BAB I
PENDAHULUAN

1.1 Latar Belakang

Seiring perkembang zaman, kegiatan menyimpan data dan informasi dalam bentuk digital memiliki banyak resiko. Diantaranya terdapat resiko masalah keamanan yang merupakan salah satu aspek terpenting dalam sistem. Namun hal ini sering kurang mendapat perhatian dari para perancang dan pengelola sistem informasi. Bahkan pada prioritasnya keamanan sering berada pada urutan setelah tampilan [1]. Pada informasi yang sensitif pada golongan tertentu, sangat fatal bila diketahui oleh pihak yang tak seharusnya mengetahuinya, maka dalam proses penyampaian dan penyimpanannya diperlukan aspek kerahasiaan.

Pada 24 November 2014 lalu, terjadi peretasan (*hacking*) terhadap Sony Pictures Entertainment. Data dan informasi yang dicuri oleh pelaku merupakan data sensitif dan rahasia, diantaranya informasi pribadi karyawan Sony Pictures beserta keluarganya, informasi gaji para eksekutif perusahaan, hasil salinan dari film-film Sony yang belum diluncurkan, dan informasi lainnya. Pelaku menyebut dirinya sebagai "Guardians of Peace" atau "GOP" dan menuntut pembatalan rilisnya film “The Interview” dengan plot cerita rencana pembunuhan presiden Korea Utara, Kim Jong-un. Para peretas mengklaim telah mengambil data setidaknya lebih dari 100 Terabyte, dan setelah dilakukan penelusuran ternyata terdapat bukti bahwa bocornya dokumen-dokumen sensitif pada Sony Pictures adalah jaringan kerja (*network*) tidak dilakukan enkripsi secara internal atau *password-protected* [2]. Dalam fakta ini dapat diambil pelajaran bahwa untuk sekelas perusahaan multi-nasional sangat diperlukan keamanan informasi yang kuat, tidak hanya perusahaan besar saja yang memerlukan aspek keamanan informasi, tapi juga semua jenis organisasai yang menyangkut kepentingan masyarakat luas, bahkan tiap individu itu sendiri.

Pengguna teknologi informasi di Indonesia, utamanya pemerintahan harus memprioritaskan peningkatan keamanan data dan informasi. Saat ini telah terjadi tindak kejahatan pencurian informasi dan penyadapan yang dilakukan oleh oknum negara-negara lain, sehingga dapat merugikan dan mengganggu kedaulatan negara yang menjadi korban, termasuk didalamnya Indonesia. Hal itu akan menimbulkan masalah yang serius dan apabila lambat ditangani akan berakibat sangat buruk. Maka dari itu aspek keamanan sangat diperlukan untuk dijadikan prioritas utama.

Untuk mengurangi tindak kejahatan yang terkait dengan keamanan data, maka kriptografi bisa dijadikan solusi yang tepat. Kriptografi dapat juga digabungkan dengan cabang ilmu lainnya seperti matematika, sebagai contoh adalah algoritma *BBS* (*Blum Blum Shub*). Teknik *BBS* (*Blum Blum Shub*) menghasilkan kemunculan angka secara acak yang merupakan syarat penting untuk memperbaiki dan meningkatkan kekuatan dalam kriptografi, karena pembangkit bilangan acak semu tidak dapat diprediksi oleh lawan cocok untuk kriptografi [3]. Penelitian memakai teknik *BBS* (*Blum Blum Shub*) sebagai pembangkit kunci lalu akan diterapkan pada algoritma *One Time Pad* yang divariasi pada pesan bertipe teks. Alasan menggunakan *One Time Pad* adalah sebuah algoritma *cipher* yang memiliki persyaratan sebagai *unbreakable cipher* yang mewajibkan kunci harus dipilih secara acak, dan panjang kunci harus sama dengan plainteks yang akan dienkripsikan. Oleh karena itu diperlukan algoritma pembangkit kunci agar memudahkan penggunanya dalam mengingat kunci. Alasan teknik *BBS* sebagai pembangkit kunci pada algoritma OTP, karena *BBS* merupakan *CSPRNG* (*Cryptographically Secure Pseudorandom Generator*) yang tahan terhadap serangan yang serius dan teruji lolos pada uji keacakan statistik. Sedangkan penelitian berfokus pada pesan bertipe teks, karena penggunaan informasi berjenis teks sangat penting dimasyarakat dalam melakukan komunikasi, hal tersebut terlihat pada kegaiatan sehari-hari seperti berkirim surat konvensional, e-mail, dan SMS (Short Message Service). Untuk cipherteks yang dihasilkan adalah berupa bilangan hexadecimal yang lebih cocok diterapkan

daripada bilangan yang lainnya sehingga dari penelitian ini aspek keamanan pada kerahasiaan pesan dapat terpenuhi.

Dari latar belakang yang telah ada, penelitian menggabungkan teknik BBS dengan OTP, sehingga penelitian dibuatlah judul "IMPLEMENTASI PENGAMANAN PESAN BERTIPE TEKS MENGGUNAKAN ALGORITMA ONE TIME PAD DENGAN PEMBANGKIT KUNCI BLUM BLUM SHUB YANG TELAH DIVARIASI" sebagai judul untuk menyusun laporan Tugas Akhir guna menyelesaikan Program Strata 1 di Universitas Dian Nuswantoro Semarang.

1.2 Rumusan Masalah

Dari latar belakang di atas, dapat merumuskan permasalahan pada penelitian yaitu :

1. Bagaimana cara meningkatkan aspek keamanan pesan yaitu kerahasiaan pada pesan bertipe teks?
2. Bagaimana cara mengatasi kelemahan teknik algoritma kriptografi yaitu OTP (*One Time Pad*) pada bagian kunci yang harus sepanjang plainteks dan sulit dalam proses penyimpanan dan mengingatnya dengan menggunakan pembangkit kunci BBS (*Blum Blum Shub*).

1.3 Batasan Masalah

Untuk menghindari penyimpangan dari penelitian serta keterbatasan pengetahuan, maka dibuat ruang lingkup dan batasan masalah yaitu :

a. Variasi kunci menggunakan iterasi, *wrapping*, atau kombinasi keduanya.
b. Hasil enkripsi yang dihasilkan program adalah hexadesimal.
c. Program hanya dapat mengenkripsi dan mendekripsi teks.
d. Program hanya memberikan aspek kerahasiaan *(confidentiality)*.

e. Program hanya berjalan pada lingkungan sistem operasi Windows.

1.4 Tujuan Penelitian

Berdasarkan rumusan masalah di atas, maka tujuan dari laporan tugas akhir yang dibuat, yaitu :

1. Meningkatkan aspek keamanan pesan berjenis teks dengan algoritma kriptografi *One Time Pad* (OTP) yang memiliki persyaratan sebagai *unbreakable cipher*.
2. Menggunakan teknik pembangkitan kunci acak *BBS* (*Blum Blum Shub*) yang dapat memudahkan sebagai pembangkitan dan mengingat kunci pada algoritma OTP.

.

1.5 Manfaat Penelitian

Ada manfaat yang didapat bagi penulis dan pihak lain dari laporan tugas akhir ini antara lain :

1. Bagi Penulis

   Menambah wawasan mengenai kriptografi dan cara mengimplemantasi. Selain itu penulis dapat menggunakan metode kriptografi dengan metode lain untuk pengembangan.

2. Bagi Pengguna Lain

   Meningkatkan keamanan data dalam pengiriman pesan, sehingga mengurangi ancaman pencurian informasi dan serangan, serta mempermudah mengingat panjang kunci dalam proses enkripsi dan dekripsi. Selain itu juga mempermudah dalam menerapkan dan menggunakan teknik kriptografi karena penerapannya yang sederhana.

3. Bagi Universitas

   Menambah koleksi jumlah penelitian yang berkaitan dengan ilmu pengetahuan dan teknologi. Dan diharapkan dapat meningkatkan minat mahasiswa dalam melakukan penelitian.