BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembangan teknologi dan informasi, manipulasi terhadap gambar, teks, atau berkas-berkas termasuk dokumen atau sertifikat hasil tes, sangat mudah dilakukan. Sehingga dapat memberikan celah untuk melaksanakan praktik pemalsuan dokumen sertifikat. Pemalsuan dokumen umumnya dilakukan dengan cara memanipulasi isi dari dokumen setelah melalui proses *scan* atau membuat dokumen baru dengan desain dan tampilan yang serupa dengan aslinya.

Alternatif yang dapat digunakan untuk menjaga kerahasiaan informasi tersebut adalah dengan menyamarkannya menjadi bentuk tersandi yang bermakna. Hal tersebut dapat dilakukan dalam kriptografi dan diimplementasikan dalam bentuk *QR-Code* (*Quick Response Code*) merupakan teknik yang mengubah data tertulis menjadi kode-kode 2-dimensi yang tercetak kedalam suatu media yang lebih ringkas (Rahmawati, 2011). Praktik pemalsuan masih dapat dilakukan terhadap isi informasi pada *QR-Code*. Untuk itu perlu adanya proses enkripsi pada informasi yang akan diubah ke bentuk *QR-Code*.

Tujuan enkripsi informasi yang diimplementasikan dalam bentuk *QR-Code* agar informasi tersebut tidak dapat diidentifikasi secara langsung format dan isinya oleh orang lain. Untuk mengatasi masalah keamanan informasi pada *QR-Code* maka penulis menggunakan metode kriptografi.

Kriptografi *Exclusive OR* merupakan algoritma kriptografi klasik, algoritma *Exclusive OR* adalah algoritma enkripsi sederhana dengan menggunakan prinsip operator logika *Exclusive OR*. Cara enkripsinya adalah dengan meng*XOR*-kan *plaintext* dengan kunci sehingga didapatkan *ciphertext*-nya. Sebaliknya untuk proses dekripsi adalah dengan meng-*XOR*-kan *ciphertext* dengan kunci sehingga didapatkan *plaintext*-nya kembali. Keutamaan dari teknik ini adalah mudah diimplementasikan dan operasi *Exclusive OR* tidak sulit secara komputasional namun *Chiper Exclusive OR* benar-benar lemah terhadap serangan plainteks umum. Kelemahan dari algoritma *Exclusive OR* adalah pada saat

dienkripsi untuk kedua kalinya, maka pesan awal akan tertayang kembali (Ilyas, 2009). Oleh karena itu perlu dilengkapi dengan mekanisme keamanan tambahan lainnya.

Algoritma *RC4* adalah algoritma kriptografi modern simetris yang termasuk *cipher* aliran (*stream cipher*) karena operasi enkripsinya dilakukan per karakter 1 *byte* untuk sekali operasi (Ariyus, 2008). Inti dari enkripsi *RC4* adalah pembangkitan kunci aliran (*keystream*) yang bersifat acak semu (*pseudo random*) (Kromodimoeljo, 2010). Untuk kriptografi modern, penulis memilih algoritma ini dikarenakan proses algoritma ini cepat dan juga kuat.

Berdasarkan uraian di atas, maka dilakukan penerapan kriptografi pengamanan informasi *QR-Code* menggunakan algoritma *Exclusive OR* yang dikombinasikan dengan algoritma *RC4* yang selanjutnya diimplementasikan dalam bentuk *QR-Code*. Oleh karena itu penulis tertarik untuk mengambil studi kasus tugas akhir yang berjudul "IMPLEMENTASI KRIPTOGRAFI EXCLUSIVE OR KOMBINASI ALGORITMA RC4 SEBAGAI PENGAMANAN DOKUMEN DENGAN MEMANFAATKAN QR-CODE".

1.2 Rumusan Masalah

Berdasarkan permasalahan yang dijelaskan pada latar belakang, maka didapatkan permasalahan sebagai berikut:

1. Bagaimana mengkombinasikan enkripsi algoritma *Exclusive OR* dengan Algoritma *RC4* dan diimplementasikan dalam bentuk *QR-Code*?
2. Apakah kriptografi *Exclusive OR* yang dikombinasikan dengan *RC4* dan diimplementasikan dalam *QR-Code* pada dokumen dapat mengurangi kecurangan/pemalsuan?

1.3 Tujuan Penelitian

1 Mampu melakukan enkripsi dan meningkatkan keamanan Algoritma *Exclusive OR* yang dikombinasikan dengan Algoritma *RC4* dan diimplementasikan ke dalam bentuk *QR-Code*.

2 Menghasilkan suatu sistem pemindai untuk membaca data *QR-Code* dan didekripsi dengan menggunakan Algoritma *Exclusive OR* yang dikombinasikan dengan algoritma *RC4* serta dapat menampilkan keterangan dokumen.

1.4 Batasan Masalah

1. Melakukan enkripsi dan dekripsi terhadap nomor dokumen/sertifikat yang berupa *QR-Code*.
2. Pemindaian *QR-Code* menggunakan *Android versi 4.0.1* keatas dan dilakukan pada media tercetak.
3. Data yang digunakan sebagai input dalam proses pengimplementasian adalah *alfanumerik*.
4. Data yang akan digunakan pada proses kriptografi adalah dalam bentuk teks yang dikodekan dalam *ASCII 128bit*.
5. Algoritma yang digunakan pada penelitian ini adalah Algoritma *Exclusive OR* dan Algoritma *RC4.*
6. Panjang kunci dibatasi sampai 3 karakter.
7. Pembangkitan *QR-Code* menggunakan *Library Zxing*
8. Bahasa pemrograman yang dipakai adalah *Java* dan *PHP*.

1.5 Manfaat Penelitian

1. Manfaat bagi penulis sendiri ialah mampu mengkombinasikan Algoritma *Exclusive OR* dengan Algoritma *RC4* yang diimplementasikan dalam bentuk *QR-Code* untuk melakukan deteksi keaslian dokumen sertifikat.
2. Dapat mengurangi atau meminimalisir terjadinya pemalsuan dokumen sertifikat pada suatu lembaga.