BAB I
PENDAHULUAN

1.1 Latar Belakang

Password merupakan kumpulan karakter atau *string* yang digunakan oleh pengguna jaringan yang mendukung banyak *user* (*multiuser*) untuk melakukan autentikasi atas identitas dirinya kepada sistem keamanan yang dimiliki oleh jaringan atau sistem tersebut. Sistem akan membandingkan input kode-kode yang dimasukkan oleh pengguna/*user* (yang terdiri atas nama pengguna/*user name* dan *password*) dengan daftar atau basis data yang disimpan oleh sistem keamanan sistem atau jaringan tersebut (dengan menggunakan metode autentikasi tertentu, seperti halnya kriptografi, *hash* atau lainnya). Jika kode yang dibandingkan cocok, maka sistem keamanan akan mengizinkan akses kepada pengguna tersebut terhadap layanan dan sumber daya yang terdapat di dalam jaringan atau sistem tersebut, sesuai dengan level keamanan yang dimiliki oleh pengguna tersebut. Idealnya *password* yang dapat dikatakan aman adalah *password* dengan gabungan dari karakter teks alfabet (*A-Z*, *a-z*), angka (*0-9*), tanda baca (*!?,.=-*) atau karakter lainnya yang tidak dapat (atau susah) ditebak oleh para *intruder* sistem atau jaringan. Meskipun begitu, banyak *user* masih menggunakan *password* yang berupa kata-kata yang mudah diingat, seperti halnya yang terdapat dalam kamus, ensiklopedia (seperti nama tokoh, dan lainnya), atau yang mudah ditebak oleh *intruder* system.

Kerahasiaan data sangat diperlukan dalam hal komunikasi data.Untuk menjamin keamanan dan kerahasiaan data tersebut diperlukan teknik tertentu untuk menyandikan data atau informasi yang disebut kriptografi. Ada berbagai

jenis algoritma kriptografi, salah satunya adalah menggunakan metode XOR. Perlu diketahui sebenarnya semakin sederhana algoritma pengenkripsian yang dibuat akan semakin baik, karena dengan demikian proses komputasinya akan semakin sedikit sehingga akan memakan waktu lebih sedikit untuk mengeksekusinya.

One time password yang dibuat dalam tulisan ini adalah suatu metode pengacakan *password* yang bekerja berdasarkan waktu. *Password* yang dihasilkan tidak akan sama disaat *user* melihat *password* yang diberikan sekarang dan 2 menit kedepan. *Password* yang dihasilkan pun tidak akan mungkin berulang, karena waktu akan terus berjalan maju kedepan sehingga tidak memungkinkan *password* tersebut muncul berulang.

Pada perancangan SISTEM MINIMUM *ONE TIME PASSWORD* MENGGUNAKAN *IC* 89C51 ini dibuat dengan tampilan LCD 2x16 dan mempunyai beberapa fitur penting yang merupakan keharusan dari alat *One time Password* yaitu sebuah modul yang dibuat hanya akan terhubung sekali untuk melakukan sinkronisasi waktu antara modul dan komputer, setelah itu modul dan alat akan tidak berhubungan sama sekali dengan komputer maupun peralatan elektronik lainnya. Walau dengan tidak adanya hubungan sama sekali dengan sistem di komputer, alat ini tetap bisa berjalan, sistem komputer akan tetap dapat menerima *input* kode-kode angka yang ditampilkan dalam tampilan LCD 2x16 berupa 8 digit angka dan huruf. Penelitian ini memiliki *research question*, yaitu bagaimana melakukan penyetaraan *clock* baik dari mikrokontroler dan komputer, bagaimana agar *password* dapat diterima oleh komputer, bagaimana merancang *hardware* supaya memiliki dimensi kecil.

1.2 Pokok Permasalahan

Di dalam zaman era modern seperti saat ini banyak orang yang tinggal di kota seperti Jakarta, tidak mungkin tidak terhubung ke dalam suatu jaringan sehingga tidak pernah memiliki *password* untuk diingat. Salah satu contohnya membuka rekening di bank, pasti secara otomatis kita akan terhubung dengan sebuah jaringan sebuah perusahaan bank itu sendiri, sehingga memungkinkan untuk dapat mengakses kartu ATM dari melakukan pengecekan saldo sampai melakukan transaksi. Jaringan itu dapat berupa ruang lingkup yang dijalani sehari-hari dimana satu sama lainnya saling mengenal. Dalam ilmu komputer, jaringan itu sendiri dapat digambarkan sebuah lingkaran besar yang di dalamnya terdapat komputer yang saling terhubung satu dengan yang lainnya. Semakin hari pengguna jaringan semakin banyak, maka dibutuhkan sebuah identitas untuk setiap penggunanya. Dalam satu identitas diperlukan sebuah *password* sebagai proses autentikasi akan kebenaran orang yang hendak masuk ke dalam sistem itu benar orang yang seharusnya.

Pada penelitian tugas akhir perancangan sistem minimum *one time password* menggunakan *IC* 89C51*,* penulis ingin membuat sebuah alat yang dapat menampilkan sebuah *password* yang dapat berubah-ubah setiap 2 menit, sehingga *user* yang memiliki modul *one time password* itu sendiri tidak akan bisa mengetahui *password* apa yang akan diberikan di menit-menit kedepan.

Alat ini dibuat dengan judul sistem minimum *one time password* menggunakan *IC* 89C51, aplikasi *one time password* yang dibuat berbasiskan kepada waktu dalam menghasilkan *password*. Alat *one time password* ini digunakan dengan *software* yang telah dirancang sedemikian rupa. Laporan ini

akan memberikan hasil pengujian sistem yang sudah dibangun, menjelaskan dan menganalisis kondisi-kondisi yang diujikan pada sistem, dan implementasi dari sistem yang sudah dibangun tersebut.

1.3 Pembatasan Masalah

Password yang dihasilkan menggunakan 8 digit deretan *password* dan dalam heksadesimal, dibatasi dengan heksadesimal dengan tujuan supaya pemakai tidak kesulitan ketika melakukan input pengetikan *password* ke dalam sistem.

Alat dirancang dengan pengaturan waktu 2 menit sekali *password* baru akan diberikan (menit genap), ini dimaksudkan untuk memberikan kerenggangan waktu kepada *user* dalam melakukan *input* 8 digit *password* ke dalam sistem.

Software yang dibuat dalam sistem komputer dibuat dengan sekecil mungkin, semata hanya untuk melakukan percobaan bahwa *password* bekerja dengan baik tanpa ada masalah. *Software* akan dilakukan pengetesan hanya dalam satu komputer, tetapi *user* bisa banyak karena keterbatasan jumlah alat yang dibuat. Dalam penelitian ini satu alat akan digunakan banyak *user*, tetapi nanti dalam penerapan sebenarnya, satu alat (*password)* akan digunakan hanya oleh satu orang dan tidak dapat dipindahtangankan. Untuk memperbanyak alat, cukup mengubah *key* yang ada di dalam program sehingga 1 pemakai akan memiliki *key* yang berbeda-beda.

Algoritma dalam mendapatkan *password* menggunakan metode XOR, dari hasil perhitungan menit, jam, tanggal, bulan, tahun kemudian hasilnya akan di XOR kan dengan membaca *key* pada tabel EncryptKey. Hasil XOR yang didapat

akan ditampilkan dalam LCD 2x16 dan akan digunakan sebagai *password* untuk masuk ke dalam sistem.

1.4 Tujuan Penelitian

Tujuan penelitian tugas akhir ini adalah membuat alat dengan sistem minimum dengan kemampuan menghasilkan sebuah *password* yang dapat berubah-ubah yang berbasiskan waktu (*one time password*). Dengan berubahnya *password* tiap dua menit sekali ini otomatis dapat berguna sekali sebagai *user* karena *user* tidak perlu direpotkan lagi dengan mengingat sebuah *password* yang memiliki kemungkinan untuk hilang atau terlupa. Untuk mencapai tujuan tersebut diperlukan studi literatur, mencari tahu ciri-ciri *password* yang aman, mencari tahu bagaimana menghasilkan sebuah *password* yang diyakini aman.

1.5 Metodologi Penelitian

Metodologi untuk menyelesaikan permasalahan yang ada pada topik ini adalah dengan melakukan studi literatur, yaitu: dengan melakukan penelitian lewat buku – buku yang ada, literatur dan *paper* yang ada, studi kasus yang pernah ada.

Selain dengan studi literatur, juga dengan melakukan studi lapangan, yaitu: dengan melihat ukuran alat yang telah beredar dipasaran, melakukan perancangan *hardware* dengan bahan dasar akrilik dan *software* yang dibutuhkan untuk implementasi penelitian ini, setelah itu melakukan pengujian dan perbaikan melalui kasus-kasus yang diujikan untuk mendapatkan informasi dan pengetahuan, baik pada perancangan *hardware* maupun *software (debugging)*.

Melalui pengalaman terhadap hasil percobaan yang terjadi melakukan perbaikan pada sistem agar dapat berjalan dengan baik (proses *trial and error*).

Pada akhirnya dilakukan penulisan laporan tugas akhir sebagai bentuk pertanggung jawaban dan hasil dari pengerjaan penelitian sistem minimum *one time password* menggunakan *IC* 89C51. Termasuk proses penulisan laporan (buku) pertanggung jawaban penelitian.

1.6 Sistematika Penulisan Laporan

Sistematika penulisan laporan tugas akhir ini secara garis besar terdiri dari beberapa bab yang terdapat pada laporan penelitian ini, seperti:

BAB I. PENDAHULUAN

Pada bab pendahuluan ini akan dipaparkan mengenai latar belakang masalah, pokok permasalahan yang dipilih, pembatasan masalah, tujuan penelitian, metodologi perancangan sistem, dan sistematika penulisan laporan yang dibuat.

BAB II. LANDASAN TEORI

Penjelasan mengenai teori-teori pendukung, metode-metode, prinsip-prinsip dan informasi tambahan lainnya dalam memecahkan masalah dan berguna dalam penelitian akan dimasukkan pada bab ini.

BAB III. PERANCANGAN SISTEM

Pada bab ini akan dipaparkan mengenai langkah-langkah yang dilakukan pada sistem minimum *one time pad* menggunakan IC89C51. Mencakup pengerjaan dari sisi *hardware* dan *software* serta bagaimana cara menghubungkan berbagai komponen elektronik agar menjadi suatu sistem yang dapat digunakan antar *hardware* tersebut.

BAB IV. PENGUJIAN DAN IMPLEMENTASI

Pada bab ini diberikan hasil pengujian perancangan *hardware*, hasil pengujian perancangan *software*, pengujian sistem yang telah dibuat dan analisis hasil keluaran sistem setelah dijalankan dan implementasi yang cocok untuk alat tersebut.

BAB V. KESIMPULAN DAN SARAN

Bab ini berisi simpulan dan saran mengenai hasil penelitian tugas akhir yang telah dilakukan.