**LAPORAN IV**

**KEAMANAN KOMPUTER**

****

**Disusun Oleh:**

**Nama : Hanifatul Azizah**

**NIM : 1400631017**

**PROGRAM STUDI MANAJEMEN INFORMATIKA**

**FAKULTAS TEKNIK**

**UNIVERSITAS MUHAMMADIYAH JEMBER**

**2015**

1. TEORI
2. Hash

Sebuah fungsi hash mengambil string dan menghasilkan string panjang tetap berdasarkan input. Output string disebut nilai hash. Fungsi hash yang ideal mematuhi berikut:  
Ini harus sangat sulit untuk menebak string masukan berdasarkan string output.  
Ini harus sangat sulit untuk menemukan 2 string input yang berbeda memiliki keluaran hash yang sama. Ini harus sangat sulit untuk memodifikasi string masukan tanpa memodifikasi nilai output hash. Fungsi hash dapat digunakan untuk menghitung checksum dari beberapa data. Bisa digunakan dalam tanda tangan digital dan otentikasi. Kita akan melihat beberapa  
aplikasi dalam rincian nanti.

b. Encryption algorithms

Algoritma enkripsi mengambil beberapa teks sebagai masukan dan menghasilkan ciphertext menggunakan kunci variabel. Anda memiliki 2 jenis cipher: blok dan aliran. cipher blok bekerja pada blok ukuran tetap (8 atau 16 byte). Stream cipher bekerja byte-bybyte. Mengetahui kunci, Anda dapat mendekripsi ciphertext.

c. Public-key algorithms

Salah satu kelemahan dengan algoritma enkripsi yang terlihat di atas adalah bahwa kedua sisi perlu tahu kuncinya. Dengan algoritma kunci publik, ada dua kunci yang berbeda: satu untuk mengenkripsi dan satu untuk mendekripsi. Anda hanya perlu untuk berbagi kunci enkripsi dan hanya Anda yang dapat mendekripsi pesan dengan pribadi Anda kunci dekripsi.

B.PRAKTIKUM

C. KESIMPULAN

Dari praktikum kali ini dapat disimpulkan bahwa kita dapat mengetahui fungsi hash dan mencoba encrypsi dan Descrypsi dengan mnggunakan aplikasi Python.