BAB 1
PENDAHULUAN

1.1. Latar Belakang

Pandemi COVID-19 adalah pandemi dari virus *corona* yang pertama kali diidentifikasi pada Desember 2019 di Wuhan, Cina (WHO, 2020). Dan Indonesia pertama kali mengkonfirmasi kasus COVID-19 pada 2 Maret 2020 dengan Bapak Presiden Joko Widodo mengumumkan ada dua orang Indonesia positif terjangkit virus *corona* (detikcom, 2020). Munculnya virus *corona* mengakibatkan aktivitas sehari-hari terganggu, salah satunya adalah berkomunikasi dengan cara bertatap muka, seperti kegiatan perkantoran, kegiatan belajar mengajar, ataupun pertemuan luring dilakukan secara daring atau *online* (Humas, 2021).

Dalam upaya meningkatkan keamanan informasi dalam bertukar informasi dengan menggunakan aplikasi yang menggunakan jaringan internet, kriptografi bisa menjadi salah satu solusi dalam merahasiakan suatu informasi. Kunci merupakan salah satu komponen dari kriptografi yang digunakan pada proses mengunci dan membuka informasi yang disembunyikan. Bilangan acak bisa digunakan sebagai kunci kriptografi dikarenakan sulit diperkirakan. Bilangan acak dapat dihasilkan menggunakan *Random Number Generator*.

Random Number Generator terdiri dari dua jenis, yaitu *True Random Number Generator* (TRNG) dan *Pseudorandom Number Generator* (PRNG). *True Random Number Generator* menghasilkan bilangan acak yang berasal dari sebuah sumber yang tidak dapat ditentukan yang dinamakan sebagai sumber entropi. Sedangkan *Pseudorandom Number Generator* menghasilkan bilangan yang terlihat acak, namun sebenarnya bisa ditentukan, karena bilangan acak yang dihasilkan *Pseudorandom Number Generator* ditentukan oleh sebuah *seed* atau nilai awal. Walau bilangan acak yang dihasilkan *True Random Number Generator* lebih dekat ke bilangan acak yang sesungguhnya, *Pseudorandom Number Generator* tetap penting dalam hal menghasilkan bilangan acak dengan cepat (Jayaraj, Gujarathi, Venkatesh, & Sanyal, 2019).

Dalam tugas akhir ini diimplementasikan *Self-Generated True Random Number Generator* yaitu *True Random Number Generator* yang menghasilkan bilangan acak

dengan menggunakan sebagian bit audio dengan format MP3 yang di enkripsi sebagai entropi (Etem & Kaya, 2020). Lalu membandingkan kinerjanya dengan *Pseudorandom Number Generator Blum Blum Shub*.

1.2. Perumusan Masalah

- Bagaimana hasil dari perbandingan kinerja kedua *Random Number Generator* tersebut.
- Apakah algoritma *Self-Generated True Random Number Generator* layak digunakan sebagai penghasil bilangan acak yang dapat digunakan sebagai kunci dalam kriptografi.

1.3. Tujuan Penelitian

Membandingkan kinerja *self-Generated True Random Number Generator* dengan *Pseudorandom Number Generator* dalam menghasilkan kunci kriptografi yang berupa bilangan acak.

1.4. Batasan Masalah

Agar pembahasan hanya terfokus pada sistem kriptografi dengan bilangan acak sebagai kunci, maka aplikasi dibuat dengan batasan masalah sebagai berikut:

- Berkas audio digital yang digunakan dengan format MP3 (.mp3).
- *Integrated Development Environment* (IDE) yang digunakan adalah Apache Netbeans 12.0.
- Bahasa pemrograman yang digunakan adalah Java dengan Java Development Kit (JDK) AdoptOpenJDK 13.0.2.8.
- *Self-Generrated True Random Number* Generator digunakan dalam menghasilkan bilangan acak dengan metode *True Random Number Generator*.
- *Blum Blum Shub* digunakan dalam menghasilkan bilangan acak dengan metode *Pseudorandom Number Generator*.
- Parameter perbandingan:
    - *Time Complexity* dari algoritma *Self-Generated True Random Number Generator* dan algoritma *Blum Blum Shub*.
    - Hasil pengujian bilangan acak dengan menggunakan pengujian *Frequency (Monobit)*.

1.5. *State of The Art*

Penyusunan tugas akhir ini mengambil beberapa referensi penelitian sebelumnya termasuk jurnal-jurnal yang berhubungan dengan penelitian ini.

Jurnal	Pembahasan
High-uncertainty audio signal encryption based on the Collatz conjecture (Renza, Mendoza, & Ballesteros L, 2019)	*State of the art* teknik enkripsi audio berfokus memberikan sinyal terenkripsi dengan korelasi linear yang sangat rendah dengan sinyal audio asli. Namun ukuran kunci bergantung pada panjangnya kunci. Ini adalah kelemahan karena tidak memungkinkan untuk pengguna menghafal kunci yang sangat panjang. Maka diajukan teknik enkripsi audio yang menggunakan *variable-length seed* untuk memilih urutan dari kode Collatz, yang menghasilkan sinyal terenkripsi berbeda. Dengan cara ini, ukuran kunci lebih besar tidak bergantung terhadap panjang kunci. Hasil penelitian tersebut menjelaskan teknik enkripsi audio yang memberikan tingkat keamanan tinggi menggunakan *variable-length* berdasarkan *Collatz conjecture*. Semakin besar ukuran kunci, semakin tinggi tingkat keamanan sistem. Namun sinyal terenkripsi memiliki bit yang lebih banyak dari sinyal asli. Maka pada tugas akhir ini diimplementasikan aplikasi kriptografi dengan data

	terenkripsi yang ukurannya sama dengan data asli.
Implementation of El-Gamal algorithm for speech signals encryption and decryption (Imran, Yousif, Hameed, Abed, & Hammid, 2020)	Algoritma El-Gamal digunakan untuk enkripsi dan dekripsi sinyal pidato. Pertama, sinyal pidato dienkripsi menggunakan algoritma El-Gamal dan dikirim kepada penerima. Kedua, penerima mengembalikan sinyal asli dengan proses dekripsi. Performa *cryptosystem* dievaluasi dengan ukuran kualitas sinyal audio termasuk *Signal to Noise Ratio, Segmented Signal to Noise Ratio* dan *Log-Likelihood Ratio*. Hasil penelitian tersebut menjelaskan beberapa cara untuk mengevaluasi kualitas sinyal audio.
PRNG *Implementation Based in Chaotic Neural Network* (Mohammed, 2019)	Penghasil bilangan acak ini menggunakan sensitivitas tinggi dan properti acak dari *chaotic functions*. 4 tingkat *Neural Network* meningkatkan kompleksitas *nonlinear* penghasil bilangan acak. Penghasil nomor acak lulus pengujian acak dengan menggunakan NIST tests. Hasil penelitian tersebut menjelaskan beberapa pengujian untuk penghasil nomor acak yang menggunakan NIST test yang digunakan pada tugas akhir ini.

XOR-*based progressive visual secret sharing using generalized random grids* (Chao & Fan, 2017)	Penelitian ini mengajukan skema GRGPVSS berdasarkan XOR dimana gambar rahasia dibagi menjadi beberapa bagian, setiap bagian memiliki ukuran yang sama dengan gambar rahasia. Setiap bagian terlihat mirip dengan gambar *noise* dan tidak menampilkan informasi apa pun mengenai gambar rahasia. Hasil penelitian tersebut menjelaskan bagaimana penggunaan operasi XOR dalam pembagian dan penyatuan kembali gambar rahasia. Operasi XOR digunakan pada tugas akhir ini dalam proses enkripsi dan dekripsi.
A cryptographic model for better information security (Kumar, Kumar, Budhiraja, Das, & Singh, 2018)	Model kriptografi untuk enkripsi gambar menggunakan *Coupled Map Lattice*. Model dianalisa dengan gambar berbeda dan banyak kunci rahasia yang dihasilkan secara acak. Evaluasi keamanan dan performa dijalankan menggunakan analisis histogram, analisis korelasi, analisis ukuran kunci, diferensial, *anti-noise*, serangan teks dan analisis sensitivitas kunci. Hasil penelitian tersebut menjelaskan bagaimana menggunakan kunci rahasia yang dihasilkan secara acak untuk

	meningkatkan keamanan gambar serta menganalisis kunci yang dihasilkan.

1.6. Sistematika Penulisan

- BAB 1 Pendahuluan

  Berisi latar belakang, perumusan masalah, tujuan penelitian, batasan masalah, *state of the art*, dan sistematika penulisan.

- BAB 2 Tinjauan Pustaka

  Berisi uraian teori tentang kriptografi, XOR *Cipher*, *random number generation*, *blum blum shub*, *self-generated true random number generator*, pengujian *frequency (Monobit*), berkas audio dengan format MP3.

- BAB 3 Analisis Dan Perancangan

  Berisi pembahasan mengenai cara kerja algoritma *blum blum shub* dan *self-generated true random number generator* dan perancangan aplikasi untuk implementasi dua algoritma tersebut dalam proses enkripsi dan dekripsi.

- BAB 4 Implementasi Dan Pengujian

  Berisi hasil implementasi dari apa yang sudah di rancang pada BAB 3 Analisis Dan Perancangan dan hasil perhitungan *time complexity* dari algoritma *blum blum shub* dan *self-generated true random number generator* serta pengujian terhadap kunci atau bilangan acak yang dihasilkan berdasarkan parameter yang telah ditentukan pada 1.4. Batasan Masalah.

- BAB 5 Kesimpulan dan Saran

  Berisi kesimpulan dari pengerjaan tugas akhir dan saran untuk pengembangan selanjutnya.