# IMPLEMENTASI KEAMANAN DATABASE MENGGUNAKAN ALGORITMA AES-192 PADA PT GURITA LINTAS SAMUDERA BERBASIS ANDROID

**Denis Arya Saputra**[1], **Dewi Kusumaningsih**[2]
Teknik Informatika, Fakultas Teknologi Informasi, Universitas Budi Luhur
Jl. Raya Ciledug, Petukangan Utara, Kebayoran Lama, Jakarta Selatan 12260
E-mail : dennisarya01@gmail.com[1], dewi.kusumaningsih@budiluhur.ac.id[2]

***Abstrak***

*Dokumen merupakan sumber informasi yang diperlukan oleh suatu organisasi. Tanpa dokumen kita akan kehilangan data yang diperlukan untuk kegiatan organisasi atau perusahaan. Dokumen-dokumen tersebut berupa teks. Seiring dengan perkembangan teknologi saat ini yang semakin maju, keamanan menjadi sangat penting pada PT Gurita Lintas Samudera untuk menghindari tindak pencurian informasi data oleh pihak yang tidak bertanggung jawab. Salah satu caranya dengan memanfaatkan teknologi kriptografi dengan menggunakan metode Algoritma Advanced Encryption Standard (AES) 192 bit berbasis Android. Teknik Kriptografi merupakan ilmu dan seni untuk menjaga pesan dengan cara mengubahnya menjadi bentuk yang tidak dapat dikenali oleh manusia. Maka dari itu dipilihlah teknik kriptografi karna diharapkan dengan algoritma AES-192 proses enkripsi-dekripsi data dapat dilakukan dengan lebih cepat dan aman untuk menjaga kerahasiaan informasi atau data tersebut.*

**Kata kunci :** Advanced Encryption Standard (AES) 192, AES-192, Kriptografi, enkripsi-dekripsi.

## 1. PENDAHULUAN

Dalam era modern perkembangan teknologi komputer dan telekomunikasi yang semakin pesat, telah merubah segala aspek kehidupan. Kemampuan untuk menyajikan data secara cepat dan tepat itu diperlukan bagi sebuah organisasi, baik yang berupa organisasi Perusahaan, perguruan tinggi dan lembaga pemerintahan. Keamanan dan kerahasiaan sebuah data merupakan hal yang harus diperhatikan, sebab data yang bersifat rahasia perlu memiliki sistem penyimpanan agar tidak mudah terbaca oleh individu maupun golongan yang tidak bertanggung jawab. Untuk menyimpan data tersebut agar benar-benar aman, tentunya dilakukan sistem informasi pengamanan yang baik, yang bebas dari cakupan orang-orang yang tidak memiliki hak, baik bebas dari cakupan secara fisik dan secara sistem. PT Gurita Lintas Samudera adalah perusahaan swasta bergerak dalam bidang pelayaran yang beralamat di jl. Tomang raya no 47-e grogol , jakarta barat berdiri sejak 1980. Setelah dilakukan sedikit penelusuran dibagian Logistik, Pengelolaan data di komputer salah satu karyawan tergolong masih kurang aman yaitu menyimpan file dalam folder tanpa pengamanan. Dengan begitu timbulnya resiko pencurian dan hilangnya informasi data tersebut yang akan merugikan perusahaan. Dilandasi persoalan tersebut maka penulis merancang aplikasi pengamanan database menggunakan teknik kriptografi AES 192 (Advanced Encryption Standart) Berbasis Android di PT Gurita Lintas Samudera untuk memudahkan penyimpanan data dan memberi cadangan data bila terjadinya hal yang tidak dinginginkan. Dalam penerapan aplikasi ini informasi data yang sudah masuk pada database server sudah dalam kondisi terenkripsi. Enkripsi adalah salah satu teknik yang baik untuk menjaga kerahasiaan suatu data dalam berkomunikasi jarak jauh. Dengan enkripsi membuat informasi / data tidak dapat terbaca oleh orang yang tidak berhak, isinya berupa sandi acak (chipertext) dan apabila informasi data dipanggil kembali data sudah dalam kondisi terdekripsi. Dekripsi adalah pengolahan data menjadi kata yang jelas dan dimengerti oleh manusia (plaintext).

Metode yang digunakan dalam penelitian ini adalah dengan melakukan metode penelitian kepustakaan, wawancara dan observasi di PT Gurita Lintas Samudera. Pada metode pengembangan sistem yang digunakan adalah dengan tahap antara lain analisis, desain, implementasi dan perawatan.

## 2. METODE PENELITIAN

### 2.1 Algoritma Advanced Encryption Standard

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang dapat pakai untuk mengamankan suatu informasi data[1]. Algoritma kriptografi tersebut masih tergolong baru dan untuk menemukannya, National Institute of Standard and Technology mengadakan kompetisi terbuka. Dalam kompetisi itu pihak National Institute of Standard and Technology mengizinkan semua orang dalam berbagai penjuru dunia

mengajukan algoritma kriptogafi yang baru untuk menggantikan algoritma yang sebelumnya yaitu algoritma kriptografi Data Encryption Standard(DES)[2].

### 2.2 Perbandingan 3 Blok Chiper AES-128, AES-192 dan AES-256

Standar enkripsi dengan kunci simetris yang diadopsi oleh pemerintah Amerika Serikat terdiri atas 3 blokcipher, yaitu AES-128, AES-192 dan AES-256, yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai Rijndael. Masing-masing cipher memiliki ukuran 128-bit, dengan ukuran kunci masing-masing 128, 192 dan 256 bit. AES telah dianalisis secara luas dan sekarang digunakan di seluruh dunia, seperti halnya dengan pendahulunya, Data Encryption Standard (DES). Setiap 3 blok chiper pada AES-128, AES-192 dan AES-256 mempunyai perbedaan pada jumlah key dan jumlah putaran sebagai berikut[3].

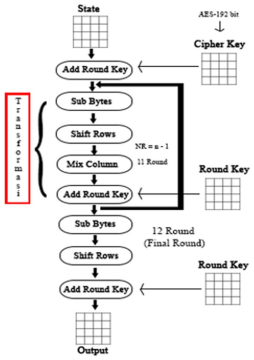
Tabel 1 : Perbandingan Jumlah Round dan Key pada Tipe AES[4]

| Tipe | Panjang Kunci | Panjang Blok Input | Jumlah Putaran |
|---|---|---|---|
| AES-128 | 4 | 4 | 10 |
| AES-192 | 6 | 4 | 12 |
| AES-256 | 8 | 4 | 14 |

Pada dasarnya, operasi Advanced Encryption Standard (AES) dilakukan terhadap Array Of Byte dua dimensi yang disebut State. *State* Mempunyai ukuran NROWS x NCOLS. Pada awal enkripsi, data masuk yang berupa in0, in2, in4, in5, in6, in7, in8, in9, in10, in11, in12, in13, in14, in15 disalin ke dalam *Array State*. *State* inilah yang nantinya dilakukan proses enkripsi dan dekripsi. Kemudian keluarannya akan ditampung ke dalam Array Out[4].


*Gambar 1 : Proses Input Bytes, State Array, dan Output Bytes pada AES*

### 2.3 Proses Enkripsi Advanced Encryption Standard 192




*Gambar 2 : Proses Enkripsi AES-192*

1) AddRoundKey

AddRoundKey adalah Mengkobinasikan sebuah Chiperkey dan State dengan menggunakan operator XOR.

2) Sub Bytes

Sub Bytes adalah menukar isi matriks yang sudah melalukan proses XOR dengan baris dan kolom pada tabel S-Box.

3) Shift Rows

Shift Rows adalah proses melakukan pergeseran pada setiap blok/table elemen yang digunakan per barisnya. Baris pertama tidak melakukan pergeseran, baris kedua melakukan pergeseran 1 byte, baris ketiga melakukan pergeseran 2 byte dan baris ke-empat melakukan pergeseran 3 bytes.

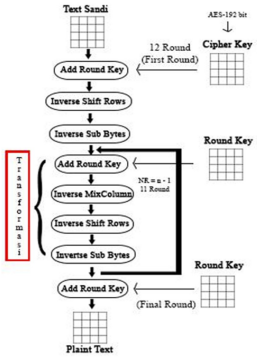
4) MixColumns

Mix Columns adalah mengalikan tiap elemen dari Blok Chiper dengan matriks yang sudah ditentukan.

5) Add Round Key

Add Round Key adalah kombinasikan Chiperteks yang sudah ada dengan Chiperkey dihubungkan pada operator XOR.

### 2.4 Proses Dekripsi Advanced Encryption Standard 192




*Gambar 3 : Proses Dekripsi AES-192*

1) InvMixColumns

InvMixColumns adalah setiap kolom dalam state dikalikan dengan matriks yang sudah ditentukan pada perkalian dalam AES-192.

2) InvShiftRows

InvShiftRows adalah transformasi byte yang berkebalikan dengan transformasi ShiftRows. Pada transformasi InvShiftRows, dilakukan pergeseran bit ke kiri.

3) InvSubBytes

InvSubBytes juga merupakan transformasi bytes yang berkebalikan dengan transformasi SubBytes. Pada InvSubBytes, tiap elemen pada state dipetakan dengan menggunakan table Inverse S-Box.

4) Invers AddRoundKey

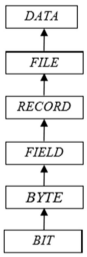
Invers AddRoundKey adalah mengkombinasikan chiperteks yang sudah ada dengan chiperkey dihubungkan pada operator XOR.

### 2.5 Database

Mengapa dibutuhkan Database dalam penggunaan Komputer :

1. Karena merupakan dasar dalam menyediakan sebuah informasi.
2. Akurat, tepat waktu dan relevan.
3. Mengurangi terjadinya duplikasi data.
4. Data yang berhubungan dapat ditingkatkan.
5. Menghemat tempat penyimpanan luar.

Data didalam database memiliki suatu susunan berbentu suatu hirarki, dapat dilihat sebagai berikut[5].




*Gambar 4 : Hirarki Data dalam Database*

## 3. RANCANGAN SISTEM DAN APLIKASI

### 3.1 Rancangan Layar Sistem

Pada sub bab rancangan layar sistem ini akan dijelaskan 2 rancangan layar dari sistem yang menjadi inti dari alur proses *enkripsi* dan *dekripsi.* Rancangan layar pada *enkripsi.*


*Gambar 5 : Rancangan Layar Enkripsi*

Rancangan layar pada gambar 4 merupakan rancangan layar form enkripsi pengguna dapat melakukan entry data ketika disimpan proses enkripsi berjalan dan data langsung masuk ke dalam database, pengeditan data yang sudah di enkripsi serta penghapusan data yang sudah di enkripsi menggunakan AES-192 pada form ini.

Setelah penjelasan dari rancangan layar porses *enkripsi.* berikut adalah gambar dari rancangan layar *dekripsi*.


*Gambar 6 : Rancangan Layar Dekripsi*

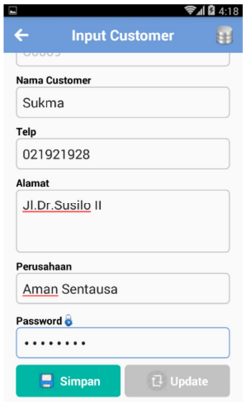
Rancangan Layar pada gambar 5 merupakan rancangan layar form dekripsi untuk melakukan pencarian data yang di enkripsi apa bila ingin di dekripsi tekan tombol pojok kanan lalu akan muncul pop up password setelah dimasukan password maka semua data akan tampil di form ini.

## 4. HASIL DAN PEMBAHASAN

### 4.1 Tampilan Layar

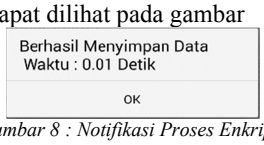
Pada bab ini akan membahas mengenai implementasi dan uji coba dari sistem yang akan dibuat. Bab ini akan menjelaskan tentang

hasil dari proses enkripsi dan dekripsi berdasarkan uji yang telah disiapkan dengan berbagai uji coba entry data pada algoritma kriptografi AES-192. Pada bab ini juga akan membuat suatu evaluasi dari pengujian program tersebut. Evaluasi tersebut bertujuan agar selanjutnya progam ini akan dikembangkan kembali menjadi lebih baik lagi dan lebih berguna bagi yang menggunakan atau user. Berikut ini adalah form untuk input data setelah di simpan akan mengalami proses enkripsi.



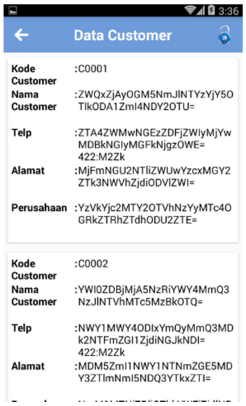

*Gambar 7 : Form Enkripsi*

Maka akan muncul notifikasi proses enkripsi berhasil. Dapat dilihat pada gambar



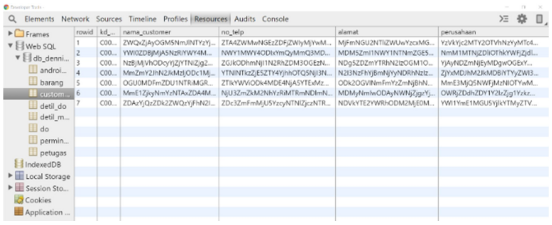

*Gambar 8 : Notifikasi Proses Enkripsi*

Berikutnya untuk melihat hasil dari proses enkripsi tadi, user dapat mengklik button tampil data, setelah itu semua data yang terenkripsi akan tampil.



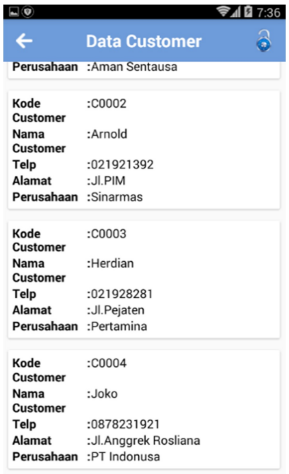

*Gambar 9 : Form Tampil Data Enkripsi*

Berikut ini memperlihatkan tampilan data yang disimpan di dalam database.



*Gambar 10 : Data didatabase*

Berikut ini adalah tampil data yang sudah terdekripsi




*Gambar 11 : Form Tampil Data Dekripsi*

Hasil pengujian diatas pada saat selesai melakukan *enkripsi*. Dapat ditraik kesimpulan bahwa tidak terjadi perubahan *data* yang di*dekripsi*. Sehingga *data* tersebut sama seperti aslinya.

## 5. KESIMPULAN

Sesuai dengan pembahasan mengenai Aplikasi Implementasi Keamanan Database Menggunakan Algoritma Kriptografi Advanced Encryption Standard (AES-192) Berbasis Android, maka kesimpulan yang dapat diambil adalah sebagai berikut :

a. Dengan adanya aplikasi pengamanan database menggunakan algoritma Advanced Encryption Standard (AES) 192 bit ini dapat mengamankan data atau informasi yang ada di PT Gurita Lintas Samudera dapat terjaga kerahasiaan datanya dari orang yang tidak bertanggung jawab.
b. Aplikasi ini dapat mengembalikan data yang sudah diamankan menggunakan metode algoritma Advanced Encryption Standard (AES) 192 bit tanpa mengalami perubahan sedikitpun.
c. Dibuatnya menu bantuan di dalam aplikasi agar karyawan dapat dengan mudah menggunakan aplikasi.

Penelitian ini masih jauh dari sempurna dan masih perlu banyak perbaikan dan pengembangan supaya menjadi lebih baik Berikut ini saran untuk pengembangan dari penelitian ini :

a. Aplikasi ini diharapkan dapat ditingkatkan sehingga data yang ingin dienkripsi tidak hanya plaintext namun dapat dalam bentuk gambar pada database.
b. Aplikasi ini hanya dapat melakukan input password satu kali, maka dari itu untuk kedepannya perlu dikembangkan untuk dapat input password lebih dari satu kali dengan password yang berbeda-beda.
c. Pengembangan lebih lanjut dapat di tingkatkan kinerjanya sehingga hasil data yang dienkripsi didatabase jumlah karakternya tidak terlalu panjang.
d. Aplikasi ini diharapkan dapat menggunakan client server untuk kedepannya.

## 6. DAFTAR PUSTAKA

[1] Munir, R., (2004). AES. Advanced Encryption Standard (AES). Departemen Teknik Informatika, Institut Teknologi Bandung, 13.

[2] Tullah, R., Dzulhaq, M. I. and Setiawan, Y. (2016). Perancangan Aplikasi Kriptografi File Dengan Metode Algoritma Advanced Encryption Standard ( AES ), 6(2).

[3] Ridwan, M. K. (2016). Aplikasi Keamanan Dokumen Digital Menggunakan Algoritma Steganografi Discrete Cosine Transform (DCT) dan Algoritma Kriptografi Advanced Encryption Standard (AES-192) Berbasis Java Desktop pada PT. Hexindo Adiperkasa Tbk.

[4] Primartha, R. (2013). Penerapan Enkripsi dan Dekripsi File menggunakan Algoritma Advanced Encryption Standard (AES). Journal of Research in Computer Science and Applications, 2(1), pp. 13–18. doi: 2301-8488.

[5] Hasrul, H. and Siregar, L. H. (2016) 'Peneraan Teknik Kriptografi Pada Database Menggunakan Algoritma One Time Pad', 2(2), pp. 41–52.