BAB I
PENDAHULUAN

1.1 Latar Belakang

Masalah terkait keamanan telah menjadi aspek penting pada era teknologi informasi saat ini terutama bagi perusahaan dan pemerintahan. Keamanan suatu negara tidak hanya dilihat dari kekuatan militer saja, tetapi juga dilihat dari informasi teknologi yang dikuasai negara tersebut. Setiap negara memiliki inteligen yang bertumpu pada informasi dan teknologi karena sifatnya yang rahasia. Dilansir dari penelitian "*2016 Data Threat Report*" yang dilakukan oleh *Vormetric Security Data*, terdapat 91% perusahaan dan pemerintahan yang rentan mengalami kebocoran data dan 61% pernah mengalaminya.

Untuk mengatasi masalah tersebut, diperlukan ilmu kriptografi yang memiliki peranan penting dalam keamanan data. Kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, autentikasi entitas, integritas data, dan autentikasi data asal. Ilmu kriptografi erat kaitannya dengan ilmu matematika diantaranya adalah konsep mengenai fungsi, permutasi dan kombinasi, teori peluang, teori bilangan, dan aljabar abstrak. Kriptografi banyak digunakan dalam kehidupan sehari-hari, misalnya transaksi mesin ATM, transaksi di bank, transaksi dengan kartu cerdas, percakapan melalui telepon genggam, *e-commerce* melalui internet, dan mengaktifkan peluru kendali.

Sebelum komputer ada, kriptografi dilakukan dengan menggunakan pensil dan kertas. Algoritma kriptografi yang digunakan saat itu digolongkan ke dalam algoritma klasik. Salah satu contoh algoritma klasik adalah *Hill cipher*. *Hill cipher* merupakan penerapan aritmatika modulo pada kriptografi. Teknik kriptografi ini menggunakan sebuah matriks persegi sebagai kunci yang digunakan untuk melakukan enkripsi dan dekripsi. *Hill cipher* dapat memecahkan cipherteks yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi.

Namun ada beberapa kekurangan *Hill cipher*, diantaranya adalah algoritmanya dirancang hanya dapat mengenkripsi karakter alfabet saja, cipherteks yang dihasilkan hanya dalam karakter abjad, jumlah elemen plainteks sama dengan cipherteks. *Hill cipher* telah dipecahkan dengan kriptanalisis *Known Plaintext Attack*, di mana kriptanalis memiliki pasangan plainteks dan cipherteks yang berkoresponden, menggunakan perkalian matriks dan persamaan linier. Makalah berjudul "Modifikasi *Hill cipher* Menggunakan *Convert Between Base*" yang diteliti oleh Alz Danny Wowor membahas modifikasi *Hill cipher* menggunakan *Convert Between Base* dan perkalian n-matriks kunci untuk setiap iterasi.

Perkembangan kriptografi hingga kini sudah sangat pesat. Kriptografi modern dibuat agar kriptanalis sulit memecahkan cipherteks tanpa mengetahui kunci. Algoritma kriptografi modern umumnya beroperasi dalam mode bit ketimbang mode karakter. Operasi dalam mode bit berarti semua data dan informasi dinyatakan dalam rangkaian (string) bit biner, 0 dan 1. *Stream cipher* merupakan salah satu algoritma modern. *Stream cipher* sering menggunakan *linear feedback shift register* sebagai pembangkit kunci *stream*. Ilmu matematika yang digunakan pada *linear feedback shift register* diantaranya adalah fungsi, teori bilangan, aljabar abstrak.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah diatas, peneliti mengajukan beberapa rumusan masalah sebagai berikut:

1. Bagaimana konsep algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base*?
2. Bagaimana menerapkan pembangkit kunci *linear feedback shift register* pada algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base*?
3. Bagaimana implementasi algoritma modifikasi *Hill cipher* dalam bentuk program aplikasi?
4. Apakah modifikasi *Hill cipher* dapat memperkuat keamanan algoritma kriptografi?

1.3 Tujuan Penelitian

Tujuan yang hendak dicapai dalam penelitian ini adalah:

1. Mengidentifikasi konsep algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base*.
2. Mengidentifikasi penerapan pembangkit kunci *linear feedback shift register* pada algoritma *Hill cipher* yang dimodifikasi menggunakan *convert between base***.**
3. Mengidentifikasi implementasi algoritma modifikasi *Hill cipher* dalam bentuk program aplikasi.
4. Mengidentifikasi keamanan modifikasi *Hill cipher*.

1.4 Manfaat Penelitian

Adapun manfaat dari penelitian ini adalah:

1. Mengamankan data agar tidak dibaca oleh pihak yang tidak berhak.
2. Menambah algoritma baru kriptografi khususnya *Hill cipher*.

1.5 Sistematika Penulisan

BAB I PENDAHULUAN

Bab pendahuluan berisi uraian latar belakang, rumusan masalah, tujuan penelitian, manfaat penelitian, struktur organisasi.

BAB II TINJAUAN PUSTAKA

Bab ini membahas teori-teori yang mendukung masalah yang akan dikaji. Pada bab ini akan dipaparkan teori dan konsep pada bidang matematika khususnya mengenai teori bilangan, konversi basis bilangan, matriks, dan bidang kriptografi khususnya mengenai *Hill cipher* dan *linear feedback shift register*.

BAB III METODE PENELITIAN

Menyajikan paparan secara rinci mengenai pendekatan dan metode penelitian termasuk prosedur yang digunakan pada *Hill cipher* dan *Linear Feedback Shift Register (LFSR).*

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini membahas dekripsi data hasil penelitian, serta pembahasan dari analisis data yang ditemukan.

BAB V SIMPULAN DAN SARAN

Bab penutup menyajikan penafsiran terhadap hasil analisis temuan penelitian, kesimpulan-kesimpulan yang diambil dari analisis data secara keseluruhan, serta berisi mengenai saran-saran.