

ABSTRAK

Kriptografi adalah ilmu yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan data, keabsahan data, integritas data dan autentikasi data. Data yang diacak biasa disebut plainteks, dan dienkripsi menggunakan kunci enkripsi sehingga menghasilkan chiperteks. Untuk mengembalikan chiperteks kembali ke bentuk semula, dilakukan proses dekripsi yang juga menggunakan kunci dekripsi. Tugas akhir ini membahas tentang salah satu algoritma kriptografi yaitu AES atau Rijndael dan bagaimana mengimplementasikan algoritma tersebut supaya dapat digunakan untuk mengamankan data berupa teks.

ABSTRACT

Cryptography is technique that studies mathematical techniques related to aspects of information security such as data confidentiality, data validity, integrity and authentication. Encrypted data called plaintext and encrypted using the encryption key so as to produce ciphertexts. To restore ciphertexts back into plaintext, do the decryption process which also uses the decryption key. This thesis discusses one of the cryptographic algorithms, AES or Rijndael and how to implement the algorithm so that it can use to secure data in the form of text.

DAFTAR ISI

ABSTRAK	i
<i>ABSTRACT</i>	ii
KATA PENGANTAR	iii
DAFTAR ISI	v
DAFTAR GAMBAR	vii
DAFTAR TABEL	ix
BAB 1 PENDAHULUAN	1
1.1 Latar Belakang Masalah	1
1.2 Rumusan Masalah	2
1.3 Tujuan	2
1.4 Pembatasan Masalah	3
1.5 Sistematika Penulisan	3
BAB 2 LANDASAN TEORI	5
2.1 Teori Dasar Kriptografi	5
2.2 Algoritma Kriptografi	6
2.2.1 Algoritma Kunci Simetri	7
2.2.2 Algoritma Kunci Asimetri	8
2.3 Teknik Dasar Kriptografi	10
2.3.1 Metode Substitusi	10
2.3.2 Teknik Blok	10
2.3.3 Teknik Permutasi Atau Transposisi	11
2.4 Serangan Terhadap Kriptografi	11
2.4.1 Berdasarkan Keterlibatan Penyerang Dalam Komunikasi	11
2.4.2 Berdasarkan Banyaknya Informasi Yang Diketahui oleh Kriptanalisis	12
2.4.3 Berdasarkan Teknik yang Digunakan Untuk Menemukan Kunci	13
2.5 Algoritma <i>AES / Rijndael</i>	14
2.5.1 Transformasi <i>Subbytes</i>	17

2.5.2 Transformasi <i>Shiftrows</i>	19
2.5.3 Transformasi <i>MixColumns</i>	20
2.5.4 Transformasi <i>Addroundkey</i>	22
 BAB 3 PERANCANGAN	 23
 BAB 4 PENGAMATAN DATA	 27
4.1 Percobaan	27
4.1.1 Percobaan 1	27
4.1.2 Percobaan 2	29
4.1.3 Percobaan 3	30
4.1.4 Percobaan 4	33
4.1.5 Percobaan 5	37
 BAB 5 KESIMPULAN DAN SARAN	 41
5.1 Kesimpulan	41
5.2 Saran	41
 DAFTAR PUSTAKA	 42
Lampiran A - <i>AES Cryptographer</i>	A-1

DAFTAR GAMBAR

Gambar 2.1 : Proses Enkripsi	7
Gambar 2.2 : Proses Dekripsi	7
Gambar 2.3 : Contoh Tabel Substitusi	10
Gambar 2.4 : Teknik Blok	10
Gambar 2.5 : Blok Diagram Enkripsi dan Dekripsi Menggunakan Algoritma AES	16
Gambar 2.6 : Proses Substitusi dengan <i>S-Box</i>	18
Gambar 2.7 : Contoh Substitusi Menggunakan <i>S-Box</i>	19
Gambar 2.8 : Hasil Substitusi dengan <i>S-Box</i>	19
Gambar 2.9 : Proses Transformasi <i>Shiftrows</i>	20
Gambar 2.10 : Hasil Transformasi <i>Shiftrows</i>	20
Gambar 2.11 : Transformasi <i>Mixcolumns</i>	21
Gambar 2.12 : Hasil Setelah Transformasi <i>Mixcolumns</i>	21
Gambar 2.13 : Transformasi <i>Addroundkey</i>	22
Gambar 3.1 : <i>Flowchart</i> program <i>AES Cryptographer</i>	23
Gambar 3.2 : <i>Flowchart</i> Proses Enkripsi	24
Gambar 3.3 : <i>Flowchart</i> Proses Dekripsi	24
Gambar 4.1 : Hasil Enkripsi Percobaan 1a	27
Gambar 4.2 : Hasil Enkripsi Percobaan 2a	29

Gambar 4.3 : Hasil Dekripsi Percobaan 3a	31
Gambar 4.4 : Hasil Percobaan 4a	34
Gambar 4.5 : Hasil Percobaan 5a	37

DAFTAR TABEL

Tabel 4.1 : Tabel Hasil Percobaan 1	28
Tabel 4.2 : Tabel Hasil Percobaan 2	30
Tabel 4.3 : Tabel Perbandingan Percobaan 3 dengan Percobaan 4	36
Tabel 4.4 : Tabel Perbandingan Percobaan 3 dan Percobaan 5	40