorang mengetahui data audio asli kecuali penerima yang telah mengetahui kunci yang telah disepakati oleh keduanya.

Salah satu cara untuk mengamankan data audio yaitu dengan melakukan transposisi. Transposisi bertujuan untuk mengacak data audio pada file audio sehingga suara yang dihasilkan tersamarkan. Salah satu cara transposisi yaitu menggunakan pembangkit bilangan acak semu, sehingga posisi dari data audio benar-benar teracak. Algoritma *Blum Blum Shub* merupakan pembangkit bilangan acak semu yang cukup mudah untuk dibangkitkan melalui persamaannya namun bilangan acak yang dihasilkan tidak mudah untuk diprediksi (Stinson, 2006). Tetapi dalam penelitian yang telah dilakukan Sinha dkk. (dalam Stallings, 2015) mengemukakan bahwa "*In this paper, the audio is encrypted only using transposition. To enchance the resistance of the audio file, the audio file can be further subjected to substitution encryption*". Dijelaskan bahwa pada penelitiannya, audio yang dienkripsi hanya menggunakan transposisi dan untuk meningkatkan ketahanan dari file audio, file audio dapat dilanjutkan dengan menggunakan enkripsi substitusi. Teknik enkripsi substitusi dari kriptografi klasik *Affine Cipher* dapat diterapkan dalam kriptografi audio untuk meningkatkan keamanan file audio di mana data audio tersebut dienkripsi dengan suatu persamaan sehingga akan memberikan *noise* atau gangguan pada file audio. Kriptografi klasik memiliki tingkat keamanan yang kurang baik jika dibandingkan dengan kriptografi modern karena algoritma kriptografi modern terbilang relatif kompleks dibandingkan kriptografi klasik. Oleh karena itu diperlukan suatu pengembangan pada algoritma *Affine Cipher* ini, salah satunya yaitu menggunakan barisan bilangan acak. Barisan bilangan acak memungkinkan suatu nilai yang sama akan menghasilkan nilai yang berbeda setelah melalui proses enkripsi. Algoritma pembangkit barisan bilangan acak yang digunakan adalah Algoritma *Blum Blum Shub.* "Proses penyandian yang diusulkan tersebut dapat menyelesaikan cacat penyandian substitusi dengan memastikan bahwa nilai yang dihasilkan berbeda, dan tidak ada pola yang dapat dikenali dari karakter yang identik saat dienkripsi" (Arroyo dan Delima, 2020).

Berdasarkan pemaparan sebelumnya, penulis tertarik untuk menggunakan kriptografi transposisi menggunakan algoritma pembangkit bilangan acak semu *Blum Blum Shub* lalu dilanjutkan dengan *Affine Cipher* yang dikembangkan dengan algoritma pembangkit bilangan acak semu *Blum Blum Shub* pada file audio. Dengan algoritma tersebut diharapkan penulis dapat mengenkripsi dan mendekripsi data audio dengan baik sehingga dapat menjamin keamanan dan kerahasiaan data audio serta suara yang dihasilkan file audio tersamarkan. Oleh karena itu, penulis mengambil judul **"Kriptografi Audio Menggunakan Transposisi dan *Affine Cipher* yang Dikembangkan dengan Algoritma *Blum Blum Shub*".**

1.2 Rumusan Masalah

Berdasarkan pemaparan latar belakang sebelumnya, permasalahan dapat dirumuskan sebagai berikut:

1. Bagaimana algoritma kriptografi file audio dengan transposisi menggunakan pembangkit bilangan acak semu *Blum Blum Shub* ?
2. Bagaimana algoritma modifikasi *Affine Cipher* dengan algoritma *Blum Blum Shub* pada file audio?
3. Bagaimana peningkatan keamanan dari *Affine Cipher* asli menjadi modifikasi *Affine Cipher* dengan algoritma *Blum Blum Shub* pada file audio?
4. Bagaimana konstruksi program aplikasi kriptografi audio dengan transposisi dan modifikasi *Affine Cipher* menggunakan *Python* ?

1.3 Batasan Masalah

Batasan masalah yang digunakan dalam penelitian ini adalah:

1. File audio yang digunakan adalah file audio 8 *bit* atau 16 *bit*
2. Format file audio yang digunakan adalah format *.wav atau *.wave

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, tujuan dari penulisan penelitian ini adalah:

1. Mengimplementasikan enkripsi file audio dengan transposisi menggunakan pembangkit bilangan acak semu *Blum Blum Shub*

2. Merancang algoritma *Affine Cipher* yang dikembangkan dengan algoritma *Blum Blum Shub* pada file audio
3. Menganalisis peningkatan keamanan dari *Affine Cipher* asli menjadi *Affine Cipher* yang dikembangkan dengan algoritma *Blum Blum Shub*
4. Mengkonstruksi algoritma *Affine Cipher* dan modifikasi *Affine Cipher* pada file audio dengan menggunakan *Python*

1.5 Manfaat Penelitian

Adapun manfaat dari penulisan penelitian ini adalah:

1. Manfaat teoritis

Secara teoritis, penilitian ini diharapkan dapat berkontribusi dalam:

a. Memberikan alternatif pengenkripsian file audio dengan transposisi menggunakan pembangkit bilangan acak semu*Blum Blum Shub*
b. Memberikan rancangan mengenai algoritma *Affine Cipher* yang dikembangkan dengan algoritma *Blum Blum Shub* pada file audio
c. Memberikan peningkatan keamanan dari algoritma *Affine Cipher* asli menjadi *Affine Cipher* yang dikembangkan dengan algoritma *Blum Blum Shub*

2. Manfaat praktis

Secara praktis, penelitian ini menghasilkan suatu *prototype* program aplikasi *Python* mengenai algoritma *Affine Cipher* yang dikembangkan menggunakan algoritma *Blum Blum Shub* pada file audio yang diharapkan dapat digunakan oleh *end user*.

1.6 Sistematika Penulisan

Dalam penulisan penelitian ini dibentuklah struktur sebagai berikut:

BAB I PENDAHULUAN menjelaskan latar belakang penelitian, rumusan masalah, beberapa batasan masalah, serta tujuan dan manfaat penelitian.

BAB II KAJIAN TEORI mengandung teori-teori yang telah dikaji dalam penelitian lain yang akan digunakan untuk menyelesaikan rumusan masalah yang telah dibuat sebelumnya.

BAB III METODE PENILITIAN membahas dan mengkaji langkah-langkah yang digunakan dalam menyelesaikan penelitian.

BAB IV HASIL DAN PEMBAHASAN membahas hasil penelitian yang telah dilakukan

BAB V KESIMPULAN DAN SARAN memberikan simpulan hasil penelitian dan menawarkan saran untuk penelitian selanjutnya.