ISBN: 978-602-74635-1-6

# PENERAPAN ALGORITMA AES DALAM UNTUK KEAMANAN DATA (STUDI KASUS : CV. RANGER RELOAD)

**Achmad Udin Zailani [1], Kholid Alwan[2]**
*Teknik Universitas Pamulang*
*Jl. Surya Kencana No. 1, Pamulang, Tangerang Selatan, Indonesia*
*E-mail: dosen00370@Unpam.ac.id[1], kholid_A@gmail.com[2]*

**Abstrak –** Kriptografi merupakan bidang pengetahuan yang menggunakan persamaan matematis untuk melakukan proses enkripsi maupun deskripsi. Teknik ini digunakan untuk mengkonversi data kedalam bentuk kode-kode tertentu, untuk tujuan agar informasi yang tersimpan tidak dapat terbaca oleh siapa pun kecuali orang-orang yang berhak dalam suatu perusahaan. Oleh karena itu sangat diperlukan sebuah sistem keamana data untuk menjaga kerahasiaan informasi agar tetap terjaga, salah satunya adalah metode algoritma simetris, karena algoritma ini menggunakan kunci yang sama pada saat melakukan proses enkripsi dan deskripsi sehingga data yang kita miliki akan sulit untuk dimengerti maknanya dan untuk proses enkripsi data yang sangat besar akan sangat cepat. Algoritma kriptografi yang digunakan adalah AES.

**Kata kunci** – kriptografi, Enkripsi, Deskripsi, AES.

## I. PENDAHULUAN

Data merupakan salah satu aset penting dalam kelangsungan hidup perusahaan manapun, instansi-instansi pemerintahan, maupun institusi-institusi pendidikan. Penyimpanan data memerlukan berbagai macam pertimbangan, terutama dari segi keamanannya dan kerahasiaannya.

Masalah keamanan merupakan suatu aspek penting dalam pengiriman data maupun komunikasi melalui jaringan. Salah satu cara untuk menjaga keamanan dan kerahasiaan suatu data maupun informasi adalah dengan teknik enkripsi dan dekripsi guna membuat pesan, data, maupun informasi tidak dapat dibaca atau dimengerti oleh orang lain, kecuali untuk penerima yang berhak [1]. Teknik pengamanan data dengan enkripsi dan dekripsi dikenal dengan kriptografi.

CV. Ranger Reload yang teletak di kota Tangerang merupakan salah satu perusahaan bergerak dibidang jasa agen pembelian pulsa (Server Pulsa). Selama ini CV. Ranger Reload dalam melakukan aktifitas penyimpanan piutang masih menggunakan metode penginputan data melalui Ms Excell. Sehingga untuk menjamin keamanan serta kevalidan data dibutuhkan sistem keamanan agar informasi data tidak diketahui atau dirubah oleh orang lain yg tidak berhak [2].

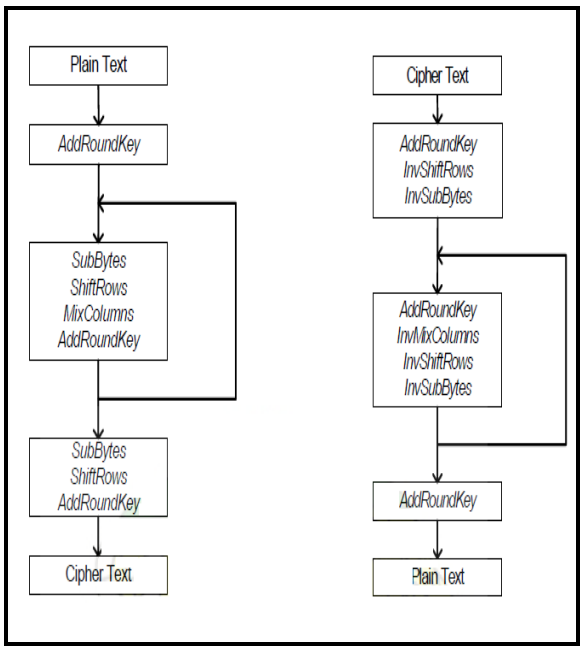
Software sebagai sarana umum dalam pengisian data, sangat rawan terhadap pencurian, penyadapan dan pemalsuan informasi. Dibutuhkan suatu pengamanan dalam pengiriman suatu paket data, apa lagi untuk data-data atau pesan-pesan yang bersifat sangat rahasia. Cara untuk mengamankan data dari kejadian-kejadian tersebut salah satunya dengan penyandian terhadap data yang akan dikirim. Penyandian ini sangat penting, apalagi dalam sektor-sektor strategis seperti bisnis, perbankan, atau pemerintahan sangat memerlukan teknologi penyandian informasi. Hal tersebut tentu saja menimbulkan resiko bila informasi yang sensitif dan berharga tersebut di akses oleh orang yang tidak bertangung jawab. Yang mana jika hal tersebut sampai terjadi, kemungkinan besar akan merugikan bahkan membahayakan orang yang akan mengirim pesan, maupun organisasinya. Informasi yang terkandung di dalamnya pun bisa saja berubah sehingga menyebabkan salah penafsiran oleh penerima pesan. Selain itu data yang di bajak tersebut kemungkinan rusak atau hilang yang menimbulkan kerugian material yang besar.

## II. METODE PENELITIAN

Algoritma AES (Advanced Encryption Standard) menggunakan substitusi, permutasi dan sejumlah putaran yang dikenakan pada tiap blok yang akan dienkripsi dekripsi. Untuk setiap putarannya, AES menggunakan kunci yang berbeda. Kunci setiap putaran disebut round key. AES beroperasi dalam orientasi byte sehingga memungkinkan untuk implementasi algoritma yang efisien ke dalam software dan hardware.

Ukuran blok untuk algoritma AES adalah 128 bit (16 byte). AES mendukung panjang kunci 128 bit sampai 256 bit dengan step 32 bit. Panjang kunci dan ukuran blok dapat dipilih secara independen. Setiap blok dienkripsidalam sejumlah putaran tertentu. Karena AES menetapkan panjang kunci adalah 128, 192, dan 256, maka dikenal AES 128, AES 192, dan AES 256 [3].

Adapun alur proses enkripsi dan dekripsi pada algorima AES dapat dilihat pada gambar dibawah ini:




Gambar. 2.1. Alur Proses Enkripsi Dan Dekripsi

## III. HASIL DAN PEMBAHASAN

### 3.1 Implementasi Metode

Proses penjadwalan kunci merupakan proses dimana cipherkey di jadwalkan untuk menghasilkan subkey-subkey yang digunakan untuk proses enkripsi dan dekripsi pada algoritma *Advanced Encryption Standard* (AES) [4]. Contoh penjadwalan kunci pada algoritma *Advanced Encryption Standard* (AES) jika diketahui kunci yang akan digunakan untuk enkripsi dengan panjang 32 byte yaitu:
Cipherkey = abcdefghijklmnopqrstuvwxyz123456

Tahap awal ubah cipherkey kedalam bentuk hexadecimal menjadi sebagai berikut:
Cipherkey = 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80

Tahap selanjutnya melakukan operasi-operasi penjadwalan kunci [5]. Operasi-operasi yang dilakukan yaitu RotWord, SubByte, dan melakukan operasi XOR untuk menghasilkan subkey. Operasi-operasi yang dilakukan yaitu sebagai berikut:

1. Masukan cipherkey tersebut kedalam blok 32 byte menjadi.

$$W = \begin{bmatrix} 61 & 65 & 69 & 6d & 71 & 75 & 79 & 7d \\ 62 & 66 & 6a & 6e & 72 & 76 & 7a & 7e \\ 63 & 67 & 6b & 6f & 73 & 77 & 7b & 7f \\ 64 & 68 & 6c & 70 & 74 & 78 & 7c & 80 \end{bmatrix}$$

2. Melakukan operasi *RotWord* pada kolom terakhir dari *ciphertext*.

$$\begin{bmatrix} \mathbf{7d} \\ 7e \\ 7f \\ 80 \end{bmatrix} = \begin{bmatrix} 7e \\ 7f \\ 80 \\ \mathbf{7d} \end{bmatrix}$$

3. Melakukan operasi *SubByte* dengan tabel *s-box* pada tabel II.2.

$$\begin{bmatrix} 7e \\ 7f \\ 80 \\ 7d \end{bmatrix} = \begin{bmatrix} f3 \\ d2 \\ cd \\ ff \end{bmatrix}$$

4. Hasil dari operasi *SubByte* dilakukan operasi XOR dengan *rcon* dan $W_1$ (kolom ke-1 dari W).

$$rcon = \begin{bmatrix} 01 & 02 & 04 & 08 & 10 & 20 & 40 & 80 & 1b & 36 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \\ 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 & 00 \end{bmatrix}$$

$$\begin{bmatrix} 61 \\ 62 \\ 63 \\ 64 \end{bmatrix} \oplus \begin{bmatrix} f3 \\ d2 \\ cd \\ ff \end{bmatrix} \oplus \begin{bmatrix} 01 \\ 00 \\ 00 \\ 00 \end{bmatrix} = \begin{bmatrix} 93 \\ b0 \\ ae \\ 9b \end{bmatrix}$$

5. Melakukan operasi XOR untuk untuk kolom selanjutnya dengan kolom yang baru.

$$\begin{bmatrix} 65 \\ 66 \\ 67 \\ 68 \end{bmatrix} \oplus \begin{bmatrix} 93 \\ b0 \\ ae \\ 9b \end{bmatrix} = \begin{bmatrix} f6 \\ d6 \\ c9 \\ f3 \end{bmatrix} \qquad \begin{bmatrix} 75 \\ 76 \\ 77 \\ 78 \end{bmatrix} \oplus \begin{bmatrix} 83 \\ a0 \\ be \\ 9b \end{bmatrix} = \begin{bmatrix} f6 \\ d6 \\ c9 \\ e3 \end{bmatrix}$$

$$\begin{bmatrix} 69 \\ 6a \\ 6b \\ 6c \end{bmatrix} \oplus \begin{bmatrix} f6 \\ d6 \\ c9 \\ f3 \end{bmatrix} = \begin{bmatrix} 9f \\ bc \\ a2 \\ 9f \end{bmatrix} \qquad \begin{bmatrix} 79 \\ 7a \\ 7b \\ 7c \end{bmatrix} \oplus \begin{bmatrix} f6 \\ d6 \\ c9 \\ e3 \end{bmatrix} = \begin{bmatrix} 8f \\ ac \\ b2 \\ 9f \end{bmatrix}$$

$$\begin{bmatrix} 6d \\ 6e \\ 6f \\ 70 \end{bmatrix} \oplus \begin{bmatrix} 9f \\ bc \\ a2 \\ 9f \end{bmatrix} = \begin{bmatrix} f2 \\ d2 \\ cd \\ ef \end{bmatrix} \qquad \begin{bmatrix} 7d \\ 7e \\ 7f \\ 80 \end{bmatrix} \oplus \begin{bmatrix} 8f \\ ac \\ b2 \\ 9f \end{bmatrix} = \begin{bmatrix} f2 \\ d2 \\ cd \\ 1f \end{bmatrix}$$

$$\begin{bmatrix} 71 \\ 72 \\ 73 \\ 74 \end{bmatrix} \oplus \begin{bmatrix} f2 \\ d2 \\ cd \\ ef \end{bmatrix} = \begin{bmatrix} 83 \\ a0 \\ be \\ 9b \end{bmatrix}$$

6. Simpan kedalam *subkey*.

$$SubKey = \begin{bmatrix} 93 & f6 & 9f & f2 & 83 & f6 & 8f & f2 \\ b0 & d6 & bc & d2 & a0 & d6 & ac & d2 \\ ae & c9 & a2 & cd & be & c9 & b2 & cd \\ 9b & f3 & 9f & ef & 9b & e3 & 9f & 1f \end{bmatrix}$$

Subkey ini yang akan digunakan untuk proses enkripsi atau dekripsi pada algoritma *Advanced Encryption Standard* (AES) pada round ke-1 untuk round selanjutnya dilakukan penjadwalan kunci kembali sampai round ke-14.

Proses enkripsi pada algoritma *Advanced Encryption Standard* (AES) terdiri dari empat operasi [6], yaitu Add Round Key, Sub Bytes, Shift Rows, dan Mix Columns. Operasi-operasi ini diulang terus-menerus hingga menghasilkan ciphertext. Jumlah perulangan yang dilakukan tergantung pada ukuran blok dan kunci yang digunakan, dalam hal ini ukuran blok dan kunci yang digunakan yaitu

256 bit, sehingga berdasarkan pada tabel 2.1, maka perulangan yang dilakukan sebanyak 14 kali. Contoh enkripsi pada algoritma advanced encryption standard, jika diketahui kunci dan plaintext yang akan digunakan untuk enkripsi dengan panjang 32 byte.

Cipherkey = abcdefghijklmnopqrstuvwxyx123456
Plaintext = UNIVERSITAS KOMPUTER INDONESIA !

Tahap awal ubah cipherkey dan plaintext kedalam bentuk hexadecimal menjadi sebagai berikut:
Cipherkey = 61 62 63 64 65 66 67 68 69 6a 6b 6c 6d 6e 6f 70 71 72 73 74 75 76 77 78 79 7a 7b 7c 7d 7e 7f 80
Plaintext = 55 4E 49 56 45 52 53 49 54 41 53 20 4b 4F 4D 50 55 54 45 52 20 49 4E 44 4F 4E 45 49 53 41 20 21

Masukan cipherkey dan plaintext ke dalam blok 32 byte sehingga menjadi

$$State = \begin{bmatrix} 55 & 45 & 54 & 4b & 55 & 20 & 4f & 53 \\ 4e & 52 & 41 & 4f & 54 & 49 & 4e & 41 \\ 49 & 53 & 53 & 4d & 45 & 4e & 45 & 20 \\ 56 & 49 & 20 & 50 & 52 & 44 & 49 & 21 \end{bmatrix} Cipherkey$$

$$= \begin{bmatrix} 61 & 65 & 69 & 6d & 71 & 75 & 79 & 7d \\ 62 & 66 & 6a & 6e & 72 & 76 & 7a & 7e \\ 63 & 67 & 6b & 6f & 73 & 77 & 7b & 7f \\ 64 & 68 & 6c & 70 & 74 & 78 & 7c & 80 \end{bmatrix}$$

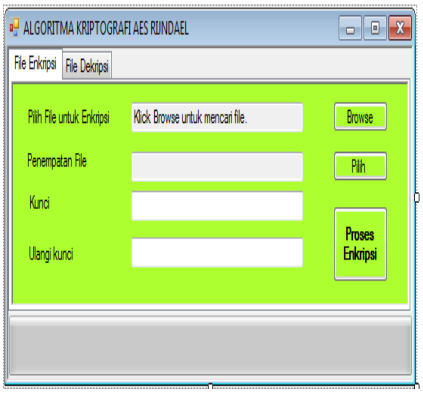
Semua operasi tersebut diulang sebanyak 10 kali hingga mendapatkan ciphertext. Untuk perulangan 1 sampai 9 dilakukan operasi SubByte, ShiftRow, MixColumn, dan AddRoundKey. Sedangkan untuk perulangan terakhir hanya dilakukan operasi SubByte, ShiftRow, dan AddRoundKey.

Proses dekripsi menggunakan algoritma *Advanced Encryption Standard* (AES) merupakan kebalikan dari proses enkripsi[7]. Operasi-operasi yang dilakukan yaitu InvSubByte, InvShiftRow, InvMixColumn, dan AddRoundKey.

3.2 Implementasi Antarmuka

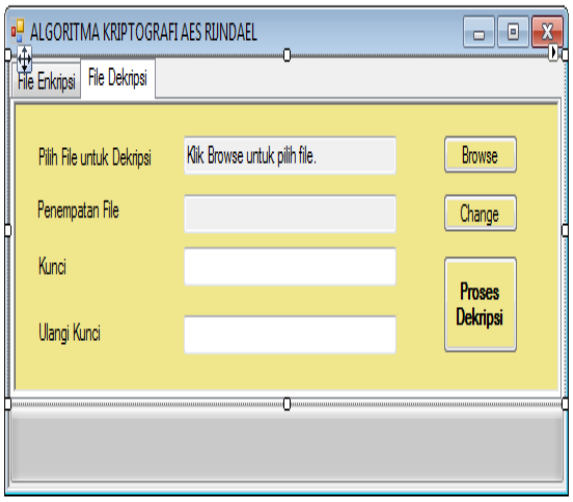
Pengertian sistem antarmuka adalah salah satu layanan yang disediakan sistem operasi sebagai sarana interaksi antara pengguna dengan sistem operasi. Antarmuka adalah komponen sistem operasi yang bersentuhan langsung dengan pengguna. Terdapat 2 (dua) jenis antarmuka, yaitu Command Line Interface (CLI) dan Graphical User Interface (GUI). Berikut ini adalah implementasi setiap antarmuka yang dibuat.

a. Implementasi Proses Enkripsi




Gambar 3.1. Implementasi Proses Enkripsi

b. Implementasi Proses Dekripsi




Gambar 3.2. Implementasi Proses Dekripsi

Tahap selanjutnya setelah mengimplementasikan perancangan kedalam program yaitu pengujian sistem. Pengujian sistem merupakan tahapan dimana sistem diuji untuk mengetahui apakah sistem yang dibangun telah sesuai dengan perancangan yang diinginkan atau tidak, dan untuk mengetahui apakah tujuan yang diinginkan telah tercapai atau belum.

## IV. KESIMPULAN

Berdasarkan hasil analisis dan penelitian dari uraian-uraian yang telah dikemukakan pada bab-bab sebelumnya tentang analisis dan perancangan keamanan data menggunakan algoritma kriptografi AES maka akan dapat kesimpulan sebagai berikut :

1. Keamanan data dengan menggunakan algoritma AES, data tidak akan bisa langsung di baca oleh pihak ketiga. Karena sebelumnya data di enkripsi terlebih dahulu menggunakan algoritma AES. Penggunaan kunci simetris yaitu kunci enkripsi sama dengan kunci pendekripsian pesan, sehingga data masih tetap terjaga keamanannya.
2. Penggunaan kunci merupakan sesuatu yang sangat penting dalam proses enkripsi dan dekripsi, sehingga dibutuhkan suatu kerahasiaan dalam pemakaian kuncinya.

## V. SARAN

Dalam penggunaan kunci diusahakan mudah diingat dan disepakati oleh kedua belah pihak. Perancangan keamanan data menggunakan kriptografi AES Rijdnael yang telah dibuat ini masih sebatas platform berbasis dekstop. Agar dikemudian hari dapat dikembangkan di platform berbasis android (mobile).

REFERENSI

[1] Dito Adiwidya, B. M. (2011). Algoritma AES (Advanced Encryption Standard) dan Penggunaannya dalam Penyandian Pengompresian Data.
[2] Kurniawan, Y. (2004). *Kriptografi Keamanan Internet dan Jaringan Komputer*. Bandung: Informatika.
[3] Munawar. (2005). *Pemodelan Visual dengan UML*. Yogyakarta: Andi.
[4] Munir, R. (2006). *Kriptografi*. Bandung: Informatika.
[5] Nazir. (2011). *Metode Penelitian.* Bogor: Ghalia Indonesia.
[6] Pabokory, F. N., Astuti, I. I., & Kridalaksana, A. H. (2015). PADA PESAN TEKS, ISI FILE DOKUMEN, DAN FILE DOKUMEN, DAN FILE DOKUMEN MENGGUNAKAN ALGORITMA AES. *Jurnal Informatika Mulawarman* , 20 -31.
[7] Sadikin, R. (2013). *Kriptografi untuk Keamanan Jaringan.* Yogyakarta: ANDI.