BAB III
METODE PENELITIAN

3.1 Waktu dan Tempat Penelitian

Penelitian ini dilakukan di Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Lampung. Waktu penelitian dilakukan selama semester ganjil dan semester genap tahun ajaran 2011-2012

3.2 Tahapan Penelitian

Dalam penelitian ini dilakukan tahapan penelitian yaitu, menentukan rumusan masalah dan batasan masalah, *study literature*, pengkodean aplikasi yang dibangun, dan pengujian aplikasi.

3.3 Algoritma Penelitian

Pada penelitian ini digunakan dua metode kriptografi, yaitu Algoritma Kriptografi RC4 dan Rijndael.

3.3.1 Algoritma Kriptografi RC4

Tahapan proses Algoritma RC4:

1. Melakukan inisialisasi larik S: S[0] = 0, …, S[255] = 255.
2. Melakukan *padding* kunci jika kunci kurang dari 256 karakter.
3. Melakukan permutasi setiap nilai-nilai dalam larik S.
4. Membangkitkan aliran kunci (*keystream*) dan lakukan enkripsi dengan operasi XOR antara aliran kunci dan plainteks untuk menghasilkan cipherteks.
5. Proses dekripsi dilakukan dengan menggunakan kunci aliran yang sama dengan yang digunakan saat proses enkripsi. (Safrina, 2006)

3.3.2 Algoritma Kriptografi Rijndael

Tahapan proses Algoritma Rijndael:

1. Siapkan *array* berukuran 4x4 bernama Kunci
2. Siapkan *array* berukuran 4x4 bernama *State.*
3. Cetak : “Masukkan 16 bilangan heksadesimal sebagai kunci : “
4. Simpan enam belas nilai tersebut sebagai nilai dari masing-masing elemen *array* Kunci.
5. Cetak : “Masukkan teks yang akan dienkripsi : “
6. Konversikan teks tersebut ke dalam bentuk *bit* menggunakan kode ASCII.
7. Konversikan kode ASCII tersebut ke dalam heksadesimal.
8. Kelompokkan *bit-bit* teks tersebut menjadi 128 *bit* tiap bagiannya.
9. Ambil 128 *bit* pertama untuk diproses.
10. Kelompokkan *bit* teks tersebut menjadi 16 bagian dengan 8 *bit* tiap bagiannya.

11. Masukkan tiap-tiap bagian teks tersebut ke dalam tiap-tiap sel pada matriks berukuran 4x4.
12. Konversikan *bit* ke dalam heksadesimal.
13. Lakukan langkah *AddRoundKey*.
14. Lakukan langkah *SubBytes*.
15. Lakukan langkah *ShiftRows*.
16. Lakukan langkah *MixColumns.*
17. Lakukan langkah *AddRoundKey*
18. Ulangi langkah 13-16 sebanyak 9 kali.
19. Jika langkah 17 sudah dilakukan, maka lakukan langkah *SubByte.*
20. Lakukan langkah *ShiftRows*.
21. Lakukan langkah *AddRoundKey*.
22. Selesai.