Times New Roman, Size = 14, 1 Spasi.

"JUDUl ARTIKEL"
"ANALISA ALGORITMA ELGAMAL DALAM PENYANDIAN DATA SEBAGAI KEAMANAN DATABASE"

Times New Roman, Size = 12, 2 Spasi.

Winda Sari[1)], Yani Maulita[2)], Achmad Fauzi[3)]

Times New Roman, Size = 12, 1 Spasi.

[123]STMIK Kaputama
Jl. Veteran No. 4A-9A, Binjai, Sumatera Utara
E-mail :fauzyrivai88@gmail.com, yassa_26@ymail.com [2]

Times New Roman, Size = 12, 1 Spasi.

ABSTRACT

The development of the world of information is now rapidly entering various fields, which seeks to utilize information technology today. Database security and confidentiality issues are one of the important aspects of an information system.

1,5 Spasi.

Keywords: Cryptography, Database File, Elgamal Algorithm

1,5 Spasi.

Abstrak : Times New Roman, Size = 12, 1 Spasi.

ABSTRAK

Perkembangan dunia informasi saat ini semakin cepat memasuki berbagai bidang, yang berusaha memanfaatkan teknologi informasi masa kini. Masalah keamanan dan kerahasiaan database merupakan salah satu aspek penting dari suatu sistem informasi.

Kata kunci: Kriptografi, File Database, Algoritma Elgamal

Masing-masing Sub-Judul Font : Time New Roman (Capital). Size : 12, cetak : Bold, 1 spasi

I. PENDAHULUAN

Salah satu perkembangan yang penting adalah semakin dibutuhkannya penggunaan alat pengolah data yang berfungsi untuk menghasilkan informasi yang dibutuhkan.dengan menggunakan alat pendukung pengolah data yaitu komputer. Dengan adanya komputer sebagai alat pengolah data, maka semua bidang dalam suatu perguruan tinggi ataupun instansi dapat dikomputerisasikan. Masalah keamanan dan kerahasiaan database merupakan salah satu aspek penting dari suatu sistem informasi. Sebuah informasi hanya ditujukan bagi pihak – pihak tertentu, hal tersebut terkait dengan bagaimana informasi tidak dapat diakses oleh orang yang tidak berhak. Pengamanan file pada database dapat dilakukan dengan

2. METODOLOGI

Dari penelitian yang dilakukan oleh Danang Tri Massandy dengan judul "Algoritma Elgamal Dalam Pengamanan Pesan Rahasia" kesimpulan dari penelitian ini adalah melakukan pengujian proses enkripsi dan dekripsi dalam pengamanan pesan rahasia. Dalam hal ini diperoleh bahwa algoritma Elgamal keamanannya terletak pada pergandaan bilangan bulat modulo prima dengan mengambil nilai bilangan prima yang besar maka upaya pemecahan pesan akan sangat sukar dan keamanan kuncinya lebih terjamin. Adapun penelitian lainnya yang berkaitan dengan algoritma Elgamal adalah suatu plainteks yang akan dienkripsi menjadi cipherteks yang berbeda – beda dikarenakan pemilihan bilangan k yang acak. Akan tetapi, walaupun cipherteks yang diperoleh berbeda – beda, pada proses dekripsi akan di peroleh plainteks yang sama.

"ISI" Font: Time New Roman , Size : 12 dan 1 Spasi.

2.1 Pengertian Kriptografi

Setiap Penurunan Sub Bab diberikan kode dalam bentuk angka

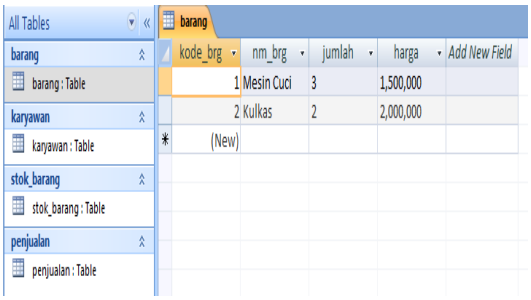
Menurut Munir (2006, h.20) Kriptografi adalah merupakan ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan,

3. HASIL DAN PEMBAHASAN

Pada proses enkripsi algoritma elgamal tersebut diasumsikan mempunyai panjang maksimal penentuan bilangan prima adalah P = 229, langkah selanjutnya melakukan analisis enkripsi file database pada Algoritma Elgamal yang bertujuan untuk merubah file asli (plaintext) ke bentuk file yang rahasia (ciphertext). Adapun urutan proses tersebut adalah :

1. Memasukkan file database/plaintext yang akan dienkripsi
   Nama file database: Penjualan Barang.accdb

Plaintext yang akan di enkripsi = **Mesin Cuci**



Fornt: Time New Roman, 12, 1 Spasi. Wajib ada analisa permasala

4. KESIMPULAN

Setelah dilakukan analisa dan implementasi pembahasan maka penelitian ini menyimpulkan beberapan yaitu :

1. Spesifikasi program aplikasi ini dapat dijalankan sesuai dengan sistem yang telah dirancang.
2. Proses enkripsi file database yang akan di enkripsi adalah isi data pada tabel (cipherteks), file database masih dapat dibuka dan dilihat akan tetapi isi data pada tabel tidak bisa dibaca, kemudian proses dekripsi untuk mengembalikan file database yang telah di enkripsi kembali menjadi file awal (plainteks).

5. SARAN

1. Pada hasil enkripsi database dapat disimpulkan daris pada table tidak dapat diproses seperti data.
2. Program aplikasi kriptografi ini dapat menyandikan sebuah file rahasia sehingga file database terjamin keamanannya.

DAFTAR PUSTAKA

[1]. Danang Tri Massandy. 2014. Algoritma Elgamal Dalam Pengamanan Pesan Rahasia. Bandung

[2]. Ariyus. Doni 2005. Computer Security. Penerbit Andi. Yogyakarta

[3]. Ariyus. Doni 2006. Kriptografi Keamanan Data Dan Komunikasi. Penerbit Graha Ilmu. Yogyakarta

[4]. Yatini Indra B. 2010 Flowchart, Algoritma Dan Pemrograman Menggunakan Bahasa C++ Builder. Penerbit Graha Ilmu. Yogyakarta

[5]. Munir, Rinaldi 2006. *Kriptografi. Informatika*, Bandung.

[6] Priyanto .Rahmat.2009 . *Langsung Bisa visual Basic.Net 2010*.Penerbit Andi. Yogyakarta

[7] Kromodimoeljo ,Sentot. 2009.*Teori Dan Aplikasi Kriptografi. Penerbit SPK IT* Consulting.

[8] Sadikin. Rifki 2012. *Kriptografi Untuk Keamanan Jaringan.Penerbit Andi*. Yogyakarta

[9]. Sugiarti Yuni S.T.M.Kom. 2013 *Analisa Dan Perancangan UML (Unified Modeling Language).* Penerbit Graha Ilmu. Yogyakarta

[10]. Fauzi Achmad dan Maulita Yani , *Analisis Hybrid Cryptosystem Algoritma Elgamal Dan Algoritma Triple Des, 2016*

"Refrensi" Font: Time New Roman , Size : 12 dan 1 Spasi.

Minimal Isi Artikel 7 Halaman