Plagiarism Checker X Originality Report

Similarity Found: 21%

Date: Monday, April 15, 2019
Statistics: 489 words Plagiarized / 2287 Total words
Remarks: Medium Plagiarism Detected - Your Document needs Selective Improvement.

ANALISA ALGORITMA MERKLE HELLMAN UNTUK KEMANAN DATABASE Magdalena Simanjuntak, Teknik Informatika magdalena.simanjuntak84@gmail.com Tioria Pasaribu, Manajemen Informatika t4y0pasaribu@yahoo.co.id Semiati Rahmadilla Sistem Informasi syemiatirahmadilla@gmail.com STMIK Kaputama Jl. Veteran No. 4A-9A, Binjai, 20714, Sumatera Utara Telp. 061-8828840, Fax.

88228845 Abstrak Perkembangan teknologi informasi saat ini membawa dampak yang sangat besar yaitu masalah keamanan dan kerahasiaan sebuah data. 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.

Masalah keamanan dan kerahasiaan database merupakan aspek terpenting dalam suatu sistem informasi. Salah satu mekanisme untuk meningkatkan keamanan database adalah dengan menggunakan algoritma asimetris seperti algoritma Merkle Hellmen. 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, yakni kunci publik dan kunci rahasia. Enkripsi menghasilkan chipertext dan dekripsi menghasilkan plaintext untuk pengamanan database yang ingin dijaga kerahasiaannya.. Kelebihan dari algoritma Merkle Hellman ini adalah tidak diperlukannya kerahasiaan pada proses pendistribusian key.

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. Kata Kunci : Kriptografi, Database, Merkle Hellman

1.

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.Salah satu mekanisme untuk meningkatkan keamanan database adalah dengan menggunakan algoritma asimetris seperti algoritma Merkle Hellmen. 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. 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 Menurut Doni Ariyus (2006). 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). 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.

Kaena 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). 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.

Langkah-langkah penjelasan Matematika sebagi berikut : 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) Untuk mengkonversikan semua karakter dari pesan ke biner. Urutan biner diwakili oleh variabel b.

Untuk memilih dua nomor integer (a) yang lebih besar dari pada jumlah semua nomor di urutan dan co-prime (r). Urutan dan nomor dan r membentuk kolektif kunci pribadi cryptosystem tersebut. 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 Semua elemen p1, p2, p3, …. pn urutan p adalah dikalika dengan unsur-unsur yang sesuai dari biner urutan b. 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 : ti= r * w mod q dimana : ti = kunci publik r = kunci rahasia w = bilangan super increasing q = bilangan pembagi Dan hitung seperti cara dibawah ini : Tabel II.1

Proses Pencarian Kunci Publik Dari tabel di atas didapatkan hasil kunci publik sebagai berikut : ti= (588,2,297,301,315,58,94,236) Untuk proses enkripsi setiap karakter siubah

kedalam bentuk bilangan ASCII kemudian dikonversikan lagi kedalam bentuk bilangan biner. Misalkan karakter yang akan dienkrisikan adalah huruf "S: sebagai contoh. Huruf "S" diubah kedalam 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 : ti*x=?y dimana : ti = kunci publik x = bilangan biner karakter y = hasil perkalian Tabel II.2

Proses Enkripsi ti _ _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=_ymodq 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 danbilangan si sehingga didapatkan 1010011berupa bilangan biner.

01010011 jika diubah ke dalam desimal adalah 83 dan karakter ASCIInya 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. 2.8 Microsoft Visual Basic. Net 2010 Menurut Kurniawan (2011, h. 2), Visual basic studio 2010 merupakan sebuah lingkungan kerja (Integrated Development Enivirontment (IDE) yang

digunakan untuk pemograman.

Net yang dapat digunakan untuk beberapa bahasa pemrograman, seperti Visual Basic (VB), C# (dibaca C Sharp), Visual C++, J# (dibaca J Sharp), F# (dibaca F Sharp), dan lain-lain. Menurut Kurniawan (2011, h. 7), Teknologi NET Framwork adalah sebuah Application Programming Languange (API), yaitu kumpulan kelas atau sebuah pustaka ini yang digunakan untuk melakukan pemrograman NET. Kelas-kelas care (inti) NET Framwork. Berbagai tool, antara lain toolbox yang berisi komponen sosial. Gambar II. 3 Tampilan Project Baru Visual Basic.Net Sumber : Kurniawan (2011, h.12) 3.1

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.

Untuk proses pembuatan penelitian ini, metode penelitian yang dilakukan adalah sebagai berikut : _ 4.1 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. 4.2 Form Menu Utama Form ini merupakan tampilan awal program untuk memilih beberapa pilihan menu pada sistem yang berjalan _4.3 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 dibawah ini : _ 4.4

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: _ 4.5 Form Tentang Aplikasi _ 5. KESIMPULAN DAN SARAN 5.1 Kesimpulan Dari hasil pengujian, analisis, perancangan dan tahap implementasi

terhadap pengkodean database yang menggunakan algoritma merkle hellman maka diambil kesimpulan sebagai berikut : 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.

Kunci yang digunakan untuk mengamankan database pada saat dienkripsi akan dipakai kembali untuk proses dekripsi dengan menggunakan aplikasi Visual Basic.Net 2010 5.2 Saran Beberapa saran yang dapat digunakan untuk tahap pengembangan penelitian ini adalah sebagai berikut : Algoritma Merkle Hellman dapat menjadi pilihan yang baik untuk membangun sistem kriptografi karena memiliki tingkat keamanan yang tinggi.

Untuk penelitian selanjutnya dapat dilakukan dengan mengkombinasikan dengan metode kriptografi yang lain agar keamanan lebih terjaga. Daftar Pustaka Ariyus, D. 2006. Computer Security. Penerbit Andi. YogyakartaAriyus, D. 2006. Kriptografi. Penerbit Graha Ilmu. Yogyakarta. Ariyus, D. 2008. Pengantar Ilmu Kriptografi. Penerbit Andi. Yogyakarta. Ariyus, D. 2006. Kriptografi Keamanan Data dan Komunkasi. Penerbit Graha Ilmu. Yokyakarta Kadir, A. 2010. Mudah Mempelajari Database Access.

Penerbit Andi. Yogyakarta Kurniawan, E. 2011. Cepat Mahir Visual basic. Penerbit. Andi Yogyakarta Ladjamudin, A. 2005..Analisis dan Desain Sistem Informasi. Penerbit Graha Ilmu, Yogyakarta Sadikin, 2012. Kriptografu untuk Keamanan Jaringan. Penerbit Andi. Yogyakarta Sutedjo, B. 2002. Perencanaan dan Pembangunan Sistem Informasi.Penerbit Andi, Yogyakarta

INTERNET SOURCES:

1% - http://header.kaputama.ac.id/lihatberita.php?id=27
1% - https://sisteminfomasi.blogspot.com/2009/10/teknik-kriptografi-untuk-pengamanan.html
3% - http://jtiik.ub.ac.id/index.php/jtiik/article/download/468/pdf
1% - https://greenvanda.blogspot.com/2012/11/keamanan-data-dari-virus.html
<1% - https://docobook.com/implementasi-kriptografi-dan-steganografi-dengan-metode.html
<1% - https://simeb.blogspot.com/2007/08/praktek-manajemen-keamanan-komputer.html
<1% - https://www.academia.edu/7612178/KEAMANAN_SISTEM_DATABASE
6% -

https://prpm.trigunadharma.ac.id/public/fileJurnal/hpPmJurnal%20Purwadi%202014.pdf
1% - https://www.academia.edu/6377708/Aplikasi_Matriks_pada_Kriptografi
1% -
http://repository.usu.ac.id/bitstream/handle/123456789/60690/Chapter%20II.pdf?sequence=4&isAllowed=y
1% - https://gokmat20.blogspot.com/2010/07/2.html
1% -
http://repository.usu.ac.id/bitstream/handle/123456789/37237/Chapter%20II.pdf;sequence=4
1% -
https://www.researchgate.net/publication/323962079_Implementasi_Kriptografi_Pengamanan_Data_Pada_Pesan_Teks_Isi_File_Dokumen_Dan_File_Dokumen_Menggunakan_Algoritma_Advanced_Encryption_Standard
1% - http://e-journals.unmul.ac.id/index.php/JIM/article/download/23/pdf
3% -
http://riset.fmipa.unpad.ac.id/data/uploads/paper/semnas/2016/014.-066-068-akik-hidayat.pdf
<1% - https://rina-aryani.blogspot.com/2011/10/tugas-keamanan-informasi.html
<1% -
https://ahmadnurfauzi007.blogspot.com/2016/08/normal-0-false-false-false-en-us-x-none.html
<1% - https://klaudiusandrisanwau.blogspot.com/2013/02/kryptografi_6931.html
1% - https://urgakun.blogspot.com/
1% - https://maeami1211.blogspot.com/2013/03/data-base-basis-data.html
<1% -
https://tantowi29.wordpress.com/2017/05/23/mari-memulai-mengenal-visual-studio-2017-community-edition/
<1% - https://www.bospedia.com/2018/05/metode-penelitian.html
<1% - https://wisatapikiran.blogspot.com/2013/09/cara-penulisan-dan-pengertian.html
<1% -
https://mudah-bahasaindonesia.blogspot.com/2016/01/contoh-kalimat-menggunakan-kata-maka.html
<1% -
https://www.scribd.com/doc/303622009/Implementasi-Blowfish-dan-Diffie-Hellman-pada-email
<1% - http://publication.gunadarma.ac.id/bitstream/123456789/1297/1/21107015.pdf
<1% - https://pageknowledge2.blogspot.com/2014/
<1% - https://santimylove.blogspot.com/feeds/posts/default
<1% - https://fajarnoverdi.blogspot.com/2013/03/keamanan-web-services.html
<1% -

https://www.academia.edu/6668625/MENGGUNAKAN_ALGORITMA_ELECTRONIC_CODE_BOOK_ECB_DAN_LEAST_SIGNIFICANT_BIT_LSB_DI_HANDPHONE
<1% - http://citec.amikom.ac.id/main/index.php/citec/article/view/10
<1% - https://reviewbukumu.blogspot.com/2017/10/katalog-buku-terbitan-dan-yang.html
1% - http://www.bukukita.com/infodetailbuku.php?idBook=2858