**ENKRIPSI DAN DEKRIPSI DENGAN MENGGUNAKAN ALGORITMA AESy**

Andre Abdirrosyid (5112100186)

Jurusan Teknik Informatika

**Abstrak :** Kerahasiaan dari suatu teks atau data sangatlah penting. Jika suatu teks atau pesan bisa dibaca begitu saja dengan orang lain, maka bisa mendatangkan hal yang tidak diinginkan. Untuk itu, dalam tugas ini saya ingin menjelaskan tentang metode enkripsi dengan mengubah urutan dan ukuran bit dari teks.

**Kata Kunci :** Kriptografi, algoritma.

1. **PENDAHULUAN**

Peranan ini, perkembangan ilmu pengetahuan dan teknologi telah mempengaruhi segala aspek kehidupan, tak terkecuali dalam aspek keamanan teks. Semakin berkembangnya teknologi, keamanan dari suatu teks menjadi berkurang atau tidak aman dalam hal penyimpanan. Tidak menutup kemungkinan ada pihak ketiga yang ingin merubah atau mengambil teks tersebut. Salah satu cara untuk mempertahankan kerahasiaan dari teks tersebut, maka teks tersebut disandikan menjadi kode-kode yang tidak dipahami, sehingga bila ada pihak ketiga yang ingin merubah akan kesulitan dalam menterjemahkan isi teks yang sebenarnya. Selanjutnya, untuk mengatasi permasalahan di atas, dapat diselesaikan dengan kriptografi. Kriptografi tidak hanya menyediakan alat untuk keamanan pesan, tetapi juga sekumpulan teknik yang berguna untuk keamanan dan kerahasiaan teks.

Algoritma yang digunakan adalah dengan mengubah urutan dan ukuran bit dari teks.

**2 LANDASAN TEORI**

**2.1 Sejarah Kriptografi**

Kriptografi mempunyai sejarah yang panjang. Informasi yang lengkap mengenai sejarah kriptografi dapat ditemukan di dalam buku David Kahn yang berjudul *The Codebreakers*. Buku yang tebalnya 1000 halaman ini menulis secara rinci sejarah kriptografi mulai dari penggunaan kriptografi oleh Bangsa Mesir 4000 tahun yang lalu (berupa *hieroglyph* yang tidak standard pada pyramid) hingga penggunaan kriptografi pada abad ke-20. Secara historis ada empat kelompok orang yang berkonstribusi terhadap perkembangan kriptografi, dimana mereka menggunakan kriptografi untuk menjamin kerahasiaan dalam komunikasi pesan penting, yaitu kalangan militer (termasuk intelijen dan mata-mata), kalangan diplomatik, penulis buku harian, dan pencinta (*lovers*). Di antara keempat kelompok ini, kalangan militer yang memberikan konstribusi paling penting karena pengiriman pesan di dalam suasana perang membutuhkan teknik enkripsi dan dekripsi yang rumit (Munir, 2006, hal 10).

* 1. **Teori Kriptografi**

Kriptografi adalah bidang ilmu yang sangat penting keberadaannya untuk menjaga kerahasiaan dan keamanan suatu informasi dan data. “Untuk mendefinisikannya lebih lanjut tentang kriptografi, Munir (2006, hal 2) menjelaskan bahwa kriptografi (*Cryptography*) berasal dari bahasa Yunani : “*cryptos*” artinya “*secret*” (rahasia), sedangkan “*graphien*” artinya “*writing*” (tulisan). Jadi, kriptografi (*Cryptography*) berarti “*secret writing*” (tulisan rahasia)”.

Kriptografi mempunyai beberapa tujuan. (Munir 2006, hal 9) menyampaikan tujuan kriptografi bahwa untuk memberi layanan keamanan (yang juga dinamakan sebagai aspek-aspek keamanan) sebagai berikut :

1. Kerahasiaan (*confidentiality*), adalah layanan yang ditujukan untuk menjaga agar pesan tidak dapat dibaca oleh pihak-pihak yang tidak berhak.
2. Integritas data (*data integrity*), adalah layanan yang menjamin bahwa pesan masih asli / utuh atau belum pernah dimanipulasi selama pengiriman.
3. Otentikasi (*authentication*), adalah layanan yang berhubungan dengan identifikasi, baik mengidentifikasi kebenaran pihak-pihak yang berkomunikasi (*user authentication* atau *entity authentication*) maupun mengidentifikasi kebenaran sumber pesan (*data origin authentication*).
4. Nirpenyalahgunaan (*non-repudiation*), adalah layanan untuk mencegah entitas yang berkomunikasi melakukan penyangkalan, yaitu pengiriman pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.
   1. **Kriptografi AESy**

Kriptografi Andre Encryption Style (AESy) adalah algortima yang mengubah ukuran dan urutan bit dari teks yang dienkripsi. Algoritma ini dibuat berdasarkan metode stream encryption.

Contoh:

Masing-masing huruf diubah menjadi angka. Misal A=1, B=2, C=3, …, Z=26. Kemudian angka tersebut diubah menjadi biner. Namun, awalnya teks yang akan dienkripsi dibalik urutannya terlebih dahulu.

Contoh:

A B C

Pertama, ubah urutannya sehingga teks tersebut menjadi C B A. Kemudian, ubah menjadi angka sesuai urutan abjad. Sehingga C=3, B=2, A=1.

Setelah itu, ubah menjadi biner. Sehingga:

C = 3 menjadi 011

B = 2 menjadi 010

A = 1 menjadi 001

Ketika digabungkan menjadi:

011 010 001

Setelah dijadikan biner (3-bit), panjang bit diubah ke 4-bit menjadi

0 1101 0001.

1. **PENUTUP**

**3.1 Kesimpulan**

Algoritma AESy masih belum sempurna. Algoritma tersebut masih memiliki kekurangan ketika orang lain ingin mengetahui pesan atau teks, orang tersebut akan dengan mudah meretas jika sudah mengetahui metode yang digunakan untuk mengenkripsi.

**3.2 Saran**

**DAFTAR PUSTAKA**

[1] [Oded Goldreich](http://id.wikipedia.org/w/index.php?title=Oded_Goldreich&action=edit&redlink=1), *Foundations of Cryptography, Volume 1: Basic Tools*, Cambridge University Press, 2001

[2] V. V. I︠A︡shchenko (2002). "[*Cryptography: an introduction*](http://books.google.com/books?id=cH-NGrpcIMcC&pg=PA6&dq&hl=en#v=onepage&q=&f=false)". AMS Bookstore. p.6.

[3]  [Singh, Simon](http://id.wikipedia.org/w/index.php?title=Simon_Singh&action=edit&redlink=1) (2000). [*The Code Book*](http://id.wikipedia.org/w/index.php?title=The_Code_Book&action=edit&redlink=1). New York: [Anchor Books](http://id.wikipedia.org/w/index.php?title=Anchor_Books&action=edit&redlink=1). hlm. 14–20.

[4] https://catatankriptografi.wordpress.com/category/stream-cipher/