BAB III

KERANGKA KONSEP PENELITIAN DAN METODOLOGI PENELITIAN

## Kerangka Konsep Penelitian

Gambar 3.1 Diagram Alir Kerangka Konsep Penelitian

### Kriptografi

Didalam kriptografi terdapat dua jenis kunci yaitu:

1. Kunci Simetris
2. Kunci Asimetris

Algoritma asimetris dapat dikelompokkan menjadi dua kategori yaitu :

1. Block Cipher

*Block cipher* merupakan suatu algoritma yang mana proses input dan outputnya berupa 1 blok, dan setiap blok terdiri dari beberapa bit (1 blok terdiri dari 64 bit atau 128 bit).

1. Stream Cipher

*Stream cipher* merupakan suatu algoritma yang mana setiap bit *plaintext* dengan bit kunci adalah kunci utama (kunci induk) yang digunakan untuk membangkitkan kunci acak semu. Pada kerangka konsep penilitian RSA menggunakan algoritma *block cipher*.



### Algoritma Rivest-Shamir-Adleman (RSA)

Algoritma RSA adalah algoritma kunci publik yang populer, Algoritma RSA diciptakan oleh tiga orang ilmuwan dari MIT (*Massachusset Institute of Technology*) pada tahun 1976, ilmuwan tersebut adalah Ron Rivest, Adi Shamir, dan Leonard Adleman, nama RSA sendiri diambil dari gabungan nama ketiga penemunya yaitu, (R)ivest (S)hamir (A)dleman. Algoritma ini dinilai aman karena melibatkan proses pemfaktoran bilangan prima yang besar.

Algoritma RSA merupakan salah satu algoritma kunci publik yang sampai saat ini paling banyak dikenal. Salah satu sifat dari sistem kripto dengan kunci publik adalah : D(E(m)) = E(D(m)) dengan E adalah proses enkripsi, D adalah proses dekripsi dan m adalah pesan/data. Sifat ini yang nantinya sebagai dasar untuk merancang sistem pengamanan pesan/data yang mampu menjamin keaslian dan kerahasiaan data.

Algoritma RSA merupakan algorithm *block cipher* (algoritma yang bekerja per blok data), dimana plaintext dan *ciphertext*-nya adalah bilangan bulat (*integer*) antara 0 dan n-1 untuk sebuah n tertentu. Algoritma ini bekerja dengan menghitung eksponen dari pesan (atau *plaintext*) dalam operasi *modulo* n (*modulo* = sisa pembagian). Jadi, sebelum sebuah *plaintext* dikirimkan, *plaintext* tersebut harus dipangkatkan dengan sebuah bilangan, yang biasa disebut sebagai e yang adalah kunci publik. Kemudian di sisi penerima, pesan tersandi (atau *ciphertext*) tersebut harus dipangkatkan dengan kunci miliknya sendiri, yang biasa dikenal d sebagai kunci privat, untuk memperoleh kembali pesan yang dikirimkan. Semua perhitungan dikerjakan pada operasi *modulo* n.

Pada kerangka konsep penelitian proses yang dilakukan menggunakan metode Rivest-Shamir-Adleman (RSA) adalah proses enkripsi dan dekripsi. Enkripsi merupakan proses penyandian *plaintext* menjadi *ciphertext*. Plaintext disebut dengan pesan asli, sedangkan *ciphertext* adalah pesan ter-enkrip (tersandi) yang merupakan hasil enkripsi. Sedangkan dekripsi adalah kebalikan dari enkripsi yakni mengubah *ciphertext* menjadi *plaintext*, sehingga kembali menjadi data awal/asli. Proses enkripsi metode Rivest-Shamir-Adleman (RSA) dapat dilakukan dengan cara mengikuti alur seperti yang di tunjukkan pada (Gambar 2.2). Sedangkan proses dekripsi dapat mengikuti alur seperti yang di tunjukkan pada (Gambar 2.4).

### File Teks

Pada penelitian ini akan digunakan *file* teks. *File* teks merupakan *file* yang berisi informasi-informasi dalam bentuk teks. Data yang berasal dari dokumen pengolah kata, angka yang digunakan dalam perhitungan, nama dan alamat dalam basis data merupakan contoh masukan data teks yang terdiri dari karakter, angka dan tanda baca. Masukan dan keluaran data teks direpresentasikan sebagai set karakter atau sistem kode yang dikenal oleh sistem komputer. Karakter yang umum digunakan untuk masukan dan keluaran pada komputer, salah satunya yaitu *ASCII*.

## Metode Penelitian



Gambar 3.2 Diagram Alir Metode Penelitian

### Riset Awal

Sebelum melakukan penelitian terlebih dahulu mempelajari segala hal yang terkait dengan topik penelitian. Bagian utama yang perlu dipelajari dan didalami adalah :

1. Konsep Kriptografi
2. Konsep Dasar File Teks
3. Algoritma Rivest-Shamir-Adleman

Setelah melakukan riset awal, kemudian dilakukan tahapan-tahapan seperti pada Gambar 3.2.

### Perancangan

Berdasarkan bahan dan materi riset awal yang sudah di kumpulkan, kemudian dilakukan perancangan implementasi algoritma RSA yang diperlukan untuk melakukan enkripsi dan dekripsi.

##### Proses Enkripsi

Pada tahap ini data yang berupa teks dienkripsi atau disandikan ke sebuah *file* teks yang tidak dapat dimengerti maknanya (*ciphertext*). Alur dari proses enkripsi sebagai berikut:

1. Input data teks pada *file*.
2. Teks yang ada di bagi menjadi beberapa blok kemudian diubah ke dalam bentuk bilangan *ASCII*.
3. Teks yang sudah menjadi bilangan *ASCII* akan diproses dengan perhitungan kunci publik dengan simbol e dan n.
4. Kemudian proses dari perhitungan e sebagai kunci publik dihitung dengan n sebagai nilai hasil pembagian atau *mod*/*modulo* seperti pada (pers. 2.1).
5. *Output*-nya adalah sebuah pesan acak yang tidak bisa di baca (*ciphertext*).
6. Proses Dekripsi

Pada tahap ini data teks yang ter-enkripsi dikembalikan ke bentuk data awal yang dapat dimengerti maknanya (*plaintext*). Alur dari proses dekripsi sebagai berikut :

Input data teks hasil enkripsi.

Teks yang sudah ter-enkripsi di bagi menjadi beberapa blok kemudian di ubah kedalam bentuk bilangan *ASCII*.

Teks yang sudah menjadi bilangan *ASCII* akan di proses dengan perhitungan kunci privat dengan simbol d dan n.

Kemudian proses dari perhitungan d sebagai kunci privat di hitung dengan n sebagai nilai hasil pembagian atau *mod*/*modulo* seperti pada (pers 2.2).

Output-nya adalah pesan yang bisa dibaca (*plaintext*).

### Pengujian

Melakukan enkripsi dan dekripsi pada file teks sesuai dengan kriteria data input yang sudah dispesifikasikan pada bab satu.

### Analisa Hasil

Hasil yang diperoleh dari pengujian kemudian dianalisa terutama pada hasil

enkripsi dan dekripsi file teks.

## Variabel Penelitian

Sebagai variabel penelitian dalam tugas akhir ini yang akan dikaji secara mendalam adalah metode RSA yang digunakan untuk pengamanan data teks dan menjaga kerahasiaan data.

## Data dan Tempat Penelitian

Data-data yang diperlukan :

1. Referensi-referensi dari penilitian Tugas Akhir sebelumnya
2. Tempat Penelitian : Politeknik Negeri Samarinda