METODE MERKLE HELLMAN UNTUK ENKRIPSI DAN DEKRIPSI PESAN WHATAPP

Dedi Leman[1], Maulia Rahman[2]
[1]Fakultas Teknik dan Ilmu Komputer, Teknik Informatika, Universitas Potensi Utama
E-mail: [1]dedileman280889@gmail.com, [2]mazrahman18@gmail.com

Abstrak: Enkripsi adalah metode merubah data pesan (*plaintext*) menjadi data sandi (*ciphertext*), sedangkan dekripsi adalah metode merubah *ciphertext* menjadi *plaintext*. *WhatsApp Messenger* adalah aplikasi pesan untuk ponsel cerdas (*smartphone*) dengan basic mirip *BlackBerry Messenger*. Aplikasi *WhatsAppMessenger* menggunakan koneksi internet 3G, 4G atau WiFi untuk komunikasi data. Dengan menggunakan *WhatsApp*, kita dapat melakukan obrolan online, berbagi file, bertukar foto dan lain-lain. Algoritma yang digunakan ada 2 (dua) macam yaitu algoritma simetris dan algoritma *asymmetries*. *Merkle-Hellman Knapsack* merupakan kriptosistem yang menggunakan algoritma *asymmetries*. Implementasi *Merkle-Hellman Knapsack* yang digunakan menggunakan logika xor. Panjang kunci yang digunakan antara 8 sampai 72 bit, Kemampuan ini membuat *Merkle-Hellman Knapsack* mempunyai keamanan yang kuat dengan panjang kunci yang pendek.. Sedangkan tujuan yang ingin dicapai yaitu mengaplikasikan metode *kriptosistem Merkle-Hellman Knapsack* menggunakan Bahasa Pemrograman Visual Studio 2010

Kata kunci: Enkripsi, dekripsi, whatapp, *Merkle-Hellman Knapsack*

Abstract: *Encryption is a method of changing message data (plaintext) into password data (ciphertext), while decryption is a method of converting ciphertext to plaintext. WhatsApp Messenger is a messaging application for smartphones that is basically similar to BlackBerry Messenger. The WhatsApp Messenger application uses a 3G, 4G or WiFi internet connection for data communication. By using WhatsApp, we can do online chat, share files, exchange photos and so on. The algorithm used is 2 (two) types, namely symmetric algorithms and asymmetries algorithms. Merkle-Hellman Knapsack is a cryptosystem that uses the asymmetries algorithm. The Merkle-Hellman Knapsack implementation used uses xor logic. The key length is used between 8 to 72 bits. This capability makes Merkle-Hellman Knapsack have strong security with a short key length. Whereas the aim to be achieved is to apply the Merkman-Hellman Knapsack cryptosystem using the Visual Studio 2010 Programming Language.*
Keywords: *Encryption, decryption, whatapp, Merkle-Hellman Knapsack*

1. 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 [1].

Whatsapp sebagai salah satu media sosial saat ini banyak yang menggunakan untuk kepentingan bersosialisasi maupun sebagai penyampaian pesan baik oleh individu maupun kelompok. Namun sejauh mana penggunaan Whatsapp oleh penggunanya maka dari latar belakang

tersebut diatas dapat diambil permasalahan seberapa besar Pemanwaatan Whatsapp sebagai media komunikasi dan kepuasan dalam penyampaian pesan Dikalangan Tokoh Masyarakat? Sedangkan tujuan penelitian ini untuk mendapatkan data dan informasi tentang Pemanwaatan Whatsapp sebagai media komunikasi dan kepuasan dalam penyampaian pesan kepada publik/audience melakukan percakapan melalui menu chat, bisa meng-copy, men-delete, atau memforward pesan. Gambar yang terkirim bisa di-forward. Selain itu juga dapat mengirim pesan suara maupun share lokasi keberadaan pengguna. Juga menyediakan fitur grup chat, dimana pengguna bisa mengumpulkan beberapa kontak untuk membuat sebuah grup chat [4].

Merkle-Hellman Knapsack merupakan kriptosistem yang menggunakan algoritma asymmetries. Implementasi Merkle- Hellman Knapsack yang digunakan menggunakan logika xor. Panjang kunci yang digunakan antara 8 sampai 72 bit. Karena dalam bahasa pemrograman Borland C++ tipe data yang paling tinggi adalah long double yang bisa menampung 18 digit. 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 [2]

Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses dimana informasi/ data yang hendak dikirim diubah menjadi bentuk yang hampir tidak dikenali sebagai informasi awalnya dengan menggunakan algoritma tertentu. Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal [3]

2. METODE KNAPSACK MERKLE HELLMAN

Metode Knapsack Merkle Hellman telah banyak digunakan untuk memodelkan solusi masalah di industri seperti pada kriptografi kunci publik. Knapsack Merkle-Hellman merupakan metode dalam kriptografi yang menggunakan algoritma asimetris dan memiliki 2 kunci utama, yakni kunci publik dan kunci privat. Kunci yang didistribusikan dikenal dengan istilah kunci publik, jika kunci publik ini diketahui oleh orang lain yang tidak berhak / berkepentingan, maka data yang dikirim akan tetap aman. Untuk kunci private adalah kunci yang tetap disimpan oleh pihak-pihak yang berhak.

ti = a* si mod p……. (1)

Dimana :

P : Bilangan Prima

S : bilangan integer superin creasing

T : Public Key

Si, p, a : Private Key

Ide dasar di balik skema enkripsi Merkle- Hellman adalah menciptakan masalah subset yang bisa dipecahkan dengan mudah dan kemudian menyembunyikan sifat *superincreasing* dengan perkalian modular dan permutasi. Vektor yang ditransformasikan membentuk pesan terenkripsi dan vektor superincreasing asli membentuk kunci pribadi dan digunakan untuk menguraikan pesan. Pada algoritma Merkle-Hellman Knapsack digunakan kunci privat dan kunci publik dalam melakukan proses kriptografinya, metode ini juga memiliki pengamanan ganda sehingga susah untuk ditembus.

3. PENERAPAN METODE MERKLE HELLMAN

Setelah melihat permasalah diatas maka peneliti mencoba untuk merancang suatu aplikasi enkripsi dan dekripsi pesan yang lebih baik sehingga dapat menghasilkan aplikasi enkripsi dan dekripsi pesan teks dengan tepat dan akurat. Sebagai comtoh pesan yang ada di whatapp yaitu :

Pesan yang ada di whatapp adalah **MEJA**

Langkah Pertama

Diberikan Private key dimana di masukkan oleh pengirim

s = (1,2,5,11,32,87,141),

a = 200,

p = 307

Langkah ke 2

Menjadikan private key menjadi public key dengan cara sebagai berikut :

Perhitungan Public Key (t) : dengan rumus

ti = a* si mod p…….(1)

t1 = a*s1 mod p = 200 * 1 mod 307 = 200

t2 = a*s2 mod p = 200 * 2 mod 307 = 93

t3 = a*s3 mod p = 200 * 5 mod 307 = 79

t4 = a*s4 mod p = 200 * 11 mod 307 = 51

t5 = a*s5 mod p = 200 * 32 mod 307 = 260

t6 = a*s6 mod p = 200 * 87 mod 307 = 208

t7 = a*s7 mod p = 200 * 141 mod 307 = 263

Didapatkan t

t = (200,93,79,51,260,208,263)

langkah ke 3

Plaintext : MEJA (77 69 74 65)

Masing – masing kode ASCII tersebut dikonversi ke biner

M= 77 : 1001101

E = 69 : 1000101

J = 74 : 1001010

A= 65 : 1000001

Langkah ke 4

Plaintext di bagi dalam block sesuai dengan banyaknya s, pada contoh ini banyaknya s adalah 7 digit.

1001101 y = 200 + 51 + 260 + 263 = 774

1000101 y = 200 + 260 + 263 = 723

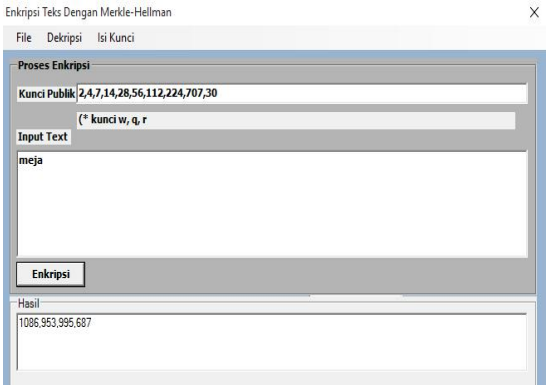
1001010 y = 200 + 51+208 = 459

1000001 y = 200 + 263 = 463

Didapatkan Ciphertext : 774, 723, 459, 463

3.1. Tampilan Enkripsi

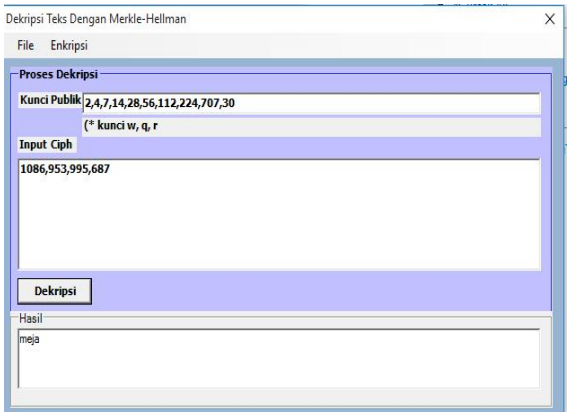
Tampilan menu form file merupakan tampilan yang berisi menu-menu yang berfungsi untuk menampilkan enkripsi dan tempat untuk isi kata- kata atau kalimat. Gambar tampilan enkripsi ditunjukkan pada gambar 1



Gambar 1. Gambar Aplikasi Enkripsi

3.2. Tampilan Dekripsi

Tampilan pada form ini merupakan proses deskripsi Gambar deskripsi ditunjukkan pada gambar 2.



Gambar 2. Gambar Aplikasi Dekripsi

4. KESIMPULAN DAN SARAN

4.1 KESIMPULAN

Berdasarkan hasil pembahasan dan uji coba yang telah dilakukan, dapat disimpulkan :

1. Hasil pengujian "Metode Merkle Hellman Untuk Enkripsi Dan Dekripsi Pesan Whatapp**"** menunjukkan bahwa kriptografi ini dapat mengindentifikasi seberapa besar kemungkinan pengirim mengirim pesan yang kepada penerima yang di *input* ke dalam sistem.
2. Hasil perhitungan metode merkle hellman yang telah diimplementasikan dalam skripsi ini telah memberikan hasil yang cukup memuaskan karena telah menggunakan metode yang sesuai dengan kebutuhan sistem yang menggunakan nilai pengirim dan penerima.
3. Bahasa pemrograman yang digunakan untuk membuat aplikasi yaitu *visual basic* 2010.

4.2 SARAN

Adapun saran untuk menyempurnakan sistem yang telah dibuat adalah sebagai berikut :

1. Sebaiknya sistem selalu dilakukan *update* secara berkala sesuai dengan perkembangan ilmu, yang tentunya berpengaruh terhadap sistem dalam enkripsi dan dekripsi, agar hasilnya lebih maksimal.
2. Selalu mem-backup data agar terhindar dari kemungkinan terjadinya kehilangan data yang penting yang disebabkan oleh kerusakan perangkat keras.
3. Untuk pengembangan sistem ini di masa yang akan datang diharapkan dapat membangun sistem yang memiliki data pengetahuan yang lebih mendetail.
4. Sebaiknya sistem ini dikembangkan dengan berbasis web sehingga bisa diakses.

DAFTAR PUSTAKA

[1] Muhammad Fadlan, 2017**."** *Rekayasa Aplikasi Kriptografi Dengan Penerapan Kombinasi Algoritma Knapsack Merkle Hellman Dan Affine Cipher***",** Vol. 4, No. 4, Desember 2017, hlm. 268-274 p-ISSN: 2355-7699

[2] Akik Hidayat, 2016**."** *Cryptography Asymmetries Merkle Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks***",** ISBN 978-602-72216-1-1, Prosiding Seminar Nasional MIPA 2016

[3] Mardalius, 2018**."** *Implementasi Aplikasi Enkripsi Dan Dekripsi Text Pada Visual Basic .Net Mengunakan Algoritma Merkle Hellman Knapsack***",** STMIK Royal – AMIK Royal, hlm. 249 – 252 ISSN 2622-6510 (online), Seminar Nasional Royal (SENAR) 2018 ISSN 2622-9986 (cetak)

[4] Murdani, 2017**."** Perancangan Aplikasi Keamanan Data Teks Menggunakan Algoritma *Merkle Hellman Knapsack***",** Jurnal Pelita Informatika, Volume 16, Nomor 3, Juli 2017 ISSN 2301-9425 (Media Cetak) Hal: 302-305

[5] Denis Surya, 2018**."** *Implementasi Aplikasi Enkripsi Dan Dekripsi Text Pada Visual Basic .Net Mengunakan Algoritma Tripel DES***",** STMIK Royal – AMIK Royal, hlm. 249 – 252 ISSN 2622-6510 (online), Seminar Nasional Royal (SENAR) 2018 ISSN 2622-9986 (cetak)

[6] Ahmad Suryadi , 2017**."** *Perancangan Aplikasi Keamanan Data Gambar Menggunakan Algoritma Merkle Hellman Knapsack***",** Jurnal Pelita Informatika, Volume 16, Nomor 3, Juli 2017 ISSN 2301-9425 (Media Cetak) Hal: 302-30

[7] Trisnani, 2017." *PEMANFAATAN WHATSAPP SEBAGAI MEDIA KOMUNIKASI DAN KEPUASAN DALAM PENYAMPAIAN PESAN DIKALANGAN TOKOH MASYARAKAT*, JURNAL KOMUNIKASI, MEDIA DAN INFORMATIKA Volume 6 Nomor 3 / November 2017