BAB I
PENDAHULUAN

1.1 Latar Belakang

Cryptographically Secure Pseudorandom Number Generator merupakan suatu pembangkit yang dapat menghasilkan bilangan acak yang tidak mudah diprediksi oleh lawan sehingga cocok untuk kriptografi. Pembangkit ini memiliki karakteristik yang bagus seperti lolos uji keacakan statistik. Di samping itu juga tahan terhadap serangan yang serius yang bertujuan untuk memprediksi bilangan acak yang dihasilkan.

Bilangan acak (*random*) banyak digunakan dalam kriptografi, misalnya untuk pembangkitan elemen-elemen kunci pada algoritma OTP, pembangkitan *initialization vector* (*IV*) pada algoritma kunci simetri, pembangkitan parameter kunci pada sistem kriptografi kunci publik dan sebagainya. Yang dimaksud acak di sini adalah bilangan yang tidak mudah diprediksi oleh pihak lawan. Sayangnya sangat sulit memperoleh bilangan acak dalam praktek kriptografi. Tidak ada prosedur komputasi yang benar-benar menghasilkan bilangan acak secara sempurna. Bilangan acak yang dihasilkan dengan rumus-rumus matematika adalah bilangan acak semu, karena bilangan acak tersebut dapat berulang kembali secara periodik. Pembangkit bilangan acak semacam itu disebut *Pseudorandom Number Generator* (PRNG).

Blum Blum Shub dan *modified* RSA adalah dua macam pembangkit bilangan acak yang termasuk dalam *cryptographically secure pseudorandom number generator* (CSPRNG), difungsikan sebagai *key* untuk enkripsi pada algoritma RC4. Algoritma RC4 saat ini banyak diterapkan pada *software* aplikasi yang memakai RC4 sebagai algoritma enkripsi, seperti aplikasi *secure sms* pada ponsel yang menggunakan J2ME dengan Netbeans IDE, dan juga digunakan secara luas pada sistem keamanan seperti protokol SSL (*Secure Socket Layer*).

Mengingat potensi penggunaan RC4 di masa kini dan masa yang akan datang, maka analisis dan peningkatan performansi RC4 merupakan topik penelitian yang penting dan menarik, sehingga diharapkan akan memperkuat algoritma enkripsi RC4.

1.2 Tujuan Penulisan Tugas Akhir

Berikut ini beberapa tujuan dari penulisan Tugas Akhir ini, antara lain :

1. Melakukan simulasi dan analisis terhadap *Blum Blum Shub* dan *modified* RSA sebagai pembangkit bilangan acak *Cryptographically Secure Pseudorandom Number Generator* (CSPRNG)
2. Menggunakan kedua pembangkit bilangan acak tersebut pada algoritma RC4 sebagai *key* untuk enkripsi dan membandingkan diantara keduanya sehingga diketahui manakah yang mempunyai performansi lebih baik

1.3 Perumusan Masalah

Dalam Tugas Akhir ini terdapat beberapa masalah dan dirumuskan sebagai berikut :

1. Pembangkitan bilangan acak menggunakan *Blum Blum Shub* dan *modified* RSA
2. Perbandingan jenis-jenis CSPRNG (*Blum Blum Shub* dan *modified* RSA) dan memilih jenis CSPRNG yang terbaik dilihat dari beberapa parameter dan kondisi
3. Proses pembuatan *ciphertext* menggunakan algoritma RC4
4. Teknik penggabungan CSPRNG (*Blum Blum Shub* dan *modified* RSA) dengan algoritma RC4 dilihat dari beberapa parameter dan kondisi
5. Keuntungan dan kerugian pada proses penggabungan tersebut serta parameter yang mempengaruhinya
6. Teknik membuat simulasi untuk proses pembangkitan bilangan acak

1.4 Batasan Masalah

Dalam penulisan Tugas Akhir ini batasan-batasan dan ruang lingkupnya adalah :

1. Informasi yang akan dienkripsi (*plaintext*) adalah *character* (huruf, angka, atau simbol) dengan format .txt dan *image* dengan format .bmp 3 layer RGB
2. Metode CSPRNG yang digunakan adalah *Blum Blum Shub* dan *modified* RSA
3. Menggunakan algoritma RC4 untuk proses enkripsi dan dekripsi
4. Tidak membahas aspek keamanan *integrity*, *authentication* dan *nonrepudiation*
5. Tidak membahas penyadapan pada kanal transmisi dan asumsi tidak ada bit yang *error* pada saat transmisi
6. Simulasi dilakukan dengan menggunakan software Matlab 2007a

1.5 Metodologi Penelitian

Metodologi penelitian yang dilakukan dalam Tugas Akhir ini meliputi :

1. Penelitian dilakukan dalam bentuk simulasi program menggunakan software Matlab 2007a sehingga dimungkinkan untuk mengamati variable-variabel input dan meneliti pengaruhnya terhadap performansi *cryptography*
2. Pengumpulan data-data penunjang diperoleh dari hasil simulasi yang dilakukan dan dari data-data yang diperoleh dari *paper* pada daftar pustaka
3. Melakukan studi *literature* dengan mempelajari permasalahan yang berkaitan dengan sistem *cryptography*
4. Proses pengujian dilakukan dengan *input* berupa *character* (huruf, angka, atau simbol). Selain dari performansinya sendiri, dilakukan analisis statistik terhadap keluaran untuk mengetahui performansi dari *cryptography* tersebut

1.6 Sistematika Penulisan

Susunan penulisan dalam Tugas Akhir ini adalah sebagai berikut :

BAB I PENDAHULUAN

Bab ini membahas tentang latar belakang, maksud dan tujuan, permasalahan, batasan masalah, metodologi penelitian dan sistematika penulisan.

BAB II DASAR TEORI

Bab ini berisi teori dasar mengenai konsep kriptografi, metode pembangkitan bilangan acak CSPRNG yang difungsikan sebagai *key* untuk enkripsi pada algoritma RC4.

BAB III PERANCANGAN DAN IMPLEMENTASI

Bab ini berisi tahapan perancangan dan pemodelan sistem yang dilanjutkan dengan implementasi hasil perancangan ke dalam fungsi dan prosedur untuk masing-masing algoritma.

BAB IV PENGUJIAN DAN ANALISIS

Bab ini berisi hasil analisis dari hasil implementasi berdasarkan pengujian sistem secara keseluruhan dengan parameter-parameter yang telah ditentukan.

BAB V KESIMPULAN DAN SARAN

Bab ini berisi kesimpulan dari hasil analisis yang telah dilakukan dan saran-saran untuk pengembangan selanjutnya.