IMPLEMENTASI ALGORITMA *ADVANCED ENCRYPTION STANDARD*-128 (AES-128) UNTUK PENGAMANAN *DATABASE* BERBASIS DESKTOP PADA ICALTOYS

Tritera Erlangga[1)], **Dewi Kusumaningsih**[2)]
Program studi, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : [1)]tritera.erlangga@gmail.com, [2)]Dewi.kusumaningsih@budiluhur.ac.id

Abstrak

Pesatnya perkembangan teknologi informasi menyebabkan keamanan data membutuhkan keamanan yang cukup baik. Sekarang, hampir semua orang dapat dengan mudah bertukar informasi dalam hal apapun, bahkan melakukan akses data secara ilegal pun merupakan hal yang sangat mungkin untuk dilakukan. Mengingat Icaltoys adalah usaha dagang yang bergerak dibidang penjualan dan pelelangan secara online, membuat data-data di dalamnya menjadi rentan untuk diretas. Data transaksi dan data pribadi pelanggan adalah data yang bersifat privasi, maka data tersebut haruslah terjaga kerahasiaannya. Orang jahat selalu mencari cara untuk mengakses data tersebut dengan cara mengakses secara langsung pada tabel database. Dengan kemungkinan akan akses langsung pada tabel database secara ilegal, maka diperlukanlah keamanan yang lebih baik untuk database Icaltoys. Dengan masalah yang ada, maka dapat diambil tujuan dari pada pembuatan aplikasi ini yaitu mengamankan dan menjaga kerahasiaan data dari orang-orang yang tak memiliki hak akses. Dalam hal ini penulis menggunakan cara dengan mengenkripsi database dengan algoritma Advanced Encryption Standard (AES-128) yang mampu meningkatkan tingkat keamanan data dan tetap menjaga kerahasiaannya. Dengan enkripsi tersebut, user yang tidak berkewenangan hanya akan melihat data yang sudah terenkripsi.

Kata kunci: *Database*, Enkripsi, Kriptografi, *Desktop*

1. PENDAHULUAN

1.1 Latar Belakang

Pesatnya perkembangan teknologi informasi menyebabkan data membutuhkan keamanan yang cukup baik. Sekarang, hampir semua orang dapat dengan mudah bertukar informasi dalam hal apapun termasuk diataranya adalah berbagi pengetahuan untuk mengakses data secara ilegal. Data yang seharusnya bersifat rahasia menjadi rentan untuk dicuri ataupun diakses oleh orang yang tak bertanggung jawab. Orang jahat selalu mencari cara untuk mengakses data tersebut, salah satunya dengan cara mengakses secara langsung pada tabel *database*. Dengan adanya kemungkinan akan akses ilegal pada *database*, keamanan yang lebih baik terhadap *database* menjadi dibutuhkan.

Icaltoys adalah sebuah usaha dagang yang bergerak di bidang penjualan dan pelelangan mainan koleksi/hobi seperti *diecast* hingga CD music secara online menggunakan media social www.facebook.com/icaltoysfp. Usaha dagang ini berdiri sejak tahun 2007 dan baru memiliki karyawan di tahun 2012, pada saat itu jumlah karyawannya hanya 2 orang, hingga saat ini total karyawan di Icaltoys berjunlah 12 orang. Icaltoys saat ini hanya memiliki 1 kantor yang berlokasi di Jl. Mertilang XI Blok KB 2 No 4, Bintaro Sektor 9, Tangerang Selatan. Seluruh data pelanggan dan transaksi tersimpan kedalam *database*, tetapi karena data yang masuk tidak berubah dengan teks-teks yang ditampilkan, membuat isi dari data tersebut menjadi riskan terhadap orang lain yang tidak bertanggung jawab untuk dapat mengetahui secara langsung isi dari *database* tersebut untuk melakukan pembocoran data. Bocornya data pernah terjadi pada Icaltoys hingga menyebabkan kerugian yang tidak sedikit. Banyak data pelanggan yang di curi oleh pihak yang tidak bertanggung jawab dan melakukan penipuan dengan mengatas namakan Icaltoys sehingga banyak pelanggan yang mempertanyakan kemanan data diri mereka yang berdampak pada penurunan minat pelanggan untuk mengikuti lelang lagi. Oleh karena itu, dikembangkan suatu ilmu yang mempelajari tentang cara-cara pengamanan data atau informasi. Pengamanan data atau informasi dapat dilakukan dengan menggunakan teknik enkripsi terhadap data atau informasi sehingga sulit untuk dibaca atau diterjemahkan yang dapat disebut juga dengan sebutan kriptografi. Kriptografi bertujuan agar data atau informasi yang diinputkan tidak diketahui oleh orang lain yang berkaitan dengan hal diatas. Demi menjaga kerahasiaannya, maka pada penelitian ini penulis membuat perancangan aplikasi untuk pengamanan *database* berbasis desktop dengan menggunakan algoritma kriptografi AES-128 untuk mengamankan data pada Icaltoys agar orang yang tidak mempunyai hak akses atau tidak berkepentingan tidak dapat membaca isi datanya. Data yang diinput kedalam *database*, akan melalui proses enkripsi dan didekripsi ketika user yang telah diberi hak akses ingin membacanya.

Agar tidak keluar dari pembahasan, maka diberikan beberapa batasan masalah sebagai berikut:

a. Aplikasi ini hanya digunakan untuk pengamanan *database* pada Icaltoys.

b. Pembuatan perangkat lunak menggunakan bahasa pemrograman java berbasis desktop.
c. Algoritma enkripsi yang digunakan adalah AES-128.

Dalam penelitian ini, penulis menggunakan metode pengembangan dengan model *Software Development Life Cycle* atau SDLC yaitu model *waterfall* untuk pengumpulan data dan untuk mempermudah analisa dan perancangan aplikasi.

2. LANDASAN TEORI

2.1. Keamanan Data

Keamanan merupakan komponen yang sangat krusial pada komunikasi data elektronis. Banyak yang masih belum menyadari bahwa keamanan (*security*) adalah sebuah komponen penting yang tidaklah murah. Bagi para perancang dan pengelola sistem informasi, masalah keamanan sering tidak diperdulikan, bahkan ditiadakan.

Keamanan dan kerahasiaan *database* adalah salah satu aspek yang penting dari sebuah sistem informasi. Suatu informasi hanya dapat ditujukan untuk golongan tertentu saja, hal tersebut berkaitan dengan bagaimana informasi tidak boleh diakses oleh orang yang tidak mempunyai hak akses. Oleh karena itu sangat penting untuk mencegah jatuhnya informasi kepada pihak-pihak lain yang tidak berkepentingan [1].

2.2. Basis Data

Basis data merupakan sebuah koleksi atau kumpulan data yang tahan lama yang digunakan untuk sistem aplikasi dari perusahaan tertentu. Perusahaan hanya istilah yang memudahkan untuk organisasi yang cukup komersial, ilmiah, teknis, atau lainnya. Terdapat juga sumber lain yang menyatakan bahwa basis data merupakan media yang menyimpan data agar dapat di akses dengan mudah dan cepat. Dapat disimpulkan bahwa basis data merupakan kumpulan informasi yang disimpan dalam sebuah media supaya dapat diakses dengan mudah dan cepat, serta tahan lama dan digunakan oleh sistem aplikasi dalam sebuah perusahaan tertentu [2].

2.3. Kriptografi

Kriptografi merupakan kata yang berasal dari bahasa Yunani yaitu *kriptos* yang berarti tersembunyi dan *graphia* yang berarti sesuatu yang tertulis, sehingga kriptografi dapat diartikan sebagai sesuatu yang tertulis secara tersembunyi[3].

Kriptografi adalah suatu bidang ilmu yang mempelajari tentang cara menyembunyikan atau merahasiakan suatu informasi ke dalam suatu bentuk yang tidak dapat dibaca ataupun dimengerti oleh siapapun serta mengembalikannya kembali kedalam bentuk informasi semula dengan menggunakan teknik-teknik yang telah ada sehingga data atau informasi tersebut tidak dapat diketahui dengan mudah oleh pihak manapun yang tidak mempunyai hak akses atau yang tidak berkepentingan. Salah satu cabang lain dari kriptografi adalah kriptanalisis (*Cryptanalysis*) yaitu studi tentang cara memecahkan mekanisme kriptografi.

2.4. *Advanced Encryption Standard*-128 (AES-128)

Pada tahun 1997, NIST mengeluarkan AES (*Advanced Encryption Standard)* untuk menggantikan DES (*Data Encryption Standard)*. AES dibuat bertujuan untuk mengamankan berbagai bidang di sektor pemerintahan. Algoritma AES haruslah mendukung 3 ukuran kunci, yaitu kunci 128 bit, 192 bit, dan 256 bit.

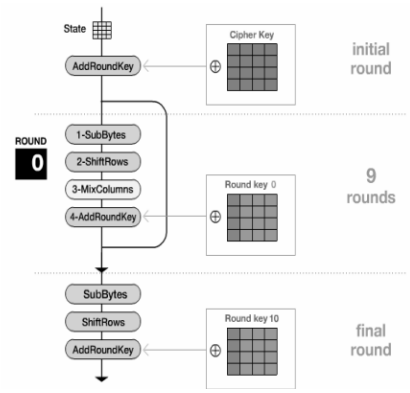
Kemudian pada Agustus 1998, NIST mengumumkan ada 15 proposal AES yang telah dievaluasi dan diterima, yang kemudian dilakukan proses seleksi terhadap algoritma yang masuk, lalu pada tahun 1999 NIST mengumumkan hanya ada 5 algoritma yang diterima, algoritma tersebut adalah: MARS, RC6, Rijndael, Serpent, dan Twofish.

Algoritma-algoritma tersebut menjalani berbagai macam pengetesan. Pada bulan oktober 2000, NIST mengumumkan bahwa Rijndael sebagai algoritma yang terpilih untuk standar AES yang baru [4].

2.5. Proses Enkripsi AES

Enkripsi adalah proses mengubah suatu pesan asli (plaintext) menjadi suatu pesan dalam bahasa sandi (*ciphertext*) [4]. Secara umum, proses enkripsi algoritma AES mempunyai beberapa tahapan, yaitu:

1) AddRoundKey: yaitu, proses melakukan X-OR (*Exclusive Or*) antara state awal (*plaintext*) dan *cipherkey*. Tahap ini disebut juga dengan *initial round*.
2) *Round*: yaitu, putaran sebanyak NR – 1 kali. Pada setiap putaran atau ronde memiliki beberapa proses, diantaranya adalah:
   a) SubBytes: yaitu, mensubstitusikan byte dengan menggunakan tabel S-Box (tabel substitusi).
   b) Shiftrows: yaitu, melakukan pergeseran tiap baris array state secara *wrapping*.
   c) MixColumns: yaitu, mengacak data pada tiap kolom array state.
   d) AddRoundKey: yaitu, melakukan X-OR antara hasil state sekarang dengan kunci hasil proses *expand key*.
3) *Final Round*: yaitu, proses untuk putaran atau ronde terakhir:
   a) SubBytes
   b) Shiftrows
   c) AddRoundKey



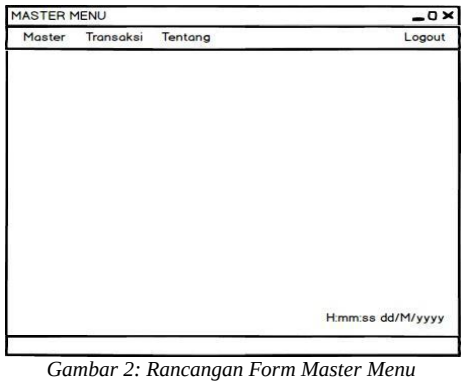
Gambar 1: Algoritma Enkripsi AES-128

3. RANCANGAN SISTEM DAN APLIKASI

3.1. Rancangan Layar Aplikasi

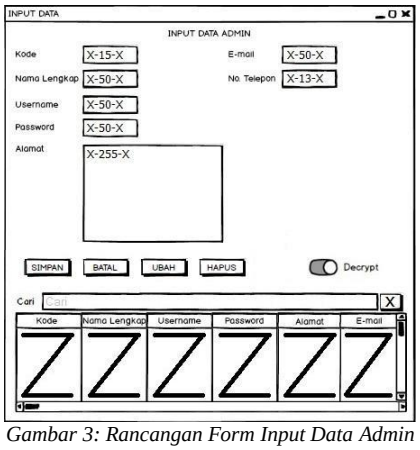
Sistem aplikasi pengamanan data ini dijalankan pada sebuah komputer yang akan dihubungkan dengan *database* kantor. lalu *admin* ketika aplikasi ini pertama kali di jalankan, menu yang pertama kali muncul adalah *form login*, setelah itu, masuk ke menu utama. Di dalam menu utama terdapat 3 menu utama, yaitu menu master, menu transaksi dan menu tentang. Di dalam menu master, terdapat 4 sub menu, yaitu submenu input data *admin*, input data barang, input data *customer*, dan log aktivitas. Pada menu transaksi terdapat 1 submenu yaitu submenu input transaksi lelang, dan pada menu tentang untuk mengetahui informasi dari penulis.

Admin kemudian akan meng-input data-data seperti data *customer* dan barang yang telah diberikan kedalam *database* komputer. Lalu *admin* memasukan semua nama pemenang lelang pada *form* transaksi lelang. Semua data yang masuk ke dalam *database* akan melalui proses enkripsi sehingga data tidak mudah dibaca jika dibuka secara langsung.



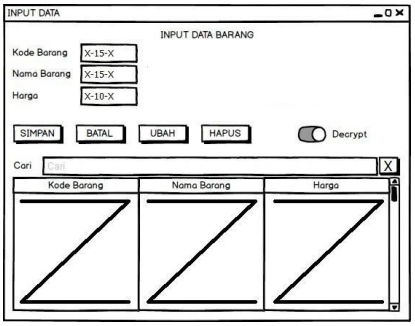
Gambar 2: Rancangan Form Master Menu

Pada Gambar 3 merupakan rancangan *Form* Input Data *Admin*. Di *form* ini lah, *admin* dapat menambahkan *admin* baru.



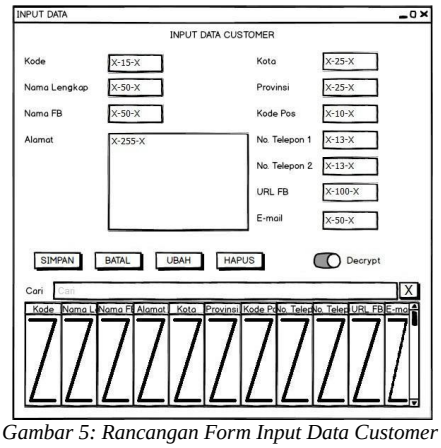
Gambar 3: Rancangan Form Input Data Admin

Pada gambar 4 merupakan rancangan *form* input data barang. Di *form* ini, *admin* menginput data-data barang yang dilelangkan.



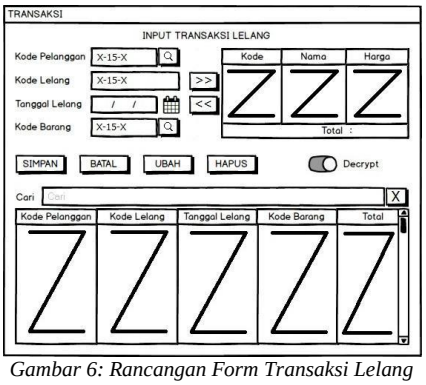
Gambar 4: Rancangan Form Input Data Barang

Pada gambar 5 merupakan rancangan *form* input data *customer*. Di *form* ini, *admin* menginput data-data *customer* yang mengikuti lelang.



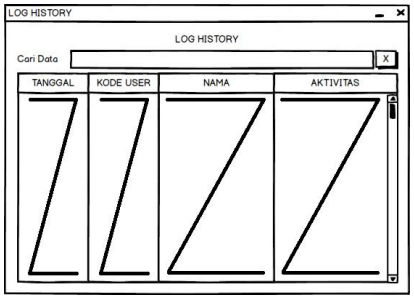
Gambar 5: Rancangan Form Input Data Customer

Pada gambar 6 merupakan rancangan *form* transaksi lelang. Di *form* ini, *admin* menginput data-data pemenang lelang beserta barang yang dimenangkannya.



Gambar 6: Rancangan Form Transaksi Lelang

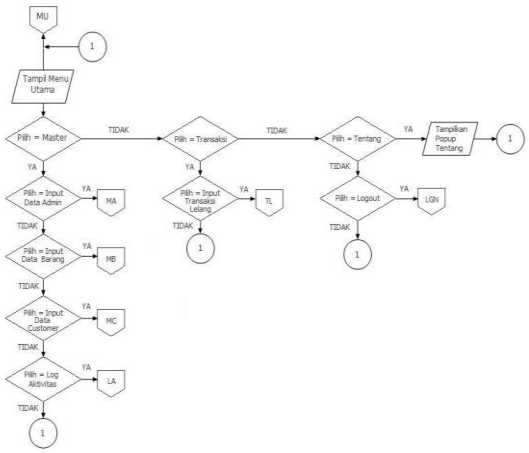
Dan yang terakhir merupakan rancangan *form* log history/log aktivitas. *Form* ini hanya dapat diakses oleh super *admin*. Fungsi *form* ini untuk mencatat aktivitas log in dan log out *admin*.



Gambar 7: Rancangan Form Log History

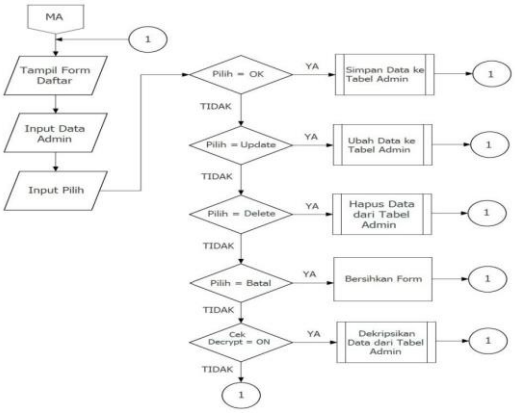
3.2. *Flowchart*

Pada bagian ini akan menjelaskan urutan-urutan proses yang digambarkan melalui bentuk *flowchart*. Berikut adalah gambaran *flowchart* dari *form* menu utama.



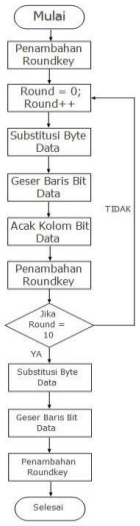
Gambar 8: Flowchart Form Master Menu

Lalu pada gambar 9 merupakan gambaran alur proses dari *form* input data *admin.*



Gambar 9: Flowchart Form Input Data Admin

Pada gambar 10 merupakan gambaran alur apa saja yang terjadi pada proses pengubahan plaintext ke *ciphertext* (enkripsi) pada AES-128.



Gambar 10: Flowchart Proses Enkripsi AES-128

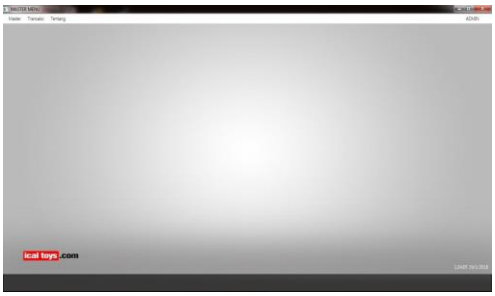
Pada gambar 11 merupakan gambaran alur apa saja yang terjadi pada proses pengubahan *ciphertext* ke plaintext (dekripsi) pada AES-128.

Gambar 11: Flowchart Proses Dekripsi AES-128

4. HASIL PENGUJIAN DAN PEMBAHASAN

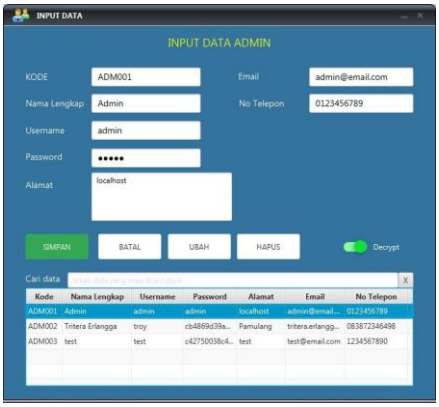
4.1. Tampilan Layar

Tampilan pertama yang akan muncul saat user/*admin* berhasil *login* adalah master menu. Pada gambar 12 merupakan tampilan layar master menu.



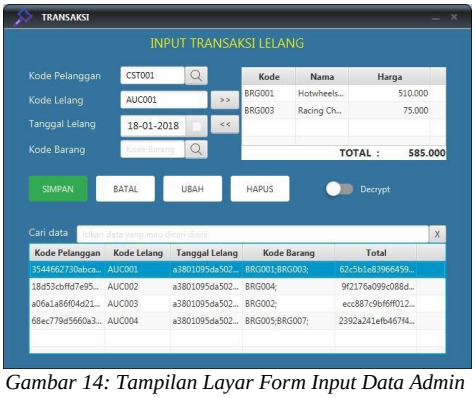
Gambar 12: Tampilan Layar Form Master Menu

Pada gambar 13 merupakan tampilan layar dari *form* input data *admin*.



Gambar 13: Tampilan Layar Form Input Data Admin

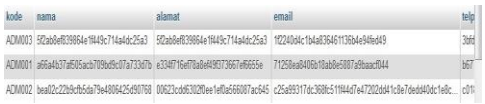
Gambar 14 merupakan tampilan layar dari *form* transaksi lelang.



Gambar 14: Tampilan Layar Form Input Data Admin

4.2. Pengujian aplikasi

Hasil uji coba proses enkripsi *database* pada tabel *admin* dapat dilihat pada gambar 15.



Gambar 15: Tampilan Isi Database Tabel Admin Setelah Proses Enkripsi

Untuk hasil uji coba dekripsi *database* untuk tabel *admin* dapat dilihat pada gambar 16.

Kode	Nama Lengkap	Username	Password	Alamat	Email	No Telepon
ADM001	Admin	admin	admin	localhost	admin@email....	0123456789
ADM002	Tritera Erlangga	troy	cb4869d39a...	Pamulang	tritera.erlangg...	083872346498
ADM003	test	test	c42750038c4...	test	test@email.com	1234567890

Gambar 16: Tampilan Isi Database Tabel Admin Setelah Proses Dekripsi

5. KESIMPULAN

Berdasarkan dari pembahasan dan pengujian diatas, maka dapat diambil kesimpulannya sebagai berikut:

a. Enkripsi AES dapat diimplementasikan untuk mengamankan *database* dengan cara mengenkripsi data-data yang masuk kedalamnya.
b. Orang yang tak mempunyai hak akses tidak dapat membaca atau mengetahui isi dari *database*.
c. Enkripsi ini mampu meningkatkan keamanan data.

Adapun beberapa saran berdasarkan hasil perancangan aplikasi diatas dapat dilakukan pengembangan, antara lain:

a. Disarankan untuk menambahkan proses kompresi untuk mengurangi ukuran data hasil enkripsi.
b. Untuk memproses data yang besar, disarankan menggunakan komputer dengan spesifikasi lebih untuk mempercepat proses enkripsi dan dekripsi.
c. *Key* dari aplikasi enkripsi ini bersifat fixed, diharapkan kedepannya input *key* dapat di-input oleh user.

6. DAFTAR PUSTAKA

[1] Santosa, E. D., 2015., Implementasi Algoritma Caesar *Cipher* dan Hill *Cipher* Pada *Database* Sistem Inventori Tb Mita Jepara.

[2] Puspitaningrum, D. A., & Susanto, A., n.d., IMPLEMENTASI ALGORITMA VIGENERE , CAESAR, DAN AFFINE *CIPHER* PADA *DATABASE* SISTEM INVENTORI TOKO WIWIN ELEKTRONIK GROBOGAN.

[3] Bahri, S., & Ps, S. D., 2012. MENGGUNAKAN METODE ENKRIPSI MD5 (Message-Digest Algorihm 5)., *Jurnal Ilmiah*, 5(5), 1–15.

[4] Murdowo, S., 2014., Mengenal Proses Perhitungan Enkripsi Menggunakan Algoritma Kriptografi Advance Encryption Standard (Aes) Rijdnael. *INFOKAM* Nomor I / Th. X/ Maret / 14, 10, 32–40.