PEMBANGUNAN APLIKASI PEMBANDING KRIPTOGRAFI DENGAN *CAESAR CIPHER* DAN *ADVANCE ENCRYPTION STANDARD* (AES) UNTUK FILE TEKS

THE DEVELOPMENT OF A CRYPTOGRAPHY APPLICATION WITH CAESAR CIPHER *AND* ADVANCE ENCRYPTION STANDARD(AES) *FOR TEXT FILE*

Aji Fitrah Marisman

Politeknik Negeri Jakarta
Jl. Prof. Dr. G.A Siwabessy, Kampus Baru UI Depok 16424
Ajifitrah123@gmail.com

Anita Hidayati

Politeknik Negeri Jakarta
Jl. Prof. Dr. G.A Siwabessy, Kampus Baru UI Depok 16424
anita.hidayati@tik.pnj.ac.id
(Diterima: 28 Agustus 2015; Direvisi: 1 Oktober 2015; Disetujui terbit: 9 Oktober 2015)

Abstrak

Keamanan data adalah hal yang sangat penting. Salah satu solusi pengamanan data yang digunakan adalah kriptografi. Kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikannya ke dalam bentuk yang tidak dapat dimengerti lagi. Pada paper ini dibangun aplikasi kriptografi menggunakan metode tradisional Caesar Cipher dan metode modern Advance Encryption Standard (AES). Pada metode Caesar Cipher, proses enkripsi/dekripsi file teks hanya dapat dilakukan untuk karakter huruf. Sedangkan pada metode AES, proses enkripsi/dekripsi file dapat dilakukan untuk seluruh karakter huruf, angka dan simbol. Hasil analisa menunjukkan bahwa metode AES lebih unggul dari Caesar Cipher. Pengujian metode AES dilakukan pada data 128 Bit,192 Bit dan 256 Bit. Berdasarkan analisa keamanan diperoleh bahwa metode AES lebih aman dari Caesar Cipher karena ciphertext tidak dapat dipecahkan dengan metode Brute Force Attack dengan tidak munculnya plaintext awal AES. Dari sisi waktu, dengan menggunakan file teks berukuran 100KB, 500 KB dan 1000KB, AES lebih unggul dari Caesar Cipher dengan rata–rata perbedaan waktu sebesar 3000 ms. Dari sisi ukuran, Caesar Cipher lebih unggul dengan perubahan ukuran sebesar 0% sedangkan AES mengalami penambahan ukuran sebesar 33%.
Kata kunci: Kriptografi, Advance Encryption Standard (AES), Caesar Cipher

Abstract

Data security is very important. One solution to secure data that is used is cryptography. Cryptography is the science and art to maintain confidentiality by means of encrypting the message into a form that can not be understood anymore. In this paper cryptographic applications built using traditional methods and modern methods Caesar Cipher Advance Encryption Standard (AES). At Caesar Cipher method, encryption/decryption process text files can only be done for character letters. While the method of the Advanced Encryption Standard, encryption/decryption of files can be done for the entire case characters, numbers and symbols. Testing AES method on the data 128 Bit, 192 Bit and 256 Bit. Based on the safety analysis shows that the AES method is more secure than the Caesar Cipher because ciphertext can not be solved by the method of Brute Force Attack with the advent of early planteks AES. In terms of time, by using the text file size of 100KB, 500KB and 1000KB, AES superior to the Caesar Cipher with an average difference in time of 3000 ms. In terms of size, the Caesar Cipher is superior to the change in size of 0% while the AES experiencing increasing the size by 33%.
Keywords: *Cryptography, Advanced Encryption Standard, Caesar Cipher*

PENDAHULUAN

Masalah keamanan dan kerahasiaan merupakan salah satu aspek penting dari suatu data, pesan dan informasi. Data menjadi hal vital di masa ini, terkait betapa pentingnya pihak atau orang berkepentingan yang dapat mengakses data tersebut. Apabila ada pihak yang tak berkepentingan mengakses data tersebut, maka dikhawatirkan akan terjadi hal yang tidak diinginkan.

Sejak lahirnya konsep *open system*, semua data dapat mengalir bebas melewati jaringan komputer. Namun, hal ini menjadi resiko tersendiri bagi pengguna karena data tersebut dapat diakses oleh pihak yang tidak berkepentingan. Berbagai cara dilakukan untuk mendapatkan data dan informasi, mulai dari tingkatan yang mudah sampai pada cara-cara yang rumit (Andri M 2009). Salah satu cara untuk mengamankan data dari tindakan kejahatan adalah menggunakan konsep kriptografi.

Kriptografi merupakan seni atau ilmu untuk menjaga keamanan data. Konsep kritografi bermula dari zaman tradisional hingga modern. Secara umum ada dua jenis kriptografi, yaitu tradisional/klasik dan modern. Kriptografi tradisional adalah suatu algoritma yang menggunakan satu kunci untuk mengamankan data. Dua teknik dasar yang biasa digunakan adalah substitusi dan transposisi (permutasi). Salah satu metode kriptografi tradisional adalah *Caesar Cipher* yang hanya mampu mengamankan data karakter a–z dan A–Z saja (Suriski dkk, 2010). Seiring berkembangnya data, munculah berbagai macam metode kriptografi modern yang dapat mengamankan semua data karakter. Kriptografi modern adalah algoritma yang lebih kompleks daripada kriptografi tradisional, hal ini disebabkan algoritma ini menggunakan komputer. Terdapat 3 algoritma pada kriptografi modern (Rachman 2010), yaitu:

1.Algoritma simetris adalah algoritma yang menggunakan kunci yang sama untuk enkripsi dan dekripsinya. Aplikasinya digunakan oleh algoritma Data Encryption Standard (DES), Advance Encryption Standard (AES), International Data Encryption Algoritma (IDEA), A5, RC4

2. Algoritma Asimetris adalah pasangan kunci kriptografi yang salah satunya digunakan untuk proses enkripsi dan satu lagi untuk dekripsi. Contoh algoritma terkenal yang menggunakan kunci asimetris adalah RSA

3. Algoritma hibrida adalah algoritma yang memanfaatkan dua tingkatan kunci, yaitu kunci rahasia (simetri) yang disebut juga *session key* (kunci sesi) untuk enkripsi data dan pasangan kunci rahasia – kunci publik untuk pemberian tanda tangan digital serta melindungi kunci simetri. Algoritma kriptografi yang beroperasi dalam mode bit dapat dikelompokkan menjadi dua kategori: *Cipher* aliran (*stream cipher*) dan *Cipher* blok (*block cipher*) (Rachman 2010).

Metode kriptografi tradisional dan metode kriptografi modern memiliki perbedaan dalam hal pengamanan data mulai dari proses hingga hasil output yang dihasilkan. Untuk itu di penelitian ini dibangun aplikasi kriptografi dengan metode kriptografi tradisional dan metode kriptografi modern.

Dalam penelitian akan dilakukan pembandingan implementasi keamanan data dari setiap metode dari sisi efisiensi waktu dan ukuran. Proses enkripsi dan dekripsi hanya dapat dilakukan untuk file teks pada masing–masing metode. Untuk metode *Caesar Cipher*, proses enkripsi/dekripsi ile teks hanya dapat dilakukan untuk karakter huruf. Sedangkan pada metode Advanced Encryption Standard, proses enkripsi/dekripsi file dapat dilakukan untuk seluruh karakter huruf, angka dan simbol.

LANDASAN TEORI

Enkripsi dan Dekripsi

Enkripsi adalah sebuah proses yang melakukan perubahan sebuah kode yang bisa dimengerti menjadi sebuah kode yang tidak bisa dimengerti. Enkripsi dapat diartikan sebagai kode atau *cipher*. Enkripsi merupakan sebuah sistem pengkodean menggunakan suatu tabel atau kamus yang telah didefinisikan untuk mengganti kata dari informasi yang dikirim. Sebuah *cipher* menggunakan suatu algoritma yang dapat mengkodekan semua aliran data (stream) bit dari sebuah pesan menjadi *cryptogram* yang tidak dimengerti (*unintelligible*). Oleh karena teknik cipher merupakan suatu sistem yang telah siap untuk diautomasi, maka teknik ini digunakan dalam sistem keamanan komputer dan jaringan (Manan and Subari 2014).

Enkripsi dimaksudkan untuk melindungi informasi agar tidak terlihat oleh orang atau pihak yang tidak berhak. Informasi ini dapat berupa nomor kartu kredit, catatan penting dalam komputer, maupun *password* untuk mengakses sesuatu. Dengan mengenkrip paket data yang lalu lalang di Internet, walaupun seseorang dapat menangkap paket-paket data tersebut, tetap saja tidak dapat memahami artinya. Enkripsi juga digunakan untuk verifikasi (Wirdasari, 2008). Saat mengunduh *software*, maka akan diketahui bahwa *software* yang diunduh adalah asli, bukan yang telah dipasang Trojan di dalamnya.

Terdapat tiga kategori enkripsi, yaitu (Wahana Komputer, 2003): kunci enkripsi rahasia, kunci enkripsi publik dan fungsi *one-way* atau fungsi satu arah yang adalah suatu fungsi dimana informasi dienkripsi untuk menciptakan "*signature*" dari informasi asli yang bisa digunakan untuk keperluan autentikasi.

Dekripsi adalah proses dengan algoritma yang sama untuk mengembalikan informasi teracak menjadi bentuk aslinya. Algoritma yang digunakan harus terdiri dari susunan prosedur yang direncanakan secara hati–hati yang harus secara efektif menghasilkan sebuah bentuk terenkripsi yang tidak bisa dikembalikan, bahkan sekalipun dengan algoritma yang sama.

Caesar Cipher

Caesar Cipher adalah salah satu teknik enkripsi paling sederhana dan paling terkenal. Sandi ini termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet (Haryanto, Apriani and Sefyanto 2012). Pada *Caesar Cipher*, tiap huruf disubstitusi dengan huruf ketiga berikutnya dari susunan alphabet yang sama. Dalam hal ini kuncinya adalah pergeseran huruf. Susunan alphabet setelah digeser sejauh 3 huruf membentuk sebuah tabel substitusi sebagai berikut:

Alfabet Biasa: A B C D E F G H I J K L M N O P Q R S T U V W X Y Z

Alfabet Sandi: D E F G H I J K L M N O P Q R S T U V W X Y Z A B C

Untuk menyandikan sebuah pesan, cukup mencari setiap huruf yang hendak disandikan di alfabet biasa, lalu dituliskan huruf yang sesuai pada alfabet sandi. Untuk memecahkan sandi tersebut digunakan cara sebaliknya. Contoh penyandian sebuah pesan sebagai berikut:

Teks Terang: JANGAN KE BLOK D
Teks Sandi: MDQJDQ NH EORN G

Dengan mengkodekan setiap huruf alfabet dengan integer: 'A'=0, 'B'=1, …, 'Z'= 25, maka secara matematis pergeseran 3 huruf alfabetik ekivalen dengan melakukan operasi modulo terhadap *plaintext* menjadi *ciphertext* dengan persamaan:

$$C = E(P) = (P + 3) \bmod 26 \quad (1)$$

Pada persamaan 1, E adalah fungsi enkripsi, P adalah *plaintext*, C adalah *ciphertext*. Dilakukan modulo dengan 26 karena ada 26 huruf di dalam alphabet. Penerima pesan mengembalikan lagi *ciphertext* dengan operasi kebalikan, secara matematis dapat dinyatakan dengan persamaan:

$$P = D(C) = (C - 3) \bmod 26 \quad (2)$$

Dapat diperhatikan bahwa fungsi D adalah balikan (invers) dari fungsi E:

$$D(C) = E\text{-}1(P)\ (3) \quad (3)$$

Penggunaan dari *Caesar Cipher* ini

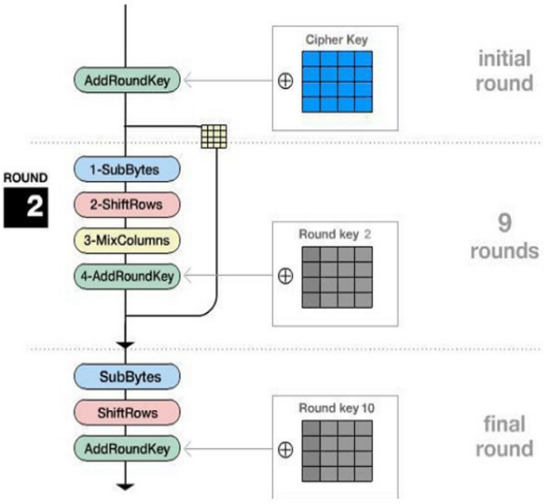
dapat dimodifikasi dengan mengubah jumlah geseran (bukan hanya 3). Jadi *Caesar Cipher* dapat digunakan dengan geser 7, misalnya. Hal ini dilakukan untuk lebih menyulitkan orang yang ingin menyadap pesan sebab semua kombinasi harus dicoba (26 kemungkinan geser)

Advanced Encryption Standard (AES)

AES adalah lanjutan dari algoritma enkripsi standar DES (*Data Encryption Standard*) yang masa berlakunya dianggap telah usai karena faktor keamanan. Kecepatan komputer yang sangat pesat dianggap sangat membahayakan DES, sehingga ditetapkanlah algoritma baru Rijndael sebagai AES (Surian 2006). Kriteria pemilihan AES didasarkan pada 3 kriteria utama yaitu: keamanan, harga, dan karakteristik algoritma beserta implementasinya (Munawar 2012). Keamanan merupakan faktor terpenting dalam evaluasi (minimal seaman *triple* DES), yang meliputi ketahanan terhadap semua analisis sandi yang telah diketahui dan diharapkan dapat menghadapi analisis sandi yang belum diketahui.

Di samping itu, AES juga harus dapat digunakan secara bebas tanpa harus membayar royalti, dan juga murah untuk diimplementasikan pada smart card yang memiliki ukuran memori kecil. AES juga harus efisien dan cepat (minimal secepat *Triple* DES) dijalankan dalam berbagai mesin 8 bit hingga 64 bit, dan berbagai perangkat lunak.

AES memiliki blok masukan dan keluaran serta kunci 128 bit. Untuk tingkat keamanan yang lebih tinggi, AES dapat menggunakan kunci 192 dan 256 bit (Lusiana, 2011). Setiap masukan 128 bit *plaintext* dimasukkan ke dalam *state* yang berbentuk bujursangkar berukuran 4×4 *byte*. *State* ini di XOR dengan *key* dan selanjutnya diolah 10 kali dengan subtitusi-transformasi *linear-Addkey*, dan di akhir diperoleh *ciphertext*. Diagram AES dapat dilihat pada Gambar 1.



Gambar 1. Diagram AES

Berikut ini adalah operasi Rijndael (AES) yang menggunakan 128 bit kunci (Munir, 2006):

Ekspansi kunci utama (dari 128 bit menjadi 1408 bit)

Pencampuran subkey

Diulang dari i=1 sampai i=10 Transformasi: *ByteSub* (subtitusi per *byte*) *ShiftRow* (Pergeseren byte per baris) *MixColumn* (Operasi perkalian GF(2) per kolom)

Pencampuran subkey (dengan XOR)

Transformasi : *ByteSub* dan *ShiftRow*

Brute Force

Brute Force adalah sebuah teknik serangan terhadap sebuah sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin. Pendekatan ini pada awalnya merujuk pada sebuah program komputer yang mengandalkan kekuatan pemrosesan komputer dibandingkan kecerdasan manusia (Pramudita 2011).

Secara sederhana, menebak *password* dengan mencoba semua kombinasi karakter yang mungkin. *Brute force attack* digunakan untuk menjebol akses ke suatu *host* (*server/ workstation/ network*) atau kepada data yang terenkripsi. Metode ini dipakai para cracker untuk mendapatkan account secara tidak sah, dan sangat berguna untuk memecahkan enkripsi. *Brute Force attack* tidak serumit dan *low-tech* seperti algoritma *hacking* yang berkembang sekarang.

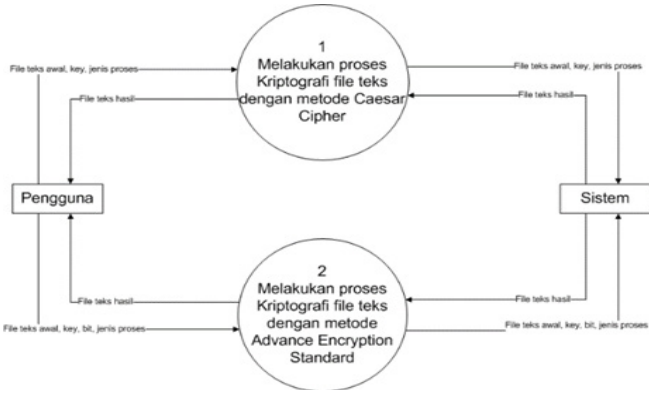
Seorang penyerang hanya cukup menebak nama dan kombinasi *password* sampai menemukan yang cocok. Mungkin terlihat bahwa *brute force attack* atau *dictionary attack* tidak mungkin berhasil. Namun yang mengejutkan, kemungkinan berhasil *brute force attack* menjadi membaik ketika *site* yang ingin diretasi tidak dikonfigurasikan dengan baik.

METODOLOGI PENELITIAN

Aliran data secara keseluruhan dari sistem terdapat pada Gambar 2 dan 3. Gambar 2 berupa diagram konteks atau DFD (Data Flow Diagram level 1.

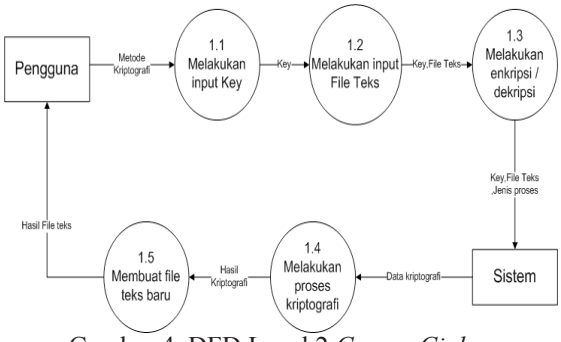
Gambar 2. DFD Level 0

Pada Gambar 3 terdapat dua proses, yaitu proses kriptografi dengan metode AES dan satunya dengan metode *Caesar Cipher*.

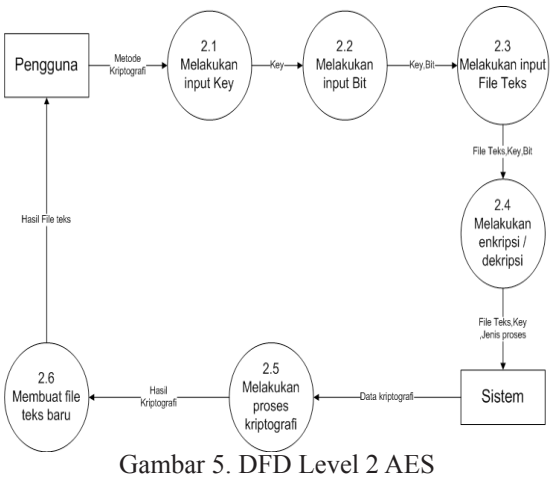


Gambar 3. DFD Level 1

Untuk proses detail yang terdiri urutan proses kriptografi dari *Caesar Cipher* terdapat di Gambar 4.



Gambar 4. DFD Level 2 *Caesar Cipher*



Gambar 5. DFD Level 2 AES

Gambar 5 diatas adalah DFD untuk metode AES.

Gambar 6.Halaman *Caesar Cipher*

Proses enkripsi/ dekripsi file teks dengan metode *Caesar Cipher* terdapat di Gambar 6. Dilakukan input *key* untuk menentukan jumlah pergeseran. Hasil pemili-

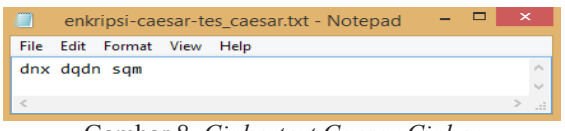
han file teks (.txt) dari *input file* akan tampil di *input text*. Pada form ini terdapat tombol *Encrypt* untuk enkripsi dan tombol *Decrypt* untuk dekripsi. Proses kriptografi dilakukan dengan menggeser setiap huruf dari isi file teks sejumlah *key* yang diinput sesuai dengan pilihan tombol *Encrypt* atau *Decrypt*.

Gambar 7. Halaman AES

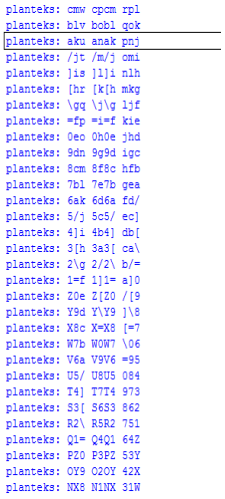
Gambar 7 berfungsi untuk melakukan enkripsi/dekripsi file teks dengan metode AES. Pengguna perlu melakukan input *key*, input bit dan input file teks. Setelah itu, pengguna memilih proses kriptografi yakni enkripsi dan dekripsi.

HASIL PENELITIAN DAN PEMBAHASAN

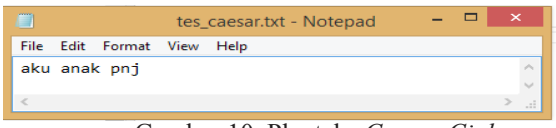
Pengujian keamanan data *Caesar Cipher* dilakukan dengan metode *Brute Force Attack* dimana teknik serangan dilakukan dengan menggunakan percobaan terhadap seluruh elemen.



Gambar 8. *Ciphertext Caesar Cipher*



Gambar 9. Uji keamanan *Caesar Cipher*



Gambar 10. Planteks *Caesar Cipher*

Efisiensi Waktu

Pengujian efisiensi *Caesar Cipher* dilakukan menggunakan tiga jenis file teks dengan ukuran berbeda. Hasil pengukuran terdapat pada Tabel 1.

Tabel 1. Efisiensi *Caesar Cipher*

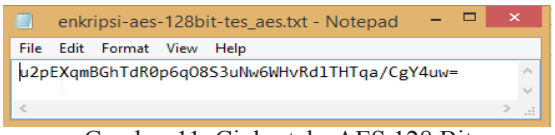
File Teks	*Size* awal	*Size* akhir	Waktu enkripsi
A	100 KB	100 KB	2300 ms
B	500 KB	500 KB	6100 ms
C	1000 KB	1000 KB	11400 ms

Pada pengujian halaman AES, dilakukan pengujian keamanan data dan efisiensi. Metode AES memiliki tiga *bit* yakni 128 *bit*, 192 *bit* dan 256 *bit*. Oleh sebab itu, setiap pengujian keamanan data dan efisiensi dilakukan sebanyak tiga kali.

Keamanan data

Pengujian keamanan data AES dilakukan dengan metode *Brute Force Attack*. Pengujian pertama dilakukan dengan

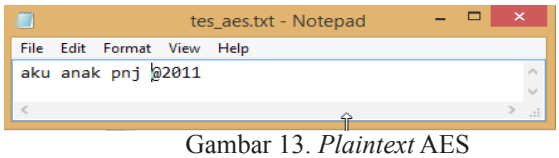
128 *Bit*. Untuk pengujian 192 bit dan 256 bit juga didapatkan hasil yang sama.



Gambar 11. Cipherteks AES 128 Bit

```
planteks: t1oDWplAFgScQ9o5pN7R2tMv5VGuQckSGSp/]BfX3tv0
planteks: sZnCVokzEfRbP8n4oM6Q1sLu4UFtPbjRFRo][AeW2su9
planteks: rYmBUnjyDeQaO7m3nL5PZrKt3TEsOaiQEQn[\zdV1rt8
planteks: qXlATmixCdP/N6l2mK4OYqJs2SDrN/hPDPm\=ycUZqs7
planteks: pWkzSlhwBcO]M5k1lJ3NXpIr1RCqM]gOCOl=0xbTYpr6
planteks: oVjyRkgvAbN[L4jZkI2MWoHqZQBpL[fNBNk09waSXoq5
planteks: nUixQjfuzaM\K3iYjH1LVnGpYPAoK\eMAMj98v/RWnp4
planteks: mThwPiety/L=J2hXiGZKUmFoXOznJ=dLzLi87u]QVmo3
planteks: lSgvOhdsx]K0I1gWhFYJTlEnWNymI0cKyKh76t[PUln2
planteks: kRfuNgcrw[J9HZfVgEXISkDmVMxlH9bJxJg65s\OTkm1
planteks: jQetMfbqv\I8GYeUfDWHRjClULwkG8aIwIf54r=NSj1Z
planteks: iPdsLeapu=H7FXdTeCVGQiBkTKvjF7/HvHe43q0MRikY
planteks: hOcrKd/ot0G6EWcSdBUFPhAjSJuiE6]GuGd32p9LQhjX
planteks: gNbqJc]ns9F5DVbRcATEOgziRIthD5[FtFc21o8KPgiW
planteks: fMapIb[mr8E4CUaQbzSDNfyhQHsgC4\EsEb1Zn7JOfhV
planteks: eL/oHa\lq7D3BT/PayRCMexgPGrfB3=DrDaZYm6INegU
planteks: dK]nG/=kp6C2AS]O/xQBLdwfOFqeA20CqC/YXl5HMdfT
planteks: cJ[mF]0jo5B1zR[N]wPAKcveNEpdz19BpB]XWk4GLceS
planteks: bI\lE[9in4AZyQ\M[vOzJbudMDocyZ8AoA[WVj3FKbdR
planteks: aH=kD\8hm3zYxP=L\uNyIatcLCnbxY7znz\VUi2EJacQ
planteks: /GOjC=7gl2yXwO0K=tMxH/sbKBmawX6ymy=UTh1DI/bP
planteks: ]F9iB06fk1xWvN9J0sLwG]raJAl/vW5x1x0TSgZCH]aO
planteks: [E8hA95ejZwVuM8I9rKvF[q/Izk]uV4wkw9SRfYBG[/N
planteks: \D7gz84diYvUtL7H8qJuE\p]Hyj[tU3vjv8RQeXAF\]M
planteks: =C6fy73chXuTsK6G7pItD=o[Gxi\sT2uiu7QPdWzE=[L
planteks: 0B5ex62bgWtSrJ5F6oHsC0n\Fwh=rS1tht6POcVyD0\K
planteks: 9A4dw51afVsRqI4E5nGrB9m=Evg0qRZsgs5ONbUxC9=J
planteks: 8z3cv4Z/eUrQpH3D4mFqA8l0Duf9pQYrfr4NMaTwB80I
planteks: 7y2bu3Y]dTqPoG2C3lEpz7k9Cte8oPXqeq3ML/SvA79H
planteks: 6x1at2X[cSpOnF1B2kDoy6j8Bsd7nOWpdp2LK]Ruz68G
planteks: 5wZ/s1W\bRoNmEZA1jCnx5i7Arc6mNVoco1KJ[Qty57F
planteks: 4vY]rZV=aQnMlDYzZiBmw4h6zqb5lMUnbnZJI\Psx46E
```

Gambar 12. Uji Keamanan AES 128 Bit



Gambar 13. *Plaintext* AES

Efisiensi

Pengujian efisiensi AES dilakukan menggunakan tiga jenis file teks dengan ukuran berbeda yakni: file teks A (*Size* = 100 KB), B (*Size* = 500 KB), C (*Size* = 1000 KB). Hasil pengujian terdapat di Tabel 2.

Tabel 2. Efisiensi AES

File	*Size*		Waktu enkripsi		
	awal	Akhir	128 bit	192 bit	256 bit
A	100 KB	133 KB	1100 ms	1400 ms	1600 ms
B	500 KB	667 KB	2800 ms	3000 ms	3300 ms
C	1000 KB	1333 KB	5000 ms	6600 ms	7600 ms

Metode *Caesar Cipher* dan AES memiliki perbedaan pada tingkat keamanan data dan efisiensi. Untuk itu, akan dilakukan analisa pada tingkat keamanan data dan efisiensi. Masing–masing metode memiliki karakteristik dalam mengamankan data.

Keamanan Data

Hasil uji keamanan data *Caesar Cipher* memberikan hasil bahwa cipherteks dapat dipecahkan dengan metode *Brute Force Attack*. Hal ini ditandai dengan munculnya planteks awal *Caesar Cipher*. Sedangkan pada *Advance Encryption Standard* memberikan hasil bahwa cipherteks tidak dapat dipecahkan dengan metode *Brute Force Attack*. Hal ini ditandai dengan tidak munculnya planteks awal AES.

Berdasarkan analisa keamanan data, metode Advance Encryption Standard lebih aman dari *Caesar Cipher* karena cipherteks tidak dapat dipecahkan dengan metode *Brute Force Attack*. Hal ini terjadi karena metode Advance Encryption Standard menggunakan bit/round sehingga lebih aman sedangkan metode *Caesar Cipher* menggunakan proses pergeseran huruf.

Efisiensi Waktu

Masing–masing metode memiliki perbedaan pada efisiensi waktu yang dihasilkan. Dari Tabel 1 dan 2 diperoleh perhitungan efisiensi waktu yang terdapat di Tabel 3.

Tabel 3. Perhitungan Efisiensi Waktu

File	Cipher	Rata-rata AES	Selisih Waktu
A	2300	1366,67	933,33
B	6100	3033,33	3066,67
C	11400	6400	5000

Rata–rata perbedaan waktu enkripsi waktu enkripsi metode *Caesar Cipher* dan AES pada file teks A, B dan C adalah:

= 3000 ms

Dari hasil perhitungan, metode Advance Encryption Standard lebih unggul dari metode *Caesar Cipher* dengan rata–rata perbedaan waktu sebesar 3000 ms.

Ukuran

Masing–masing metode memiliki perbedaan pada efisiensi ukuran yang dihasilkan. Berdasarkan analisa efisiensi ukuran pada file teks A, B dan C di Tabel 1 dan 2, metode *Caesar Cipher* lebih unggul dengan perubahan ukuran 0% sedangkan metode Advance Encryption Standard mengalami perubahan ukuran 33%.

PENUTUP

Berdasarkan analisa data yang telah dilakukan pada sistem, dapat disimpulkan bahwa dalam hal keamanan data, metode Advance Encryption Standard lebih aman dari metode *Caesar Cipher* karena cipherteks tidak dapat dipecahkan dengan metode *Brute Force Attack*. Hal ini terjadi karena metode Advance Encryption Standard menggunakan bit/round sehingga lebih aman sedangkan metode *Caesar Cipher* menggunakan proses pergeseran huruf.

Dalam hal efisiensi waktu, metode Advance Encryption Standard lebih unggul dari metode *Caesar Cipher* dengan rata–rata perbedaan waktu sebesar 3000 ms. Hal ini terjadi karena proses kriptografi Advance Encryption Standard menggunakan matriks sehingga lebih efisien sedangkan metode *Caesar Cipher* menggunakan proses pergeseran huruf.

Dalam hal efisiensi ukuran, metode *Caesar Cipher* lebih unggul dengan perubahan ukuran sebesar 0% sedangkan metode Advance Encryption Standard mengalami perubahan ukuran sebesar 33%. Hal ini terjadi karena pada *Caesar Cipher*, jumlah karakter output sama dengan jumlah karakter input sedangkan pada Advance Encryption Standard, jumlah karakter output lebih banyak dari jumlah karakter input.

Aplikasi ini dirancang untuk membandingkan dua metode kriptografi. Untuk pengembangan selanjutnya, diharapkan dapat dibandingkan lebih dari dua metode kriptografi sehingga didapatkan hasil yang lebih luas dan akurat. Dapat juga digunakan parameter pengukuran yang lebih bervariasi.

UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Jurusan Teknik Informatika dan Komputer Politeknik Negeri Jakarta atas dukungannya pada penelitian ini.

DAFTAR PUSTAKA

Sitinjak, Suriski, Yuli Fauziah, and Juwairiah. "Aplikasi Kriptografi File Menggunakan Algoritma Blowfsh." Yogyakarta, 2011.

Akbar, Muhammad. "Penggunaan Teknik Kriptografi Hybrid untuk Pengamanan SMS pada Perangkat Android." *Jurnal TICOM* Vol.2 , no. No. 2 (Januari 2014): 80-89.

Andri M, Yuli. *Implementasi Algoritma Kriptografi DES, RSA dan Algoritma Kompresi LZW pada Berkas Digital.* Universitas Sumatera Utara, 2009.

Fairuzabadi, Muhammad. "Implementasi Kriptografi Klasik Menggunakan Borland Delphi." *Jurnal Dinamika Informatika* Volume 4, no. Nomor 2 (September 2010): 65 – 78.

Haryanto, T, M Apriani, and T Sefyanto. "Peran Algoritma Caesar Cipher dalam Membangun Karakter Akan Kesadaran Keamanan Informasi." Yogyakarta, November 2012.

Lusiana, Veronica. "Implementasi Kriptografi pada File Dokumen Menggunakan Algoritma AES-

128." *Jurnal Dinamika Informatika* Vol , no. No 2 (2011).

Manan, S, and A Subari. "Implementasi AES CIPHER CLASS Untuk Enkripsi URL Di Informasi Akademik Fakultas Teknik Universitas Diponegoro." *Jurnal Sistem Komputer Universitas Diponegoro*, 2014.

Munawar. "Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris." *Jurnal Komputer dan Informatika (KOMPUTA) 11* Volume. 1, no. Edisi. I (Maret 2012).

Pramudita, K E. "Brute Force Attack dan Penerapannya pada Password Cracking." 2011: Jurnal STEI ITB.

Rachman, Arif Kurnia. "Perbandingan Mode Chiper Electronic Code Book dan Chiper Block Chaining dalam Pengamanan Data", , :." *Jurnal Teknologi* Volume 3, no. No 1 (Juni 2010): 84-89.

Sasongko, Jati. "Pengamanan Data Informasi menggunakan Kriptografi Klasik Pengamanan Data Informasi menggunakan Kriptografi Klasik." *Jurnal Teknologi Informasi DINAMIK* Volume X, no. No. 3 (September 2005): 160-167.

"Surian, Didi." Algoritma Kriptografi AES Rijndael",." *TESLA Jurnal Teknik Elektro Vol. 8 No. 2, 97 – 101 (Oktober 2006)* Vol. 8, no. No. 2 (Oktober 2006): 97 – 101.

Wahana Komputer. *Memahami Model Enkripsi & Security Data.* Yogyakarta: Andi, 2003.

Wirdasari, Dian, ". "Prinsip Kerja Kriptografi dalam Mengamankan Informas." *Jurnal SAINTIKOM* Vol. 2, no. No.2 (Agustus 2008): 174-184.