ABSTRAKSI

Seiring dengan berkembangnya teknologi, maka semakin meningkat pula kebutuhan akan keamanan data. Hal ini disebabkan karena seringnya terjadi penyalahgunaan atau penyelewengan teknologi sebagai sarana untuk membobol data milik orang lain, bahkan sering juga yang memanfaatkan data orang lain untuk kepentingan pribadi, seperti: pembobolan kartu kredit dan pembobolan rekening tabungan.

Oleh karena itu, banyak sistem yang menggunakan sistem password untuk menjaga keamanan datanya, seperti: untuk membuka e-mail atau setiap kali melakukan transaksi di ATM (Anjungan Tunai Mandiri) diperlukan password yang tepat.

Sistem password digunakan untuk dapat *login* ke dalam suatu sistem. Sistem akan mencocokkan nama *user* dengan password yang diinputkan, jika terbukti cocok atau sesuai maka user tersebut dapat masuk ke dalam sistem dan mengakses datanya.

Jika seseorang mempunyai password dan *user name* yang berbeda untuk setiap sistem, maka orang tersebut akan mengalami kesulitan untuk menghafal atau menyimpan setiap password dan *user name* dari setiap sistem tersebut. Karena jika kurang berhati-hati dalam menyimpan data-data tersebut, maka data-data tersebut bisa disalahgunakan bahkan dimanfaatkan oleh orang lain.

Untuk menjaga agar data-data tersebut dapat tersimpan dengan baik maka diperlukan sebuah aplikasi yang dapat menyimpan data-data password tersebut dalam bentuk terenkripsi. Untuk dapat membuka aplikasi tersebut diperlukan sebuah key-disks dan password.

Key-disks adalah sebuah kunci file yang menyimpan sebuah string (*key*) yang telah dienkripsi dengan menggunakan SHA1, yang dapat disimpan pada memory card pada PDA (Personal Digital Assistant). Yang kemudian key-disks akan dimasukkan pada PDA ketika hendak mengakses data password (keydisks, username dan password akan dicocokkan dengan data yang tersimpan pada database).

Sebagai *back-up* untuk data-data yang telah dibuat, maka dibuat web yang dapat menampilkan data-data yang sama dengan yang ada pada PDA (Personal Digital Assistant). Untuk mengakses web juga diperlukan keydisk dan login.

Proses kriptografi menggunakan komponen TwoFish dan SHA1, dimana komponen SHA1 digunakan untuk menghasilkan *message digest* yang kemudian digunakan sebagai *key* pada algoritma Twofish untuk melakukan proses enkripsi maupun dekripsi.

Kata kunci: password manager, twofish, SHA-1