KOMBINASI KRIPTOGRAFI ALGORITMA VIGENERE CIPHER DAN ALGORITMA AES UNTUK PENGAMANAN PESAN TEKS

Heru Triansyah[1],Anjas Pratama[2], MHD. Fazar Syahputra[3], Indra Gunawan[4]
Teknik Informatika, STIKOM Tunas Bangsa Pematangsiantar
ia1heru555@gmail.com
anzas152@gmail.com
fazarsyahputra02@gmail.com
indra@amiktunasbangsa.ac.id

Abstrak

Abstrak - Pada saat ini,perkembangan teknologi informasi terutama pada sistem pengamanan data untuk menjaga sebuah keamanan data telah berkembang pesat.Dalam menjaga keamanan data informasi terdapat sebuah cabang ilmu diantaranya seperti kriptografi.Kriptografi suatu hal yang sangatlah penting dalam pengamanan data untuk menjaga isi sebuah data dari para orang yang tidak berkepentingan yang dapat merugikan pemilik data.Dengan demikian kita perlu meningkatkan keamanan data,agar keaslian data dapat terjaga dengan aman dan data lebih terlindungi dari serangan-serangan yang dapat merusak isi dari data yang disimpan,terutama agar tidak terjadi bocornya sebuah informasi.Agar keamanan data lebih terjaga dapat pula mengkombinasi sebuah algoritma seperti mengkombinasikan algoritma vigenere cipher dan algoritma AES.

Kata Kunci: kriptogragfi , vigenere cipher, AES.

1. Pendahuluan

Perkembangan teknologi komputer dan telekomunikasi saat ini telah mengalami kemajuan yang sangat pesat,sehingga dibutuhkannya pengamanan data untuk menjaga suatu informasi yang tersimpan dalam bentuk digital.Banyak sekali permasalahan dalam keamanan sistem informasi seperti data hilang, data yang disadap,padahal *user* telah menggunakan pengamanan data berupa password.Oleh karena itu munculah cabang ilmu yang

DOI : https://doi.org/10.29103/techsi.v11i3.1874

mempelajari tentang cara-cara pengamanan data atau dikenal dengan istilah Kriptografi[1].Agar dapat mengamankan data dari berbagai ancaman tersebut dibutuhkanya pengelolaan kemaanan data digital dengan mengkombinasi 2 (dua) buah algoritma kriptografi,yaitu algoritma vigenere cipher dan algoritma aes dalam meningkatkan pengamanan sebuah pesan teks agar tidak mudah disadap oleh pihak yang tidak pertanggung jawab.

1.1 Defenisi Kriptografi

Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga pesan agar aman. (Cryptography is the art and science of keeping messages secure) "Crypto" berarti "secret" (rahasia) dan "graphy" berarti "writing" (tulisan). Jadi, kriptologi adalah ilmu dan seni untuk menjaga keamanan pesan yang akan dikirim ke penerima sehingga data atau pesan tersebut aman dan tidak diketahui oleh pihak ketiga [2].

Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem Kriptografi (Cryptosystem) adalah kumpulan dari fungsi enkripsi dan dekripsi yang berkoresponden terhadap kunci enkripsi dan dekripsi [3]. Menurut Menezes, kriptografi adalah ilmu yang mempelajari teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, otentikasi entitas, dan otentikasi asal data [4].

Kriptografi bertujuan untuk memberikan layanan keamanan [5],sebagai berikut :

-Kerahasiaan (Confidentiality)

Menjaga isi informasi dari orang yang tidak memiliki otoritas untuk mengaksenya.

- Keutuhan Data (Integrity)

Sistem harus mampu menjaga keaslian data terhadap manipulasi oleh pihak lain..

- Autentikasi (Message Autentication)

Menjaga kepastian identitas yang terlibat dan keaslian sumber data dari manipulasi pihak lain.

- Nirpenyangkalan (Nonrepudiation)

Menghindari adanya penyangkalan dari pengiriman.

DOI : https://doi.org/10.29103/techsi.v11i3.1874

2.Metode Penelitian

2.1 Algoritma Vigenere

Vigenère cipher adalah salah satu algoritma kriptografi klasik yang diperkenalkan pada abad 16 atau kira-kira pada tahun 1986. Algoritma kriptografi ini dipublikasikan oleh seorang diplomat dan juga kriptologis yang berasal dari Prancis, yaitu *Blaise de Vigenère*, namun sebenarnya algoritma ini telah digambarkan sebelumnya pada buku La Cifra del Sig. Giovan Batista Belaso, sebuah buku yang ditulis oleh Giovan Batista Belaso, pada tahun 1553 [6].

Vigenère cipher kunci yang digunakan berbentuk deretan huruf.Kunci yang berbetuk deretan kata tersebut akan memungkinkan setiap huruf plainteks untuk dienkripsi dengan kunci yang berbeda. Jika panjang kunci yang digunakan lebih pendek dari panjang *plainteks* maka kunci akan diulang sampai panjang kunci samdengan panjang *plainteks*.

Algoritma ini akan meminimalkan kemungkinan dipecahkannya *cipherteks* jika satu huruf plainteks diketahui. Model matematika dari enkripsi pada algoritma *Vigenère cipher* ini adalah seperti berikut:

Ci = (Pi + Ki) mod 26

Dan model matematika untuk deskripsinya adalah:

Pi = (Ci - Ki) mod 26

Keterangan:

Ci = nilai desimal karakter ciphertext ke-i

Pi = nilai desimal karakter plaintext ke-i

Ki = nilai desimal karakter kunci ke-i

Dimana nilai desimal karakter :A=0,B=1...Z=25.

Contoh :

Plaintext:STIKOMTB

Key:VIGENERE

Ciphertext :NBVOUQKF

Dimana jika pada proses enkripsi hasil Pi+Ki lebih dari 26 maka pengunaan mod 26 digunakan jika tidak maka langsung saja masukkan nilai dari hasil dari Pi+Ki.Dan jika pada proses deskripsi hasil dari Pi-Ki adalah nilai negatif, mod 26 tidak

DOI : https://doi.org/10.29103/techsi.v11i3.1874

berlaku,melainkan hasil nilai negatif langsung dijumlahkan dengan 26.

Namun algoritma ini memiliki kelemahan yaitu kuncinya yang pendek dan penggunaanya yang berulang-ulang,kunci yang berulang ini menimbulkan berbagai celah berupa penggeseran yang sama untuk setiap plainteks yang disubtitusikan oleh teks pada kunci yang sama[7].

2.2 Algoritma AES(Advanced Encryption Standard)

Advanced Encryption Standard (AES) adalah algoritma kriptografi yang menjadi standar algoritma enkripsi kunci simetris pada saat ini. Advanced Encryption Standard (AES) dipublikasikan oleh NIST (National Institute of Standard and Technology) pada tahun 2001. AES merupakan blok kode simetris untuk menggantikan DES (Data Encryption Standard) [8].

Saat ini, AES merupakan algoritma kriptografi yang cukup aman untuk melindungi data atau informasi yang bersifat rahasia.Pada tahun 2006, AES adalah salah satu algoritma populer yang digunakan dalam kriptografi kunci simetris [9].

Urutan data yang sudah terbentuk dalam satu kelompok 128 bit tersebut disebut juga sebagai blok data atau plaintext yang nantinya akan dienkripsi menjadi ciphertext. Cipher key dari AES terdiri dari key dengan panjang 128 bit, 192 bit, atau 256 bit. Perbedaan panjang kunci akan mempengaruhi jumlah *round* yang akan diimplementasikan pada algoritma AES ini. Berikut ini adalah Gambar.1 yang memperlihatkan jumlah *round* / putaran (Nr) yang harus diimplementasikan pada masingmasing panjang kunci.

DOI : https://doi.org/10.29103/techsi.v11i3.1874

	JUMLAH KEY (NK)	UKURAN BLOK (NB)	JUMLAH PUTARAN (NR)
AES - 128	4	4	10
AES - 192	6	4	12
AES - 256	8	4	14

Gambar 1. Perbandingan Jumlah *Round* dan *Key*

Pada saat permulaan, input bit pertama kali akan disusun menjadi suatu array *byte* dimana panjang dari array *byte* yang digunakan pada AES adalah sepanjang 8 bit data.Array *byte* inilah yang nantinya akan dimasukkan atau di*copy* ke dalam state dengan urutan dimana r (row / baris) dan c (column/kolom) :

$s[r,c] = in[r+4c]$ untuk $0 \leq r < 4$ dan $0 \leq c < Nb$

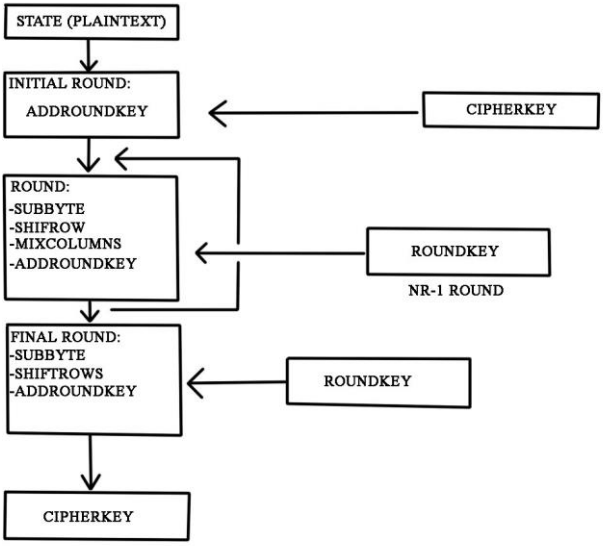
sedangkan dari state akan di*copy* ke *output* dengan urutan :

$out[r+4c] = s[r,c]$ untuk $0 \leq r < Nb$ [10].

a.Enkripsi

Proses enkripsi pada algoritma Adavanced Encryption Standard terdiri dari 4 jenis transformasi bytes, yaitu SubBytes, ShiftRows, Mixcolumns, dan AddRoundKey. Pada awal proses enkripsi, input yang telah dikopikan ke dalam state akan mengalami transformasi byte AddRoundKey.Setelah itu, state akan mengalami transformasi SubBytes, ShiftRows, MixColumns, dan AddRoundKey secara berulangulang sebanyak Nr. Proses ini dalam algoritma AES disebut sebagai *round function*.*Round* yang terakhir agak berbeda dengan *round-round* sebelumnya dimana pada *round* terakhir, state tidak mengalami transformasi MixColumns[11].Diagram alur proses enkripsi pada algoritma Advanced Encryption Standard dapat dilihat pada gambar 1.

DOI : https://doi.org/10.29103/techsi.v11i3.1874



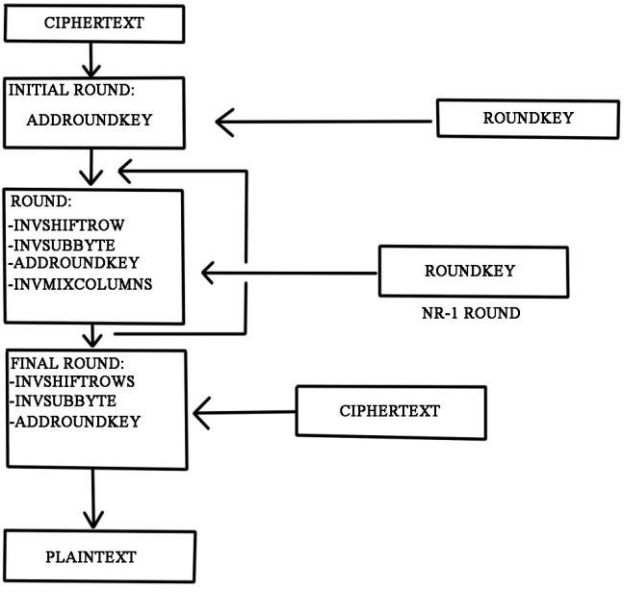
Gambar 2. Diagram Proses Enkripsi Pada Algoritma AES

Ada pula Pseudocode dari proses enkripsi vigenere cipher,sebagai berikut :

```
For (int = i = 0,j = 0;i < text.length();++i)
{
Char c = text[i];
If (c >=  'a' && c <= 'z')
c+='A'-'a' ;
else if (c < 'A' || c > 'Z')
continue;
out +=(c +key[j]-2*'A')%26+'A';
j = (j + 1) % key.length();
}
```

b.Deskripsi

Dan dalam proses deskripsinya dapat dibalikkan dan diimplementasikan dalam arah yang berlawanan untuk menghasilkan inverse cipher yang mudah dipahami untuk algoritma AES. Transformasi byte yang digunakan pada invers cipher adalah InvShiftRows, InvSubBytes, InvMixColumns, dan AddRoundKey[11].Diagram alur proses deskripsi pada algoritma Advanced Encryption Standard dapat dilihat pada gambar 2.



Gambar 3. Diagram Proses Deskripsi Pada Algoritma AES

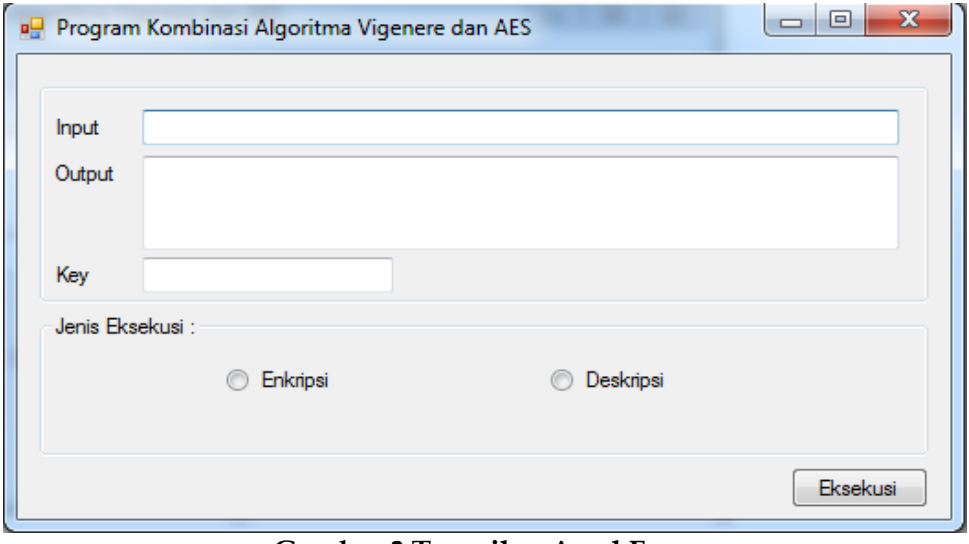
Ada pula Pseudocode dari proses deskripsi vigenere cipher,sebagai berikut :

DOI : https://doi.org/10.29103/techsi.v11i3.1874

```
For (int = i = 0,j = 0;i < text.length();++i)
{
Char c = text[i];
If (c >=  'a' && c <= 'z')
c+='A'-'a' ;
else if (c < 'A' || c > 'Z')
continue;
out +=(c - key[j]+26')%26+'A';
j = (j + 1) % key.length();
}
```

3. Hasil dan Diskusi

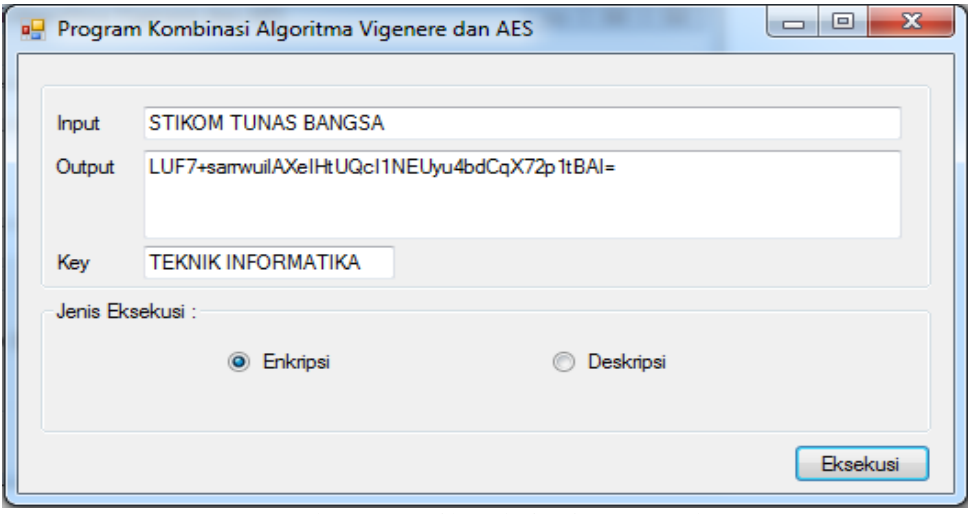
Pada perancangan ini penulis menggunakan Visual Basic .NET 2010.Dimana jika dipilih *radio button* 1 maka akan dilakukan proses enkripsi dan sebaliknya jika dipilih *radio button* 2 maka akan dilakukan proses deskripsi.Berikut adalah tampilan awal aplikasi.



Gambar 3.Tampilan Awal Form

Jika mengetikkan data teks berupa "STIKOM TUNAS BANGSA" pada *textbox1* dengan memasukkan *key* "TEKNIK

INFORMATIKA"dan melakukan proses enkripsi maka akan menghasilkan *ciphertext* LUF7+sarrwuilAXeIHtUQcI1NEUyu4bdCqX72p1tBAI=

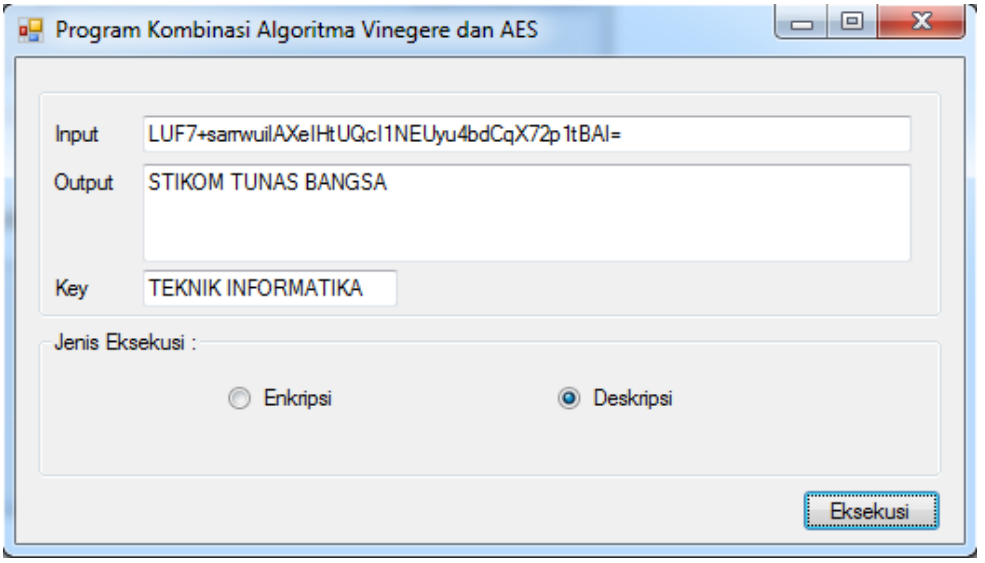


Gambar 4.Hasil Enkripsi Data Teks

Dimana pada proses pengenkripsian akan terlebih dahulu dilakukan dengan algoritma Vigenere Cipher dan menghasilkan sebuah *ciphertext*.Setelah itu *ciphertext* akan dienkripsikan kembali menggunakan algoritma AES.

Pada proses pendeskripsian data teks dapat dilakukan dengan menyalin hasil *ciphertext* yang telah dienkripsikan kedalam kolom input pada aplikasi dan memilih *radio button* 2.Maka
ciphertext yang dienkripsikan akan kembali menjadi *plaintext*.

DOI : https://doi.org/10.29103/techsi.v11i3.1874



Gambar 5.Hasil Dekripsi Data Teks

4.Kesimpulan

Kombinasi vigenere cipher dan algoritma aes dapat membantu meningkatkan keamanan data teks,jika dibandingkan hanya dengan menggunakan satu metode pengamanan data saja.Dengan mengkombinasikan sebuah algortima kriptografi pastinya data lebih terjaga keasliannya dan terhindar dari para penyadap.

Daftar Pustaka

G. Indra, "Kombinasi Algoritma Caesar Cipher dan Algoritma RSA Untuk Pengamanan File Dokumen dan Pesan Teks," *Jurnal Nasional Informatika dan Teknologi Jaringan*, vol. 2, no. 2, p. 125, 2018.

R. Munir, "Bahan Kuliah IF5051 Kriftografi," Institut Teknologi Bandung:Departemen Teknik Infomatika, 2006.

Mollin, R. A, *An Introduction to Cryptography*, 2nd Edition. Chapman & Hall/CRC : Boca Raton, Florida, 2007.

DOI : https://doi.org/10.29103/techsi.v11i3.1874

Menezes, A. J., Oorschot, P. C. v. & Vanstone, S. A, *Handbook of Applied Cryptography*.1st penyunt.Boca Raton: CRC Press, 1996.

Paar, C. & Pelzl, J, *Understanding Cryptography*.Springer Verlag: Berlin, 2010.

Efrandi, *et al*, "Aplikasi Kriptografi Pesan Menggunakan Algoritma Vigenere Cipher", *Jurnal Media Infotama,* vol. 10, no. 2, p. 120 – 128, 2014.

R. Sadikin, "Kriptografi Untuk Keamanan Jaringan dan Implementasinya dalam Bahasa Java", Yogyakarta: Andi, 2012.

A. Arif and P. Mandarani, "Rekayasa Perangkat Lunak Kriptografi Menggunakan Algoritma Advanced Encryption Standard (AES) 128 Bit Pada Sistem Keamanan Short Message Service (SMS) Berbasis Android," Teknoif, vol. 4, no. 1, p. 1–10, 2016.

P. I. G. Andika and W. I. M. Widhi, "Sistem Pengamanan Data Sidik Jari Menggunakan Algoritma AES Pada Sistem Kependudukan Berbasis Radio Frequency Identification (Rfid)",*Jurnal Ilmu Komputer,* vol. 5, no. 2, p. 30, 2012.

Gani and R. Antonius, "Enkripsi dan Deskripsi Dengan Algoritma AES 256 Untuk Semua Jenis File",*Jurnal Informatika*, vol. 5, no. 1, p. 23, 2009.

P. F. Narda,A. I. Fitri, and K. A. Harsa, "Implementasi Kriptografi Pengamanan Data Pada Pesan Teks,Isi File Dokumen,dan File Dokumen Menggunakan Algoritma Advanced Encryption Standard",*Jurnal Informatika Mulawarman,* vol. 10, no. 1, p. 23-24, 2015.

DOI : https://doi.org/10.29103/techsi.v11i3.1874