Implementasi Algoritma Merkle Hellman untuk Keamanan Database

[1)]Magdalena Simanjuntak
STMIK Kaputama, Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia
E-Mail : *magdalena.simanjuntak84@gmail.com*

[2)]Tioria Pasaribu
STMIK Kaputama, Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia
E-Mail : t4y0pasaribu@yahoo.co.id

[3)]Semiati Rahmadilla
STMIK Kaputama, Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara, Indonesia
E-Mail : syemiatirahmadilla@gmail.com

ABSTRACT
The development of information technology today has a huge impact, namely the issue of security and confidentiality of data. One solution that can be used to guarantee the confidentiality and security of information is cryptography. By using cryptography, a data can be secured through the decryption and encryption process. Security issues and database confidentiality are the most important aspects of an information system. One mechanism to improve database security is to use asymmetric algorithms such as the Merkle Hellmen algorithm. Merkle Hellman is one of the crypto systems that uses the key type of asymmetry. In the Merkle Hellman system, the keys used are 2 different keys, namely the public key and the secret key. Encryption generates ciphertext and decryption produces a plaintext for securing databases that want to be kept confidential. The advantages of this Merkle Hellman algorithm is that there is no need for confidentiality in the key distribution process. From the results of experiments that have been done with this application, the encrypted database becomes a form of message that cannot be understood (ciphertext), but after the decryption process is done, the database is successfully returned to its original form (plaintext) that can be understood.

Keywords: Cryptography, Database, Merkle Hellman

PENDAHULUAN

Perkembangan teknologi informasi saat ini membawa dampak yang sangat besar yaitu masalah keamanan dan kerahasiaan sebuah data yang merupakan hal yang sangat penting agar terhindarnya suatu proteksi terhadap pengrusakan data dan pemakaian data oleh pihak-pihak yang tidak bertanggung jawab yang memanfaatkan celah-celah keamanan agar dapat melihat, mengambil serta memanipulasi data. Oleh karena itu, diperlukan sebuah sistem atau aplikasi yang aman sehingga tidak mudah dibaca oleh pihak yang tidak punya kewenangan.

Salah satu solusi yang dapat digunakan untuk menjamin kerahasiaan dan keamanan suatu informasi adalah kriptografi. Dengan menggunakan kriptografi, maka suatu data dapat diamankan melalui proses dekripsi dan enkripsi. Terdapat beberapa metode kriptografi dalam melakukan proses dekripsi maupun enkripsi. Dan dalam penelitian ini yang akan diamankan adalah *database*. Masalah keamanan dan kerahasiaan *database* merupakan aspek terpenting dalam suatu sistem informasi. Karena dengan berkembangnya pengolahan data, sering kali satu aplikasi menggunakan *database* yang sama sehingga terjadi kegiatan copy paste *file database*[1]. Salah satu mekanisme untuk meningkatkan keamanan *database* adalah dengan menggunakan algoritma asimetris seperti algoritma Merkle Hellmen.

DASAR TEORI

2.1 Sejarah Kriptografi

Kriptografi mempunyai sejarah yang sangat menarik dan panjang. Kriptografi sudah digunakan 4000 tahun yang lalu, diperkenalan oleh orang-orang Mesir lewat *hieroglyph.* Dikisahkan, pada Zaman Romawi Kuno, pada suatu saat Julius Caesar ingin mengirinkan pesan rahasia kepada seorang jenderal di medan perang. Pesan tersebut

harus dikirimkan melalui seorang kurir. Karena pesan tersebut mengandung rahasia, Julius Caesar tidak ingin pesan rahasia tersebut sampai terbuka dijalan. Julius caesar kemudian memikirkan bagaimana mengatasinya[2]. Ia kemudian mengacak pesan tersebut hingga menjadi suatu pesan yang tidak dapat dipahami oleh siapapun terkecuali oleh jenderalnya saja. Tentu sang jenderak telah diberi tahu sebelumya bagaimana cara membaca pesan teracak tersebut. Yang dilakukan Julius Caesar adalah mengganti semua susunan alfabaet a, b, c yaitu a menjadi d, b menjadi e, c menjadi f dan seterusnya.

Dari ilustrasi tersebut, beberapa istilah kriptografi dipergunakan untuk menandai aktivitas-aktivitas rahasia dalam mengirim pesan. Apa yabg dilakukan Julius Caesar yang mengacak pesan, disebt sebagai enkripsi. Pada saat sang jenderal merapikan pesan yang teracak itu, prose itu disebut dekripsi. Pesan awal yang belum diacak dan pesan yang telah dirapikan, disebut *plaintext,* sedangkan pesan yang telah diaak disebut *ciphertext*.

2.2 Kriptografi

Kriptografi berasal dari bahasa Yunani. Menurut bahasa tersebut kata "kriptografi" dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan Graphia berarti writing (tulisan)[2]–[4].

Kriptografi merupakan seni dan ilmu ntuk menjaga kerahasiaan pesan dengan cara menyandikannya kedalam bentuk yang tidak dapat dimengerti lagi maknanya. Kriptografi disebut sebagai ilmu karena didalamnya terdapat metode (rumusan) yang digunakan, dan dikatakan sebagai seni karena dalam membuat suatu teknik kriptografi itu sendiri merupakan ciri tersendiri dari si pembuat dan memerlukan teknik khusus dalam mendesainnya. Dalam ilmu kriptografi, terdapat dua buah proses yaitu melakuan enkripsi dan deskripsi. Pesan yang dienkripsi disebut sebagai plaintext (teks biasa), disebut demikian karena informasi ini dengan mudah dibaca dan dipahami oleh siapa saja.

2.3 Merkle Hellman

Merkle Hellman adalah salah satu sistem kripto yang menggunakan tipe kunci asimetri. Pada sistem Merkle Hellman ini, kunci yang digunakan adalah 2 kunci yang berbeda. Satu kunci untuk mengenkrip dan satu kunci untuk mendekripsi.

Secara umum dapat digambarkan cara kerja sistem kriptografi Merkle-Hellman sebagai berikut :

a) Pesan dikonveri ke dalam bilangan biner yang kemudian dikalikan dengan kunci pblik. Hasil perkalian dijumlahkan lalu dikirim ke penerima pesan.
b) Penerima pesan menggunakan kunci rahasia untuk mencari terget sum. Dengan menggunakan algoritma target sum, penerima mendapatkan nilai pesan yang masih berupa bilangan biner {0,1}*. Untuk mendapatkan pesan aslinya, konversi bilangan biner ini ke karakternya.

2.4 Keunggulan Merkle Hellman

Keunggulan algoritma ini adalah proses pendistribusian kunci pada media yang tidak aman seperti internet, tidak memerlukan kerahasiaan. Karena kunci yang didistribusikan adalah kunci publik. Sehingga jika kunci ini sampai hilang atau diketahui oleh orang lain yang tidak berhak, maka pesan sandi yang dikirim akan tetapkan. Sedangkan kunci privat tetap disimpan (tidak didistribusikan)[5].

Merkle Hellman Knapsack punya kelebihan lain pada efesiensi jumlah kunci publik. Jika terdapat n user, maka hanya membutuhkan 1 kunci publik, sehingga untuk jumlah user yang sangat banyak, sistem ini sangat efesien. Dengan adanya pertukaran kunci dalam enkripsi-dekripsi data dengan kriptosistem krva eliliptik adalah pengamanan data berupa teks untuk menghindari adanya penyadapan yang dilakukan oleh pihak-pihak yang tidak berkepentingan[6]. Langkah-langkah penjelasan Matematika sebagi berikut :

1. Memilih urutan *superincreasing* dari jumlah bilangan bulat positif. Urutan *superincreasing* adalah salah satu dimana setiap nomor lebih besar dari jumlah semua sebelumnya angka. s = (s1, s2, s3, ….sn)
2. Untuk mengkonversikan semua karakter dari pesan ke biner. Urutan biner diwakili oleh variabel b.
3. Untuk memilih dua nomor integer (a) yang lebih besar dari pada jumlah semua nomor di urutan dan *co-prime* (r).
4. Urutan dan nomor dan r membentuk kolektif kunci pribadi *cryptosystem* tersebut.
5. Semua elemen – s1, s2, s3, … sn, dari urutan *s* adalah dikalikan dengan jumlah *r* dan *modulus* dari beberapa diambil dengan membagi dengan angka. Oleh karena itu, *pi* = *r si* mod *a*

6. Semua elemen p1, p2, p3, …. pn urutan p adalah dikalika dengan unsur-unsur yang sesuai dari biner urutan b.
7. Angka-angka tersebut kemudian ditambahkan untuk membuat pesan terenkripsi. Urutan M = (M1, M2, M3…Mn) membentuk kunci-kunci *cryptosystem.*

2.5 Proses Enkripsi

Dalam pembahasan aplikasi sistem algoritma Merkle Hellman ini akan ditinjau bagaimana cara seorang pengiriman pesan, sebut saja Alice. Sistem algoritma Merkle Hellman menggunakan tipe kunci enkripsi yang bersifat asimetris. Dengan demikian kunci yang digunakan untuk mengenkrip dan mendekrip pesan berbeda. Untuk kasus ini, misalnya Alice akan mendekrip pesan yang diterianya dari Bob maka Alice harus terlebih dahulu tahu kunci rahasia yang dia punya yang digunakan untuk mendapatkan kunci umum untuk Bob. Misalnya, Alice punya deretan integer superincreasing sebagai berikut w = 1 + 3 + 6 + 11 + 32 + 87 + 141 + 354 = 635. Karena jumlahnya 281 maka Alice memilih *q* bilangan prima yang lebih besar dari 635, misalnya 881, dan sembarang bilngan bulat *r* yang nilainya di antara 1 sampai w-1 yakni 588. Jadi kunci rahasia yang dimiliki Alice adalah :

$w_=$ (1,3,6,11,32,87,141,354)
q = 881
r = 588
keterangan :
w = bilangan super *increasing*
r = kunci *private*
q = bilangan pembagi
Untuk mendapatkan kunci publik maka digunakan rumus :

$t_{i=}$ r * w mod q

dimana :
t_i = kunci publik
r = kunci rahasia
w = bilangan super increasing
q = bilangan pembagi
dan hitung seperti cara di bawah ini :

Tabel 1. Proses Pencarian Kunci Publik

r		w		q		t_i
588	*	1	mod	881	=	588
588	*	3	mod	881	=	2
588	*	5	mod	881	=	297
588	*	11	mod	881	=	301
588	*	32	mod	881	=	315
588	*	87	mod	881	=	58
588	*	141	mod	881	=	94
588	*	354	mod	881	=	236

Dari tabel di atas didapatkan hasil kunci publik sebagai berikut :

t_i= (588,2,297,301,315,58,94,236)

Untuk proses enkripsi setiap karakter diubah ke dalam bentuk bilangan ASCII kemudian dikonversikan lagi ke dalam bentuk bilangan biner. Misalkan karakter yang akan dienkripsikan adalah huruf “S: sebagai contoh. Huruf “S” diubah ke dalam bentuk ASCII (S=83) agar dapat dipecah menjadi bilangan biner. Biner dari huruf “S” adalah 1010011. Setelah mendapatkan bilangan biner dari karakter yang dimaksud maka proses enkripsi dilakukan dengan rumus :

t_i*x=∑y

dimana :
t_i = kunci publik
x = bilangan biner karakter
y = hasil perkalian

Tabel 2. Proses Enkripsi

t_i		x	x	Y
588	*	0	=	0
2	*	1	=	2
297	*	0	=	0
301	*	1	=	301
315	*	0	=	0
58	*	0	=	0
94	*	1	=	94
236	*	1	=	236
Jumlah				633

Maka hasil enkripsi yang didapatkan dari huruf S adalah 633

2.6 Proses Dekripsi

Setelah menerima pesan yang terenkripsi maka dilakukan proses dekripsi dengan menggunakan rumus :

z= y mod q

Keterangan :
z = target sum / hasil perkalian
r = kunci private
= invers dari r
y = chipertext yang diterima
q = bilangan pembagi

belum diketahui nilainya. Untuk mendapatkan nilainya dapat digunakan algoritma extended eucidian gcd (q,r) dimana :
q = bilangan pembagi
r = kunci private

Langkah dekripsi pertama akan dilakukan dengan mencari nilai (moduler invers) dengan rumus = (1+km)/a yaitu sebagai berikut:
= (1+km)/r :
= (1+881 k / 588, coba k = 0,1,2,……, maka k = 442.
Setelah nilai didapatkan maka langkah dekripsi selanjutnya adalah mengalikan

setiap kriptogram (chipertext) dengan mod q, lalu nyatakan hasil kalinya sebagai penjumlahan elemen-elemen kunci privat (w) untuk memperoleh plaintextsebagai berikut:
442 * 633 mod 881 = 234

(0*1) + (1*3) + (0*5) + (1*11) + (0*32) + (0*87) + (1*141) + (1*354) = 509
Kemudian pisahkan tanda tambah dan bilangan s_i sehingga didapatkan 1010011 berupa bilangan biner. 01010011 jika diubah ke dalam desimal adalah 83 dan karakter ASCII-nya adalah “S”. Maka deskripsi dari *chipertext* “509” adalah “S”.

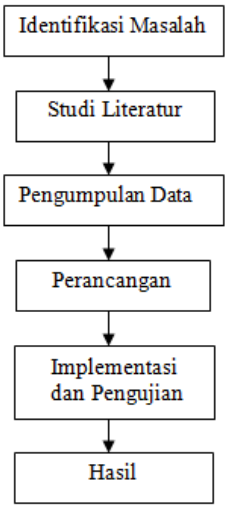
2.7 Pengertian Database

Database merupakan kumpulan informasi informasi yang disimpan didalam komputer secara sistematik sehingga dapat diperiksa menggunakan suatu proram untuk memperoleh informasi dari *basis data* tersebut.Pengertian umum dari Database adalah sistem penyimpanan data dimana data yang sudah banyak di input disiman dalam satu sistem penyimpanan. Sistem database sudah banyak digunakan dibanyak bidang, tidak hanya bidang teknologi, bahkan saat ini database sudah digunakan diperusahaan dari yang keil hingga besar, universitas, perkantoran, supermarket bahkan rumah-rumah.

METODE PENELITIAN

Metode dilakukan untuk mencari informasi secara sistematis dengan menggunakan metode ilmiah serta sumber yang jelas. Dalam proses penelitian akan memberikan gambaran rancangan penelitian untuk meningkatkan sejumlah pengetahuan yang merupakan suatu usaha yang sistematis dan terorganisasi untuk menyelidiki masalah tertentu agar mendapatkan hasil yang bemanfaat bagi para pengguna[7].

Untuk proses pembuatan penelitian ini, metode penelitian yang dilakukan adalah sebagai berikut :



Gambar 1. Alur Kerja Algoritma Merkle Hellman

PEMBAHASAN

Program aplikasi database menggunakan Algoritma Merkle Hellman ini dibangun dengan tujuan untuk menjaga keamanan pada database dengan menggunakan kunci *Asimetris* dalam proses enkripsi dan dekripsi data menjadi tidak dapat dimengerti pihak lain walaupun data tersebut telah dimiliki atau dicuri. Kelebihan dari algoritma Merkle Hellman ini adalah tidak diperlukannya kerahasiaan pada proses pendistribusian key. Hal ini dikarenakan key yang disalurkan berupa *public key*. Meskipun kunci ini diketahui oleh orang lain yang tidak berwenang, maka pesan tersebut akan tetap terjaga kerahasiaannya. Sedangkan *privat key* akan tetap disimpan atau tidak didistribusikan.

4.1. Form Menu Utama

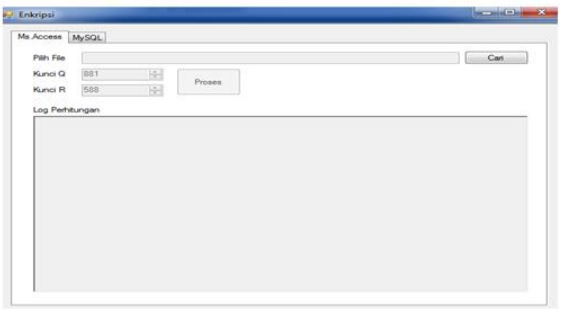
Form ini merupakan tampilan awal program untuk memilih beberapa pilihan menu pada sistem yang berjalan

Gambar 2. Form Menu Utama

4.2. Form Menu Enkripsi

Pada form enkripsi ini dimulai dari memilih file database yang akan dienkripsi dan memasukan kunci Algoritma Merkle Hellman, lalu lakukan proses enkripsi. Maka akan

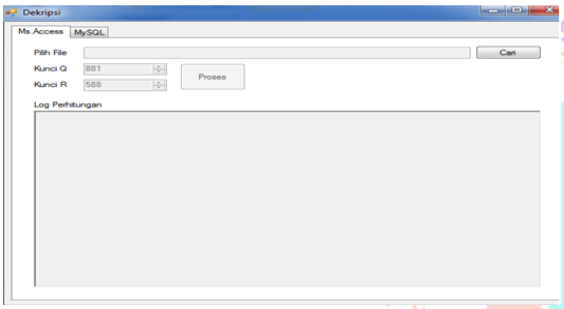
muncul proses perhitungan dekripsi pada kolom log perhitungan seperti gambar yang ada di bawah ini :



Gambar 3. Form Enkripsi

4.3. Form Menu Dekripsi

Pada form dekripsi ini dimulai dari memilih file database yang akan didekripsi dan memasukan kembali kunci Algoritma Merkle Hellman, lalu lakukan proses dekripsi. Maka akan muncul proses perhitungan dekripsi pada kolom log perhitungn sebagai berikut:



Gambar 4. Form Dekripsi

KESIMPULAN

Dari hasil pengujian, analisis, perancangan dan tahap implementasi terhadap pengkodean database yang menggunakan algoritma merkle hellman maka diambil kesimpulan sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan dengan aplikasi ini, database yang sudah di enkripsi menjadi bentuk pesan yang tidak dapat dipahami (cipherteks), namun setelah dilakukan proses dekripsi maka database berhasil kembali menjadi bentuk semula (plainteks) yang dapat dipahami denan menerapkan algoritma Merkle Hellman.
2. Kunci yang digunakan untuk mengamankan database pada saat dienkripsi akan dipakai kembali untuk proses dekripsi dengan menggunakan aplikasi Visual Basic.Net 2010

DAFTAR PUSTAKA

[1] D. Ariyus, “Kriptografi keamanan data dan komunikasi,” *Yogyakarta Graha Ilmu*, 2006.

[2] R. Munir, “Kriptografi,” *Inform. Bandung*, 2006.

[3] R. Sadikin, “Kriptografi untuk keamanan jaringan,” *Penerbit Andi, Yogyakarta*, 2012.

[4] “Kriptografi untuk keamanan jaringan dan implementasinya dalam bahasa Jawa / Rifki Sadikin,” p. 2012, 2012.

[5] A. Hidayat and R. Rosyadi, “Cryptography Asymmetries Merkle-Hellman Knapsack Digunakan untuk Enkripsi dan Dekripsi Teks,” pp. 27–28, 2016.

[6] A. F. Helmi, S. Arifianto, J. T. Informatika, and U. M. Malang, “ANALISA KOMBINASI ALGORITMA MERKLE-HELLMAN KNAPSACK DAN ANALYSIS OF A COMBINATION OF MERKLE-HELLMAN ALGORITHMS AND,” vol. 5, no. 3, pp. 325–334, 2018.

[7] T. Sutabri, *Konsep Sistem Informasi*. Penerbit Andi, 2012.