DAFTAR ISI

LEMBAR PENGESAHAN ..... **i**

PERNYATAAN ..... **ii**

ABSTRAK ..... **iii**

ABSTRACT ..... **iv**

KATA PENGANTAR ..... **v**

DAFTAR ISI ..... **vii**

DAFTAR TABEL ..... **x**

DAFTAR GAMBAR ..... **xi**

BAB I PENDAHULUAN **1**

1.1 Latar Belakang 1

1.2 Rumusan Masalah 2

1.3 Tujuan Penelitian 3

1.4 Manfaat Penelitian 3

1.5 Sistematika Penulisan 3

BAB II TINJAUAN PUSTAKA **5**

2.1 Kekongruenan 5

2.2 Matriks 6

2.3 *Convert Between Base* 7

2.4 Kriptografi 8

2.4.1 Pesan, Plainteks, dan Cipherteks 8

2.4.2 Pengirim dan Penerima 8

2.4.3 Enkripsi dan Dekripsi 8

2.4.4 *Cipher* dan Kunci 9

2.4.5 Sistem Kriptografi 10

Srita Tania Bonita, 2017
PEMBANGKIT KUNCI LINEAR FEEDBACK SHIFT REGISTER PADA ALGORITMA HILL CIPHER YANG DIMODIFIKASI MENGGUNAKAN CONVERT BETWEEN BASE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

2.4.6 *Hill cipher* 11
2.4.7 *Linear Feedback Shift Register* 15
2.4.8 MATLAB 18
2.4.7 Pencocokkan Kurva 18
BAB III METODE PENELITIAN 19
3.1 Perumusan Masalah 19
3.2 Model Dasar 19
3.3 Pengembangan Model 19
3.4 Perancangan Program Aplikasi 20
3.5 Pembuatan Program Aplikasi 20
3.6 Validasi 20
3.7 Penarikan Kesimpulan 20
BAB IV PEMBAHASAN 21
4.1 Modifikasi *Hill cipher* sebagai Teknik Kriptografi 21
4.1.1 Proses Enkripsi 22
4.1.2 Proses Dekripsi 23
4.2 Modifikasi *Hill cipher* sebagai Sistem Kriptografi 23
4.3 LFSR dan CBB pada *Hill cipher* 24
4.4 Ketersediaan Kunci 25
4.5 Contoh Program Modifikasi *Hill cipher* 29
4.6 Contoh Proses Enkripsi Modifikasi *Hill cipher* 29
4.7 Proses Dekripsi Modifikasi *Hill cipher* 30
4.8 Kriptanalisis Modifikasi *Hill cipher* 31
4.9 Uji Ketahanan LFSR 34
4.10 Kebutuhan Waktu 35

Srita Tania Bonita, 2017
PEMBANGKIT KUNCI LINEAR FEEDBACK SHIFT REGISTER PADA ALGORITMA HILL CIPHER YANG DIMODIFIKASI MENGGUNAKAN CONVERT BETWEEN BASE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu

BAB V KESIMPULAN DAN SARAN **37**

5.1 Kesimpulan 37

5.2 Saran 37

DAFTAR PUSTAKA **38**

LAMPIRAN **39**

Srita Tania Bonita, 2017
PEMBANGKIT KUNCI LINEAR FEEDBACK SHIFT REGISTER PADA ALGORITMA HILL CIPHER YANG DIMODIFIKASI MENGGUNAKAN CONVERT BETWEEN BASE
Universitas Pendidikan Indonesia | repository.upi.edu | perpustakaan.upi.edu