TEKNIK KEAMANAN DAN PENYIMPANAN DATA MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA AES DAN ALGORITMA RSA

Ilham Tri Yulian Akbar   
Program Studi Teknik Informatika S1  
Universitas Dian NuswantoroSemarang Jawa Tengah, Indonesia  
[111201609617@mhs.dinus.ac.id](mailto:111201609617@mhs.dinus.ac.id), ilhamtriyulian22@gmail.com

*Abstract* – Dengan berkembangan zaman, maka semakin berkembang pula kebutuhan manusia terutama kebutuhan akan penyimpanan data. Oleh karena itu maka diperlukanlah suatu pengamanan data yang menjamin keamanan data yang ketat dan keutuhan data ketika data tersebut disimpan untuk keperluan penting. Keamanan penyimpanan data dapat diselesaikan dengan menggunakan kriptografi. Salah satu algoritma yang digunakan untuk proses kriptografi yaitu dengan menggunakan algoritma Advanced Encryption Standard (AES) dan Rivest Shamir Adleman (RSA). Untuk menyimpan data tidaklah cukup dengan menyimpan biasa, penyimpaan tersebut bisa diamankan dengan metode Encryption. Hasil dari penelitian yaitu menghasilkan aplikasi yang dapat mengamankan data dengan baik dan menutup pengguna lain yang tidak ijin dengan pengguna data tersebut

Keywords—AES,RSA,Kriptografi,Encryption

# Introduction (*Heading 1*)

Keamanan data merupakan hal sangat penting untuk zaman era saat ini. Pada umumnya, setiap institusi memliki dokumen dokumen penting dan bersifat rahasia yang mendapat ijin dari orang orang tertentu. System keamanan data yang dikembangkan harus menjamin keamanan dan kerahasiaan dokumen-dokumen tersebut. Namun kendalanya bahwa dokumen dokumen sering dipakai oleh orang yang tidak dapat ijin oleh orang yang mempunyai dokumen tersebut.

Kriptografi (cryptography) merupakan ilmu dan seni untuk menjaga data atau pesan secara aman.( Cryptography is the art and science of keeping messages secure) “Crypto” berarti “secret” (rahasia)vdan “graphy” berarti “writing” (tulisan). Para pelaku atau praktisi kriptografi disebut cyrptographers. Sebuah algoritma kriptografik (cryptographic algorithm), disebut cipher, merupakan persamaan matematik yang digunakan untuk proses enkripsi dan dekripsi. Biasanya persamaan kedua matematik (untuk enkripsi dan dekripsi) tersebut memiliki hubungan matematis yang cukup erat.

AES adalah suatu algoritma standar [enkripsi](https://id.wikipedia.org/wiki/Enkripsi" \o "Enkripsi) dengan kunci-simetris yang diadopsi oleh pemerintah Amerika Serikat. Standar ini terdiri atas 3 blok [cipher](https://id.wikipedia.org/w/index.php?title=Cipher&action=edit&redlink=1), yaitu [AES-128](https://id.wikipedia.org/w/index.php?title=AES-128&action=edit&redlink=1), [AES-192](https://id.wikipedia.org/w/index.php?title=AES-192&action=edit&redlink=1) and [AES-256](https://id.wikipedia.org/w/index.php?title=AES-256&action=edit&redlink=1), yang diadopsi dari koleksi yang lebih besar yang awalnya diterbitkan sebagai **[Rijndael](https://id.wikipedia.org/w/index.php?title=Rijndael&action=edit&redlink=1" \o "Rijndael (halaman belum tersedia)).** Masing-masing cipher memiliki ukuran 128-[bit](https://id.wikipedia.org/wiki/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,

RSA adalah suatu algoritma  sebuah algoritme pada enkripsi public key. RSA merupakan algoritme pertama yang cocok untuk digital signature seperti halnya enkripsi, dan salah satu yang paling maju dalam bidang kriptografi public key.

Tetapi pada zaman saat ini.teknik keamanan dengan menggunakan kriptografi dirasa masih kurang. Setelah dilakukan proses keamanan data pada kriptografi tersebut maka kita perlu mengamankan data dengan cara memberi password yang tidak ada beberapa orang mengetahui data tersebut yaitu menggunakan encryption dan di amankan oleh dua algoritma yaitu RSA dan AES.

Berdasarkan masalah diatas, maka saya mengusulkan judul penelitian yaitu “Teknik Keamanan Dan Penyimpanan Data Menggunakan Kriptografi Dengan Algoritma AES dan Algoritma RSA”

# Ease of Use

## Kriptografi (Heading 2)

.Kriptografi merupakan ilmu mengenai teknik enkripsi dimana “naskah asli” (plaintext) diacak menggunakan suatu kunci enkripsi menjadi “naskah acak yang sulit dibaca” (ciphertext) oleh seseorang yang tidak memiliki kunci dekripsi. Dekripsi menggunakan kunci dekripsi bisa mendapatkan kembali data asli. Probabilitas mendapat kembali naskah asli oleh seseorang yang tidak mempunyai kunci dekripsi dalam waktu yang tidak terlalu lama adalah sangat kecil.

Dalam mengenkripsi data tersbut, Data akan berubah menjadi tidak bisa dipakai atau tidak dibisa dibaca. Dan harus mengetehui terlebih dahulu oleh password enkripsi data tersebut.

Kriptografi mempunyai 4 tujuan yaitu :

1. Kerahasiaan

Menjamin data tersebut akan tersimpan secara benar dan aman dari siapapun yang tidak memiliki password enkripsinya dan data tersebut akan berbentuk password yang di enkripsinya

1. Intergritas data.

Dalam kriptografi akan dilakukan proses pengecekan data apakah data yang sampai di penerima merupakan data yang dikirim oleh pertama kali yang mengirim.

1. Autentikasi.

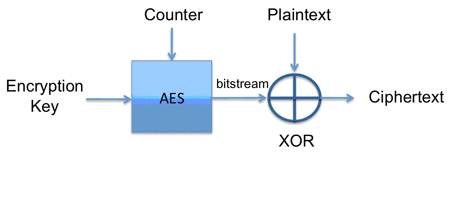
Pada proses autentikasi ini data akan dicek apakah data tersebutt mengalami manipulasi dalam isinya seperti penyisipan, penghapusan dan penggantian data

1. Non – Repudasi

Jika seseorang sudah mengirimkan data, maka orang tersebut tidak dapat membantah/ menyangkal pengiriman data tersebut.

## Algoritma AES

Algoritma Aes menggunakan ciphertext untuk mengenkripsi data. Setiap data yang enkripsi pada aes tersebut tidak akan terbaca oleh pengguna yang tidak tau key nya, karena algoritma aes tersebut diberi key oleh pengguna yang mempunyai file. Lebih jelasnya dapat dilihat pada gambar dibawah ini :



Gambar 1 : Proses Berjalannya AES

Pada proses enkripsi diatas, data akan diencryption key, data tersebut akan berubah menjadi aes dan akan keluar outputnya menjadi ciphertext.

## Algoritma RSA

Algoritma Rsa menggunakan dua kunci atau yang disebut dengan sandi asimetris untuk mengenkripsi data pada rsa tersebut. Tingkat keamanan pada algoritma RSA sangat bergantung pada asimetris yang ada pada algoritma tersebut

Maka disaat besaran ukuran kunci akan tambah semakin sulit untuk ditembus pada algoritma tersebut.

Besaran-besaran yang digunakan pada algoritma RSA:

1.      *p*dan *q*bilangan prima (rahasia)

2.      *r*= *p*⋅ *q*(tidak rahasia)

3.      m = (*p*– 1)(*q*– 1) (rahasia)

4.      *PK*(kunci enkripsi) (tidakrahasia)

5.      *SK*(kunci dekripsi) (rahasia)

6.      *X*(plainteks) (rahasia)

7.      *Y*(cipherteks) (tidak rahasia)

# Metode penelitian

## Metode Pengumpulan data

Dalam penelitian ini data yang digunakan merupakan data sekunder. Penulis mendapat data dari pustaka dan artikel artikel yang penulis dapat dari pustaka pendukung, informasi dari internet dan jurnal=jurnal.

## Metode Pengembangan Sstem

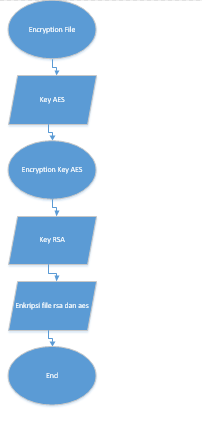
Pengembangan Sistem yang digunakan adalah Rapid Application Development (RAD) adalah pengembangan software yang diciptakan untuk mendesain serta mengimplementasiakn system sehingga dihasilkan siklus pengembangan yang sangat pendek.

suatu pendekatan berorientasi objek terhadap pengembangan sistem yang mencakup suatu metode pengembangan serta perangkat-perangkat lunak. RAD bertujuan mempersingkat waktu yang biasanya diperlukan dalam siklus hidup pengembangan sistem tradisional antara perancangan dan penerapan suatu sistem informasi. Pada akhirnya, RAD sama-sama berusaha memenuhi syarat-syarat bisnis yang berubah secara cepat.

Kelebihan pada metode rad

* Penghematan waktu dalam keseluruhan fase projek dapat dicapai.
* RAD mengurangi seluruh kebutuhan yang berkaitan dengan biaya projek dan sumberdaya manusia.
* RAD sangat membantu pengembangan aplikasi yang berfokus pada waktu penyelesaian projek.
* Perubahan desain sistem dapat lebih berpengaruh dengan cepat dibandingkan dengan pendekatan SDLC tradisional.
* Sudut pandang user disajikan dalam sistem akhir baik melalui fungsi-fungsi sistem atau antarmuka pengguna.
* RAD menciptakan rasa kepemilikan yang kuat di antara seluruh pemangku kebijakan projek.

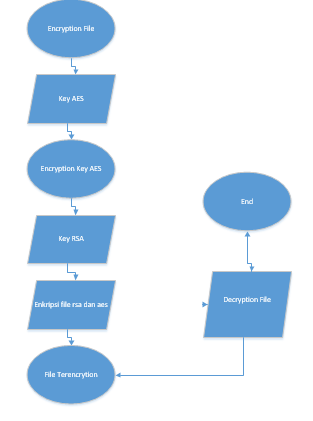
## Pemodelan Proses

Beriukut ini merupakan pemodelan proses penulis yang diajukan :

Gambar 2 : Proses Encryption Data

Pemodelan proses untuk proses diatas yaitu mempunyai 2 buah inputan awal yaitu key, AES dan RSA, kemudian file akan dienkripsi oleh aes. Setelah dienkripsi oleh aes. File yang berbentuk aes akan dienkripsi lagi menjadi enkripsi RSA.

Di RSA tersebut akan mendapat password atau key yang akan menjadi lebih aman lagi untuk file tersebut dan hanya bisa dibuka untuk yang sudah diijinkan kepada pembuat data tersebut. Untuk membuka file tersebut diperlukan dekripsi untuk membuka file yang sudah dienkripsi oleh pembuat data tersebut.



Gambar 3 : Proses deskripsi data

## Kesalahan Umum pada data

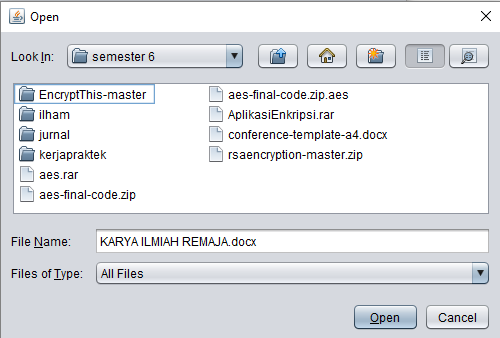
Beberapa kesalahan umum pada data

* Kesalahan pada pengerjakan data tersebut.
* Ketika data tidak sesuai dengan apa yang di inginkan data tersebut tidak akan keluar.
* Salah memasukan key atau tidak sesuai password yang di enkripsikan

# HASIL PENELITIAN

Pada penelitian ini penulis mencoba untuk menggabungkan antara algoritma keduanya. Dan tidak hanya menggabungkan antara kedua algoritma tersebut, penulis juga mencoba untuk menenkripsi file. Dan mendekripsi kan file tersebut.

## 

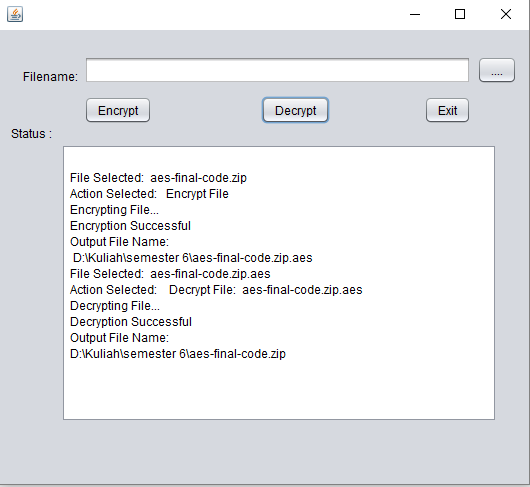


Gambar 4 : Proses Hasil Enkripsi

Pada hasil yang gambar diatas menunjukan file yang terenkripsi berhasil.

Dengan adanya .aes yang menunjukan file itu sudah terenkripsi oleh algoritma Aes Dan Rsa.

Berikut proses dekripsi pada file tersebut :



## 

## Gambar 5 : Proses Hasil Dekripsi

Pada gambar diatas proses hasil dekripsi tersebut menunjukkan file tersebut sudah berhasil didekirpsi. Dan kembali seperti semula.

Pada ukuran file tersebut tidak ada menandakan file itu terlalu besar ataupun kecil.

File yang dienkrispi bisa berbagai file. Seperti word,pdf,rar, dan sebagainya.

1. Table Type Styles

| Table Head | HASIL PENELITIAN BERDASARKAN FILE | | |
| --- | --- | --- | --- |
| Encrypdata | Decrption |  |
| Aes-final-code.  zip | Aes-final-code.  Zip.aes | Aes-final-code.  Zip |  |

1. Sample of a Table footnote. (*Table footnote*)
2. Example of a figure caption. (*figure caption*)

Pada Tabel diatas menunjukkan bahwa. Disaat file di enkripsi aAes-final-code.Zip berubah menjadi Aes-final-code.Zip.aes.

Disaat sesudah selesai dienkripsi. Data tersebut didekripsi guna membalikkan data seperti semula dan berubah sepeerti semula lagi.

# Kesimpulan

## Kesimpulan

Dari hasil perancangan dan pembuatan aplikasi Enkrispi dan deskripsi dengan Kriptografi menggunakan Algoritma AES dan algoritma RSA maka didapatkan hasil sebagai berikut :

1. Dari hasil percobaan yang telah dilakukan pada aplikasi ini dapat mengamankan data dan menyimpan data dan menutup data dengan menggunakan password algoritma AES dan algoritma RSA.
2. Pada proses enkripsi data tersebut bisa diamakan dengan baik tanpa sepengetahuan seseorang yang akan membuka data tanpa seijin pembuat data.
3. Pada proses dekripsi data tersebut bisa dibuka kembali seperti semula oleh seorang yang memegang kunci data tersebut.
4. Penggabungan antara 2 algoritma tersebut data lebih semakin aman dan tidak ada kendala yang terjadi. Hanya saja data bisa dibuka dengan ada tulisan .aes
5. Untuk hasil enrkripsi data akan berbentuk isi yang kosong atau rusak kalua tidak dibuka dengan kunci yang dipegang oleh seorang pembuat data.

## Saran

Saran yang dapat digunakan untuk tahap pada aplikasi enkripsi dan dekripsi data yaitu dengan menghilangkan tulisan pada .aes nya. Sehingga seseorang yang tidak bertanggung jawab tidak akan mengetahui dimana titik letak data tersebut.

##### References

1. TEKNIK KEAMANAN DATA MENGGUNAKAN KRIPTOGRAFI DENGAN ALGORITMA VIGENERE CIPHER DAN STEGANOGRAFI DENGAN METODE END OF FILE (EOF) 1 Patricia Handoko, 2 Aripin, M.kom
2. <https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/>
3. Kriptografi Advanced Encryption Standard (AES) Untuk Penyandian File Dokumen, Aditia Rahmat Tulloh, Yurika Permanasari, Erwin Harahap, Jurnal Matematika UNISBA Vol 15 No 1, Mei 2016.
4. <http://kriptografijaringan.blogspot.com/2016/03/enkripsi-algoritma-aes-advanced.html>
5. <http://kandisbuana.blogspot.com/2011/05/algoritma-rsa.html>
6. <https://piyaneo.wordpress.com/2014/05/10/rapid-application-development-rad/>
7. <https://www.maxmanroe.com/kunci-data-dengan-teknologi-enkripsi.html>