BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini sangat pesat sekalidenganbanyaknya penemuan-penemuan yang telah ditemukan. Salah satu perkembangan teknologi yang terlihat adalah perkembangan di bidang teknologi informasi. Teknologi informasi sudah menjadi kebutuhan hidup bagi setiap orang, hampir semua orang tidak bisa lepas dari teknologi informasi ini. Banyak sekali penemuan di bidang teknologi informasi yang sudah sangat penting dalam kehidupan, seperti teleponselular, laptop, internet dan lain-lain.

Perkembangan teknologi ini banyak sekali dimanfaatkan oleh pihak perusahaan atau departemen pemerintahan. Di dalam perusahaan banyak sekali pekerjaan yang bisa diselesaikan dengan komputer, untuk membuat laporan, menyimpan dokumen dan sebagainya. Penggunaan internet saat dibutuhkan sekali untuk bisa mengetahui *update* berita terkini dan informasi yang dibutuhkan dari perusahaan ataupun kita mengirim data ke perusahaan lain. Sama halnya di departemen pemerintahan teknologi informasi banyak sekali di gunakan dalam proses pemerintahan.

Begitupesatnya teknologi informasi berkembang pasti ada sisi negatifnya dari perkembangan tersebut. Contohnya *cyber crime* atau dalam bahasa Indonesianya kejahatan dunia maya adalah yaitu kejahatan menggunakan komputer atau jaringan komputer menjadi alat, sarana, tempat terjadinya kejahatan. Kejahatan

dunia maya diantaranya adalah penipuan secara *online*, pembuatan cek palsu, pornografi, penipuan indentitas dan sebagainya.

Salah satu lini yang mengantisipasi adanya tindak kejahatan dalam dunia maya adalah perbankan. Pada zaman sekarang kegiatan perbankan sudah dapat di akses dimana saja tanpa harus pergi kecabang suatu bank.Teknologi ini disebut *e-banking*, salah satu dari *e-banking* adalah internet *banking*. Di dalam internet *banking* untuk melakukan transfer ke rekening lain membutuhkan alat otentikasi berupa token. Alat otentikasi inilah yang merupakan pengaman dari tindak kejahatan dunia maya.

Di dalam proses otentikasi internet *banking* dengan token pada bank-bank di Indonesia biasanya menggunakan angka dalam proses otentikasinya. Biasanya terdiri dari 8 angka yang di berikan dan harus di masukan ke dalam token, setelah dimasukan maka akan keluar angka respon dari token tersebut yang nantinya harus dimasukan kembali kedalam internet banking tadi untuk dilakukan pencocokan. Untuk ituakandibuat token yang menggunakan huruf dalam proses otentikasinya, karena jika dihitung dalam permutasinya jumlah *challenge* atau respon yang dihasilkan lebih banyak huruf di bandingkan dengan angka.Di dalam proses otentikasinya maka digunakan algoritma RSA. RSA merupakan salah satu jenis kriptografi asimetri karena memiliki 2 kunci yaitu kunci publik (*public key*) dan kunci pribadi (*private key*). Awal terciptanya algoritma RSA ini adalah oleh tiga orang peneliti yang berasal dari MIT (*Massachusscet Institute of Technology*), yaitu Ron Rhivest, Adi Shamir, Leonard Adleman. Ketiganya menciptakan algoritma ini dan menamainya sesuai dengan inisial nama mereka,

(R)ivest, (S)hamir, (A)dleman. Dibantu dengan algoritma Diffie-Hellman, yaitu algoritma pertukaran kunci yang membantu dalam proses otentikasinya.

1.2 Rumusan Masalah

Berdasarkan latar belakang di atas, masalah utamadalam penelitian ini adalah ”Bagaimana membuat perangkat lunak untuk proses otentikasi pada internet *banking* dengan menggunakan *e-secure* berupa tokenberbasishuruf dalam proses transfer ke rekening lain dengan memanfaatkan algoritma Diffi-Hellman dan RSA?”.Sedangkan kajian khusus yang di teliti adalah sebagai berikut:

1. Bagaimana pembuatan token berbasis huruf dengan memanfaatkan algoritma RSA?
2. Bagaimana proses otentikasi dengan menggunakan algoritma RSA dan Diffie-Hellman?
3. Bagaimana memodelkan proses otentikasi pada internet banking dan token?

1.3 Pembatasan Masalah

Dari rumusan masalah di atas maka dibuat pembatasan masalah agar penelitian bisa difokuskan sebagai berikut:

1. Token dibuat dengan 2 proses yaitu denganDiffie-Hellman dan RSA.
2. Dalam proses otentikasi digunakan token berbasis huruf *lower case*.
3. Proses otentikasi dilakukan pada saat transaksi transfer antar rekening.

1.4 Tujuan

Tujuan dilakukannya penelitian ini adalah sebagai berikut

:

1. Membuat token berbasis huruf dengan memanfaatkan algoritma RSA.
2. Menerapkan algoritma RSA dan Diffie-Hellman dalam proses otentikasi internet *banking*.
3. Membuat pemodelan penerapan proses otentikasi token berbasis huruf dan internet *banking*.

1.5 Manfaat

Manfaat yang diharapkan dari penelitian ini adalah:

1. Mendapatkan model token alternative berbasis huruf dengan memanfaatkan algoritma RSA dan Diffie-Hellman yang memiliki jumlah permutasi *challenge* yang lebih banyak.
2. Memotivasi penelitian berikutnya, baik untuk permasalahan serupa maupun permasalahan lainnya menggunakan metode yang sama.

1.6 Metodologi Penelitian

Metode yang digunakan dalam penelitian yaitu:

1. Metode Pengumpulan Data
   a. Studi Literatur

      Pengumpulan data dari berbagai sumber yang berhubungan dengan permasalahan. Yaitu semua hal yang berhubungan dengan perbankan dan kriptografi.
2. Metode Pembangunan Perangkat Lunak

   Dalam hal pembangunan perangkat lunak penulis menggunakan metode *linear sequence model*. Adapun tahapan dari metode tersebut diantaranya:

a. Analisis Kebutuhan perangkat lunak

Pada tahap pertama dilakukan analisis terhadap permasalahan yang di hadapi. Sehingga nantinya akan muncul solusi bagaiamana cara masalah tersebut dapat diimplementasikan kedalam suatu perangkat lunak. Pada tahap ini dibutuhkan banyak sekali referensi supaya hasil dari analasisnya bisa menjawab permasalahan tadi.

b. Design Perangkat Lunak

Setelah proses analisis selesai maka dilakukanlah proses desain perangkat lunak. Proses ini adalah proses dimana kita akan membuat perangkat lunak. Bagaimana tampilan yang akan digunakan, antara tampilan satu dengan tampilan yang lainnya. Proses kerjanya akan seperti apa.

c. *Coding*

Dalam tahap *coding* baru desain yang tadi sudah di buat di implementasi kedalam bahasa pemograman.

d. Pengujian

Tahap pengujian dilakukan jika ketiga tahap tersebut telah dilalui. Gunanya untuk mengecek apakah perangkat lunak tersebut sesuai dengan yang kita harapkan atau mengecek apabila masih ada galat yang terjadi.

1.7 Sistematika Penulisan

Secara garis besar penulisan penelitian ini digunakan dalam 5 bagian yaitu :

BAB 1 PENDAHULUAN

Pada bab ini berisi latar belakang penelitian, rumusan masalah, batasan masalah, tujuan, manfaat, metodologi penelitian, serta sistematika penulisan yang akan dibuat dalam penelitian ini.

BAB 2 LANDASAN TEORI

Bab ini berisi teori yang mendasari penulis dalam melakukan penelitian, serta teori-teori yang membantu dalam penelitian. Yaitu teori mengenai e-banking dan algoritma RSA.

BAB 3 METODOLOGI PENELITIAN

Pada bab ini berisi tahap-tahap pembuatan sistem. Pada bab ini dituliskan tahap analisis perangkat lunak dan perancangan perangkat lunak yang akan di buat.

BAB 4 HASIL PENELITIAN DAN PEMBAHASAN

Pada bab ini membahas secara lebih lengkap mengenai penelitian yang telah dilakukan beserta penjelasan dari pengujian dengan menggunakan data-data.

BAB 5 KESIMPULAN DAN SARAN

Pada bab ini penulis membuat kesimpulan dari penelitian yang telah dilakukan beserta saran-saran yang diharapkan oleh penulis atau bagi para pembaca.