Seminar Nasional Royal (SENAR) 2018 ISSN 2622-9986 (cetak)
STMIK Royal – AMIK Royal, hlm. 249 – 252 ISSN 2622-6510 (online)
Kisaran, Asahan, Sumut - 3 September 2018

IMPLEMENTASI APLIKASI ENKRIPSI DAN DEKRIPSI TEXT PADA VISUAL BASIC .NET MENGUNAKAN ALGORITMA MERKLE HELLMAN KNAPSACK

Mardalius
Sistem Informasi, STMIK Royal
email : mardalius@royal.ac.id

Abstrak: *Pada saat ini dimasa globalisasi perkembangan teknologi sangatlah pesat terutama teknologi komunikasi dan informasi yang berbasiskan komputer, dimana teknologi menjadi andalan dan kebutuhan masyarakat dunia, sehingga setiap orang dengan mudahnya mengirim dan menerima pesan. Setiap pesan yang dikirim maupun diterima yang sifatnya rahasia maka diperlukanlah keamanan untuk menjaga pesan tersebut agar tidak di ketahui oleh orang lain. Keamanan suatu pesan merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan pesan itu sendiri, terutama bila pesan tersebut hanya boleh diketahui pihak tertentu saja. Ada banyak cara yang dilakukan untuk menjaga kerahasiaan dimulai dari pengamanan atau perlindungan secara fisik hingga kedalam bentuk algoritma berbasis matematika yang membuat pesan menjadi tidak terbaca.Sehingga pesan yang ada di dalamnya tidak dapat mudah diketahui oleh pihak-pihak yang tidak berhak dan hanya penerima pesan yang mampu menguraikan pesan yang diterimanya. Untuk melindungi akses pesan dari pihak-pihak yang tidak berkepentingan tersebut maka sangat diperlukan enkripsi dan dekripsi. Agar dapat dilakukan dengan baik, dibutuhkan suatu algoritma untuk enkripsi dan dekripsi. Algoritma yang digunakan disini adalah Algoritma Merkle Hellman Knapsack yang kemudian diiplementasikan dalam bentuk aplikasi menggunakan Bahasa pemprograman Visual Basic.Net.*

Kata kunci: *Enkripsi, Dekripsi, Merkle Hellman Knapsack, Visual Basic.Net*

PENDAHULUAN

Enkripsi adalah metode merubah data pesan (plaintext) menjadi data sandi (ciphertext), sedangkan dekripsi adalah metode merubah ciphertext menjadi plaintext. Algoritma yang digunakan ada 2 (dua) macam yaitu algoritma simetris dan algoritma asymmetries. Algoritma simetris adalah algoritma yang menggunakan kunci yang sama pada proses enkripsi dan dekripsinya. Sedangkan algoritma asymmetries adalah algoritma yang menggunakan kunci publik pada proses enkripsi dan kunci private pada proses dekripsinya. Merkle-Hellman Knapsack merupakan kriptosistem yang menggunakan algoritma asymmetries.Implementasi MerkleHellman

Knapsack yang digunakan menggunakan logika xor. Panjang kunci yang digunakan antara 8 sampai 72 bit Misalnya saja dalam perhitungan perkalian antara 2 (dua) bilangan dengan panjang 9 digit akan menghasilkan bilangan dengan panjang 18 digit yang akan ditampung dalam tipe long double, kemudian dengan fungsi modulo akan dihasilkan kembali bilangan dengan panjang 9 digit.

METODOLOGI

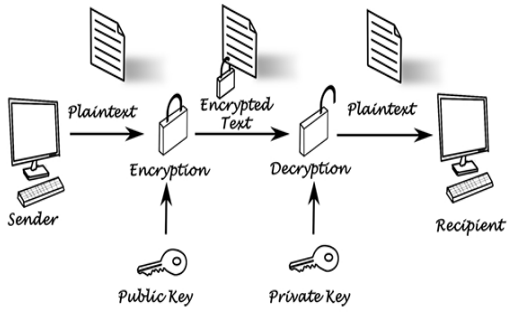
Metodologi dipergunakan oleh penulis untuk menganalisa, mengerjakan dan mengatasi masalah yang dihadapi. Kerangka teoritis atau kerangka ilmiah merupakan metode-metode ilmiah yang akan diterapkan dalam pelaksanaan penelitian. Pada kerangka kerja penelitian yang digunakan yaitu mempelajari literatur, mengumpulkan data, menganalisa data, menganalisa metode.

Kriptografi adalah ilmu pengetahuan dibidang teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, autentifikasi bagian, dan autentifikasi data asli. Kriprografi bukan hanya teknik untuk menyediakan keamanan informasi tetapi lebih dari sekedar suatu kumpulan teknik. Ilmu kriptografi merupakan salah satu cabang dari ilmu matematika. Dapat diartiakan pula kriptografi adalah ilmu pembacaan sandi yang membahas tentang penyandian dan penguraian dari isi sandi rahasia.

Konsep kunci public *cryptosystem* diperkenalkan oleh Whitfield Diffie dan Martin Hellman tahun 1976 dan dikembangkan menjadi kunci umum kritografi pada tahun 1978 oleh R.C Merkle dan M.E Hellman. Sistem

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

kriptografi Merkle-Hellman *Knapsack* meliputi 5 komponen yaitu Data *plaintext*, data *chipertext*, kunci kriptografi, fungsi transformasi enskripsi dan fungsi transformasi deskripsi. Blok diagram sistem kriptografi dengan metode knapsack dapat dilihat pada Gambar 1



Gambar 1. Pola Kerja Enkripsi Dan Deskripi

Langkah Langkah melakukan Enkripsi dan Deskripsi Menggunakan Algoritma Merkle-Hellman Knapsack adalah sebagai berikut

1. Menentukan superincreasing urutan *w* dibuat

$$w = (w_1, w_2, \ldots\ldots\ldots, w_n)$$

2. Menentukan Private Key (*r*)

Private key = $\sum w$

3. Kemudian, memilih nomor *q* yang lebih besar dari jumlah tersebut.

q > Private Key

4. Juga, memilih nomor *r* yang ada di
5.
6. kisaran $[1, q)$ dan coprime untuk *q*

$$r = 1 \leq w \leq q$$

7. kuci pribadi trdiri dari w, r, dan q
8. menghitung kunci publik, menghasilkan urutan β dengan mengalikan setiap elemen dalam *w* oleh *r* mod *q*

$$\beta = r\ w_i\ mod\ q$$

HASIL DAN PEMBAHASAN

Pada pembahasan disini akan kita ambil sebuah contoh bagaimana enkripsi dan dekripsi menggunakan metode Merkle - Hellman Knapsack sebagai berikut ;

1. Kunci Pribadi :
   w = {2, 7, 11, 21, 42, 89, 180, 354}
   r = 588
   q = 881
2. Plaintext : a (huruf a kecil)
3. Kunci Public :
   (2 * 588) mod 881 = 295
   (7 * 588) mod 881 = 592
   (11 * 588) mod 881 = 301
   (21 * 588) mod 881 = 14
   (42 * 588) mod 881 = 28
   (89 * 588) mod 881 = 353
   (180 * 588) mod 881 = 120
   (354 * 588) mod 881 = 236

   β = {295, 592, 301, 14, 28, 353, 120, 236}

4. huruf "a" ke biner (dalam hal ini, menggunakan ASCII atau UTF-8)

   01100001

5. mengalikan setiap bit masing dengan jumlah yang sesuai pada β

Tabel 1. Hasil Perkalian dengan β

0 * 295	0
1 * 592	592
1 * 301	301
0 * 14	0
0 * 28	0
0 * 353	0
0 * 120	0
1 * 236	236
Jumlah	1129

Maka hasil enskripsi dari huruf “a” adalah 1129

6. Untuk mendekripsi kembali mengalikan 1129 oleh r^{-1} mod q

   1129 * 442 mod 881 = 372

7. Sekarang terurai 372 dengan memilih elemen terbesar di *w* yang kurang dari atau sama dengan 372. Kemudian memilih elemen terbesar berikutnya kurang dari atau

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

sama dengan perbedaan, sampai perbedaan adalah 0 (nol):

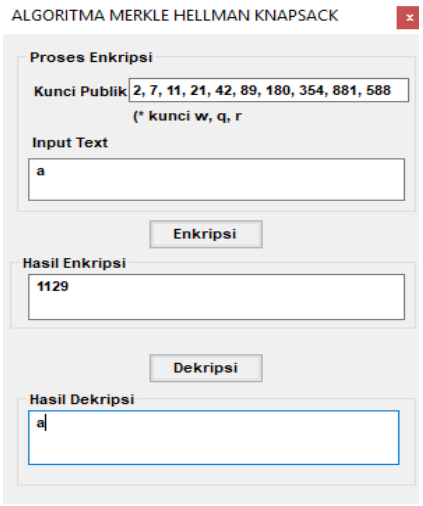
Tabel 2. Hasil Perkalian w dengan bilangan biner *a*

0 * 2	0
1 * 7	7
1 * 11	11
0 * 21	0
0 * 42	0
0 * 89	0
0 * 180	0
1 * 354	354
Jumlah	372

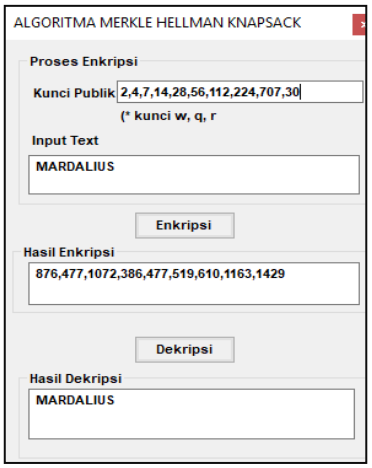
8. Ketika diterjemahkan kembali dari biner, ini "a" adalah pesan didekripsi akhir

Pada Implementasi Dan Pengujian kedalam Bahasa pemprograman disini kita menggunakan Bahasa pemprograman Visual Basic.Net kita akan membandingkan bagaimana hasil pengolahan data secara manual dengan hasil pengolahan data menggunakan sebuah software.

Pada gambar 1 merupakan hasil dari perhitungan menggunakan aplikasi yang di buat menggunakan Bahasa pemprograman Bisual Basic.Net :



Gambar 2. Hasil Enkripsi dan Dekripsi Huruf "a"



Gambar 3. Hasil Enkripsi dan Dekripsi Kata "MARDALIUS"

Pada Gambar 2 dan Gambar 3 adalah hasil dari proses Enkripsi Dan Dekripsi menggunakan Bahasa Pemprograman Visual Basic. Net

SIMPULAN

Algoritma Merkle Hellman Knapsack yang diimplementasikan ke dalam bahasa pemograman Visual Basic .Net. Dengan kunci yang dibentuk secara otomatis dari aplikasi memudahkan user untuk mendapatkan kunci, dan melakukan enkripsi dan dekripsi.

Pengujian aplikasi dalam enkripsi dan dekripsi menghasilkan chipertext berupa deretan angka dan menghasilkan plaintext input yang sama dengan plaintext output dari proses dekripsi.

ISSN 2622-9986 (cetak)
ISSN 2622-6510 (online)

DAFTAR PUSTAKA

Murdani, M. (2017). Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma Merkle Hellman Knapsack. *Pelita Informatika: Informasi Dan Informatika*, *16*(3).

Fadlan, M., & Hadriansa, H. (2017). Rekayasa Aplikasi Kriptografi dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman dan Affine Cipher. *Jurnal Teknologi Informasi dan Ilmu Komputer*, *4*(4), 268-274.

Primartha, R. (2014). Penerapan enkripsi dan dekripsi file menggunakan algoritma Data Encryption Standard (DES). *Jurnal Sistem Informasi*, *3*(2).

Hidayat, A., & Akmal, R. R. Cryptography Asymmetries Merkle-Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks.

Hasugian, A. H. (2013). Implementasi Algoritma Hill Cipher Dalam Penyandian Data. *Pelita Informatika Budi Darma*, *4*(2), 115-122.