# Analisis AES Rijndael terhadap DES

Michell Setyawati Handaka / 135 08 045[1]
*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia*
[1]*if18045@students.if.itb.ac.id*

***Di samping serangan XSL, sebuah teknik kriptanalisis terhadap cipher blok dengan sistem persamaan* overdefined *– oleh Nicolas T. Courtois dan Josef Pieprzyk–, algoritma Rijndael dipercaya sebagai algoritma enkripsi simetris berbasis blok yang secara praktis dapat diandalkan untuk memberikan layanan kriptografi. Sebagai algoritma yang terpilih menjadi* Advanced Encryption Standar *menggantikan DES, Rijndael tentulah memiliki sejumlah keunggulan yang menyebabkan algoritma ini dianggap layak menggantikan DES dan turunannya (seperti 3DES).***

***Sekalipun serangan yang berhasil dilakukan terhadap DES merupakan serangan yang mahal dan secara praktis tidak akan dilakukan dalam kehidupan sehari-hari sehingga banyak pihak yang tetap berani memberikan klaimnya mengenai keamanan yang ditawarkan, algoritma Rijndael dikatakan memenangkan pertempuran keamanan secara mutlak bahkan jika dibandingkan dengan 3DES.***

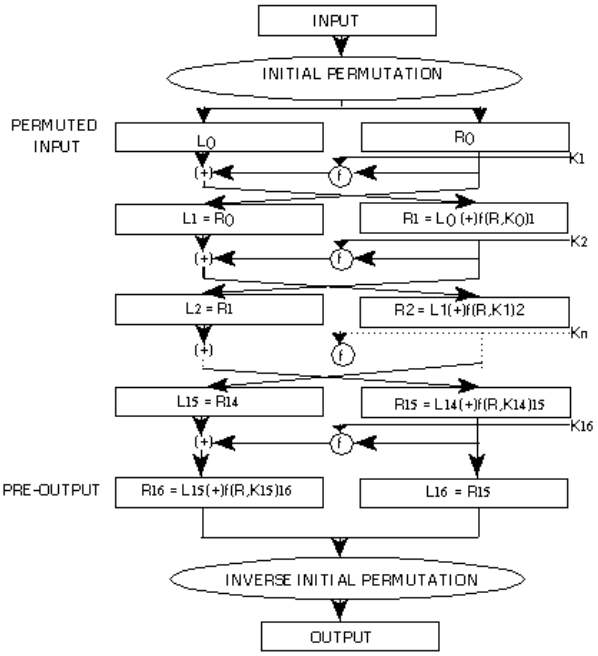
***Sebagaimana algoritma kriptografi modern yang tidak merahasiakan algoritmanya, kerahasiaan Rijndael hanyalah terletak pada kunci. Pertanyaannya adalah struktur yang bagaimana yang dapat menawarkan tingkat keamanan yang tinggi dengan kondisi bahwa struktur tersebut umum diketahui karena dijadikan standar, dan mengapa struktur tersebut aman? Untuk menjawabnya, akan dicoba dilakukan analisis terhadap struktur algoritma Rijndael yang telah distandarisasi menjadi AES.***

***Untuk menganalisa letak kelebihan dan kekuatan stuktur algoritma Rijndael, akan dilakukan studi struktur relatif terhadap algoritma sejenis, yaitu DES. Analisis akan dilakukan dengan membandingkan stuktur kedua algoritma ini dan akan dicoba untuk ditarik suatu kesimpulan dari letak perbedaan struktur tersebut apa yang menyebabkan suatu algoritma enkripsi kunci simetri berbasis blok menjadi algoritma yang sulit untuk dipecahkan.***

***DES, AES, Rijndael,Cipher Blok Kunci Simetri***

## IV. DATA ENCRYPTION STANDARD [1]

Secara umum spesifikasi dari *Data Encryption Algorithm* adalah seperti yang dijelaskan berikut ini, yaitu baik setiap *block* data maupun kunci berukuran masing-masing sebesar 64 bit. Proses enkripsi dilakukan dengan melewatkan pesan ke dalam ***I**nitial **P**ermutation*, komputasi kompleks fungsi cipher *f* yang bergantung kepada kunci internal yang dibangkitkan oleh fungsi penjadwalan kunci *KS*, dan kemudian terakhir adalah $IP^{-1}$. Sementara itu, proses dekripsi mengikuti jalur yang sama mengingat sifat simetris dan reversible dari DEA.




**Gambar 1. Komputasi Proses Enkripsi**

*IP* adalah suatu matriks permutasi dengan input berupa data 64 bit yang menghasilkan susunan baru data 64 bit berdasarkan pemetaan bit-bit tersebut menggunakan matriks. Angka *j* pada matriks posisi ke-*i* menyatakan bahwa bit output pada posisi ke-*i* berasal dari bit input pada posisi ke-*j*. $IP^{-1}$ adalah inversi dari matriks *IP*.

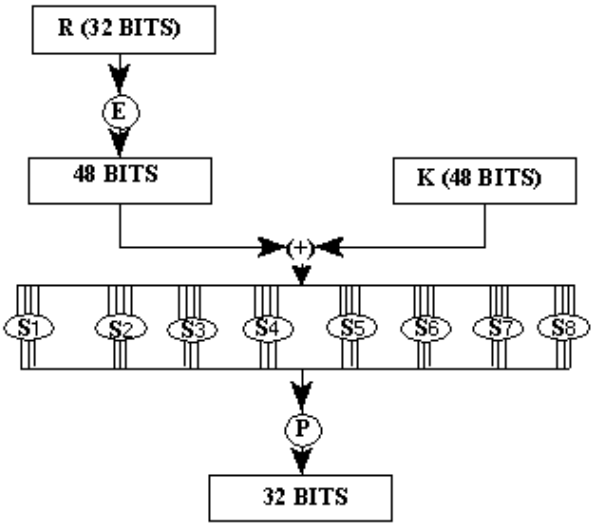
Fungsi komputasi kompleks diiterasi sebanyak *16* kali masing-masing menggunakan kunci internal yang berbeda-beda $(K_i | i = [1..16])$, - *i* menyatakan iterasi ke-*i* -, yang merupakan hasil komputasi fungsi penjadwalan kunci *KS* terhadap kunci yang dimasukan oleh pengguna. Untuk setiap iterasi berlaku : output dari iterasi ke-*i* akan menjadi input dari iterasi ke-(*i+1*). Dimana input dari iterasi pertama adalah output dari *IP*.

Dengan demikian jelaslah bahwa input dari fungsi komputasi kompleks ini adalah data berukuran 64 bit. Data ini dipecah menjadi 2 bagian sama besar, dengan kata lain keduanya 32 bit, **L** dan **R** dimana berlaku :

$L_n = R_{n-1}$,

$R_n = L_{n-1} \oplus f(R_{n-1}, K_n)$ dimana *n* menyatakan iterasi ke-*n*

Berbeda dengan *block* **L** dan **R** yang masing-masing berukuran 32 bit, *block* data pada **K** berukuran 48 bit.

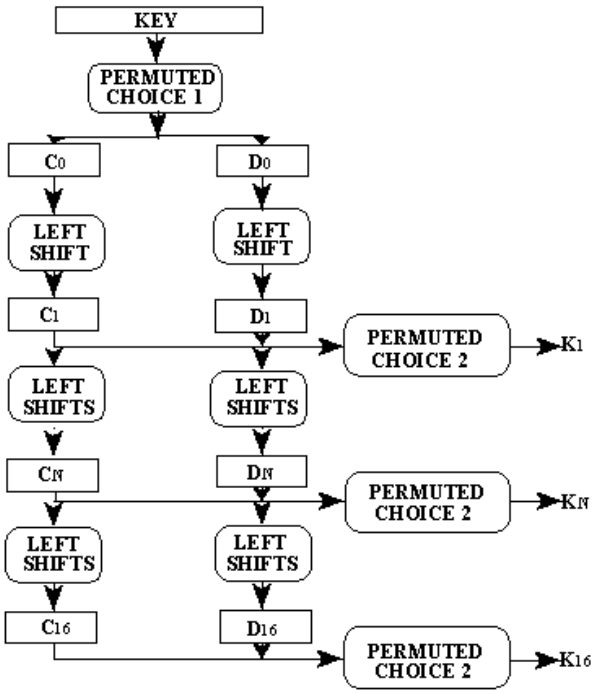



**Gambar 2. Fungsi Cipher *f***

*E* adalah sebuah matriks ekspansi dengan karakteristik seperti *IP* hanya saja menerima input 32 bit dan menghasilkan output 48 bit. Dengan kata lain terdapat bit-bit input yang digandakan untuk menghasilkan output.

Sementara itu, matriks fungsi seleksi $S_i$ menerima 6 bit input dan menghasilkan 4 bit output berdasarkan matriks yang berbeda-beda untuk setiap *i* yang berbeda. Dari diagram jelas terlihat bahwa hasil operasi XOR dari *E(R)* dan *K* yang menghasilkan 48 bit data dipecah 8 sama bagian menjadi masing-masing 6 bit yang kemudian akan masuk ke dalam matriks $S_i$ dan hasil penggabungan 8 buah *block* 4 bit ini akan menjadi data 32 bit. Matriks *S* memetakan data 6 bit $d_1d_2d_3d_4d_5d_6$ menjadi data 4 bit yang berada pada baris ke $d_1d_6$ kolom $d_2d_3d_4d_5$.

Matriks fungsi permutasi *P* seperti juga pada *IP* melakukan permutasi terhadap 32 bit-bit input dan menghasilkan 32 bit data output.




**Gambar 3. Fungsi Penjadwalan Kunci *KS***

Untuk fungsi penjadwalan kunci, terdapat matriks *PC-1*, Tabel Pergeseran Kiri, dan matriks *PC-2*. *PC-1* terdiri dari 2 bagian yang masing-masing adalah matriks 28 sel. Dengan kata lain, dari 64 bit kunci, hanya 56 di antaranya yang digunakan untuk membangkitkan kunci internal sementara sisanya digunakan sebagai bit paritas. *C* adalah hasil permutasi menggunakan matriks *PC-1* bagian *1;* sementara *D* adalah hasil permutasi menggunakan matriks *PC-1* bagian *2*. Keduanya adalah data 28 bit. Sementara *PC-2* adalah matriks permutasi seperti *IP* yang menerima 56 bit data dan menghasilkan 48 bit data.

## V. SERANGAN PADA **DES** [2]

Beberapa serangan telah dilakukan terhadap DES, baik secara praktis maupun teoritis. Adapun semua serangan ini tidak ada yang efektif dan secara teknis membutuhkan biaya yang relatif sangat mahal dibandingkan dengan pencapaian yang didapatkan. Akan tetapi dengan berhasilnya suatu serangan yang benar-benar menembus jaringan pertahanan DES ini, secara otomatis DES dikategorikan sebagai obsolet.

**SERANGAN PRAKTIS** : BRUTE FORCE ATTACK

Serangan ini dilakukan dengan mencoba seluruh kemungkinan kunci pada DES yang secara praktis terdiri atas 56 bit. Dengan kata lain terdapat $2^{56}$ kemungkinan kunci untuk suatu cipherteks tertentu.

Pada tahun 1977 sebuah proposal dari Diffie dan Hellman mengklaim sebuah mesin seharga US$20 juta dapat menjebol pertahanan DES hanya dalam satu hari. Berikutnya pada tahun 1993, Wiener menawarkan sebuah proposal mengenai mesin seharga US$1 juta yang dapat memecahkan kunci DES hanya dalam 7 jam. Pada tahun 1997 sebuah kompetisi berhadiah US$10.000 berhasil memecahkan cipher DES menggunakan komputer yang sedang menganggur pada jaringan internet atas nama tim DESCHALL Project yang dipimpin oleh Rocke Verser, Matt Curtin, dan Justin Dolske. Pada tahun 1998 EFF menghabiskan US$ 250.000 untuk menciptakan sebuah mesin yang dapat memecahkan DES dalam waktu sekitar melebihi sedikit dari 2 hari hanya untuk membuktikan bahwa secara praktis dan teoritis DES adalah cipher yang dapat dipecahkan. Pada 2006 US$10.000 dapat memecahkan DES dalam waktu kurang dari 1 hari.

**SERANGAN TEORITIS**

Sekalipun secara praktis tidak dimungkinkan, secara teoritis terdapat beberapa serangan yang dapat dilakukan terhadap DES, antara lain adalah sebagai berikut ini, yakni :

- Differential Cryptanalysis [1980, Eli Biham & Adi Shamir] membutuhkan sekitar $2^{47}$ plainteks diketahui untuk memecahkan DES.
- Linear Cryptanalysis [1993, Mitsuru Matsui] bekerja pada $2^{43}$ plainteks diketahui, dan Multiple Linear Cryptanalysis [1994, Kaliski & Robshaw; 2004, Biryukov *et al.*; 2000, Knudsen dan Mathiassen; 2001, Junod]

mereduksinya menjadi $2^{39}$-$2^{41}$.

- Improved Davies' Attack [1980-an, Donald Davies; 1997, Biham dan Biryukov] memiliki kompleksitas $2^{50}$ dengan tingkat keberhasilan mencapai 51%.

## VI. ADVANCED ENCRYPTION STANDARD [3], [4]

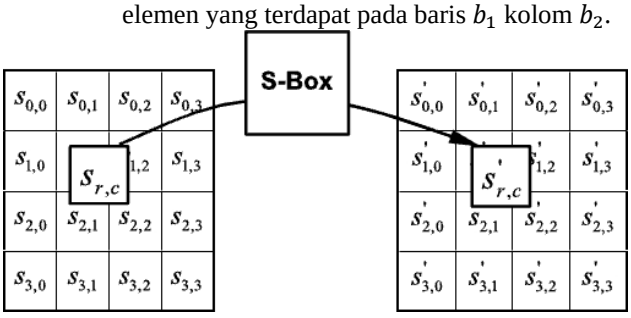
Berbeda dengan DEA, Algoritma Rijndael tidaklah menggunakan jaringan feistel di dalamnya, sebaliknya setiap trasformasi putaran terdiri atas 3 buah lapisan seragam tetapi berbeda yang dapat dibalik dengan fungsinya masing-masing.

- Lapisan *Linear-Mixing*
  menjamin tingkat difusi adalah tinggi dengan banyaknya putaran.
- Lapisan *Non-Linear*
  aplikasi paralel dari S-Box yang memiliki properti nirlanjar optimum pada kasus terburuk.
- Lapisan *Key-Addition*
  operasi XOR sederhana kunci internal terhadap state sementara.

Secara umum spesifikasi dari Algoritma Rijndael adalah seperti yang dijelaskan berikut ini, yaitu state awal yang merupakan matriks[baris, kolom] berukuran 4 x (panjang *block* / 32) dibangun dari plainteks secara menurun. Matriks kunci dibangun menggunakan cara yang sama dengan catatan bahwa ukuran *block* data dan kunci mungkin saja berbeda.

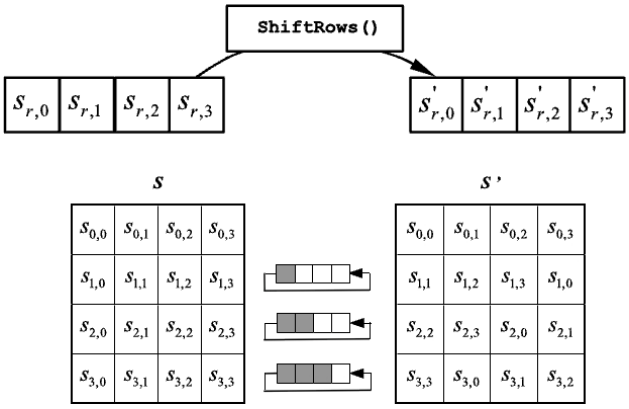
Setiap bit data akan melalui transformasi sebanyak sedikitnya 10 kali (untuk *block* data 128bit, dan bertambah 1 untuk masing-masing 32 bit tambahan) sebelum memasuki putaran final. Transformasi putaran pada Rijndael terdiri atas komponen transformasi sebagai berikut ini :

- Transformasi *SubBytes*
  adalah transformasi affine atas invers multiplikasi medan terbatas GF($2^8$) atas GF(2) dengan elemen {0, 0} dipetakan pada dirinya sendiri. Secara sederhana operasi ini dapat dilakukan dengan menggantikan elemen pada matriks dengan hasil pementaannya dari matriks S-Box. Elemen $b_1 b_2$ dipetakan ke elemen yang terdapat pada baris $b_1$ kolom $b_2$.



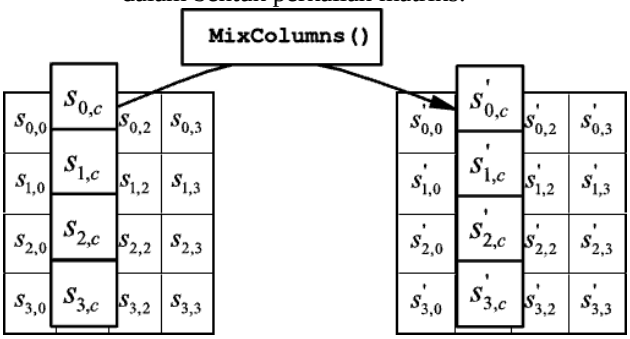

**Gambar 4. Transformasi *SubBytes***

- Transformasi *ShiftRows*
  adalah pergeseran sel matriks secara siklis ke kiri sebanyak posisi baris.



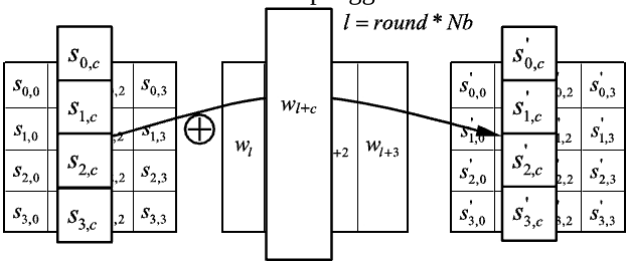

**Gambar 5. Transformasi *SubBytes***

- Transformasi *MixColumns*
  adalah operasi kolom per kolom yang memperlakukan setiap kolomnya sebagai polinomial suku empat yang dikalikan dengan polinomial berkoefisien terdefinisi dan konstanta tertentu yang dapat dinyatakan dalam bentuk perkalian matriks.




**Gambar 6. Transformasi *MixColumns***

- Transformasi *AddRoundKey*
  adalah proses XOR setiap sel pada state dengan sel dari kunci internal / kunci putaran yang dibangkitkan menggunakan algoritma penjadwalan kunci dari kunci eksternal yang dimasukkan oleh pengguna.

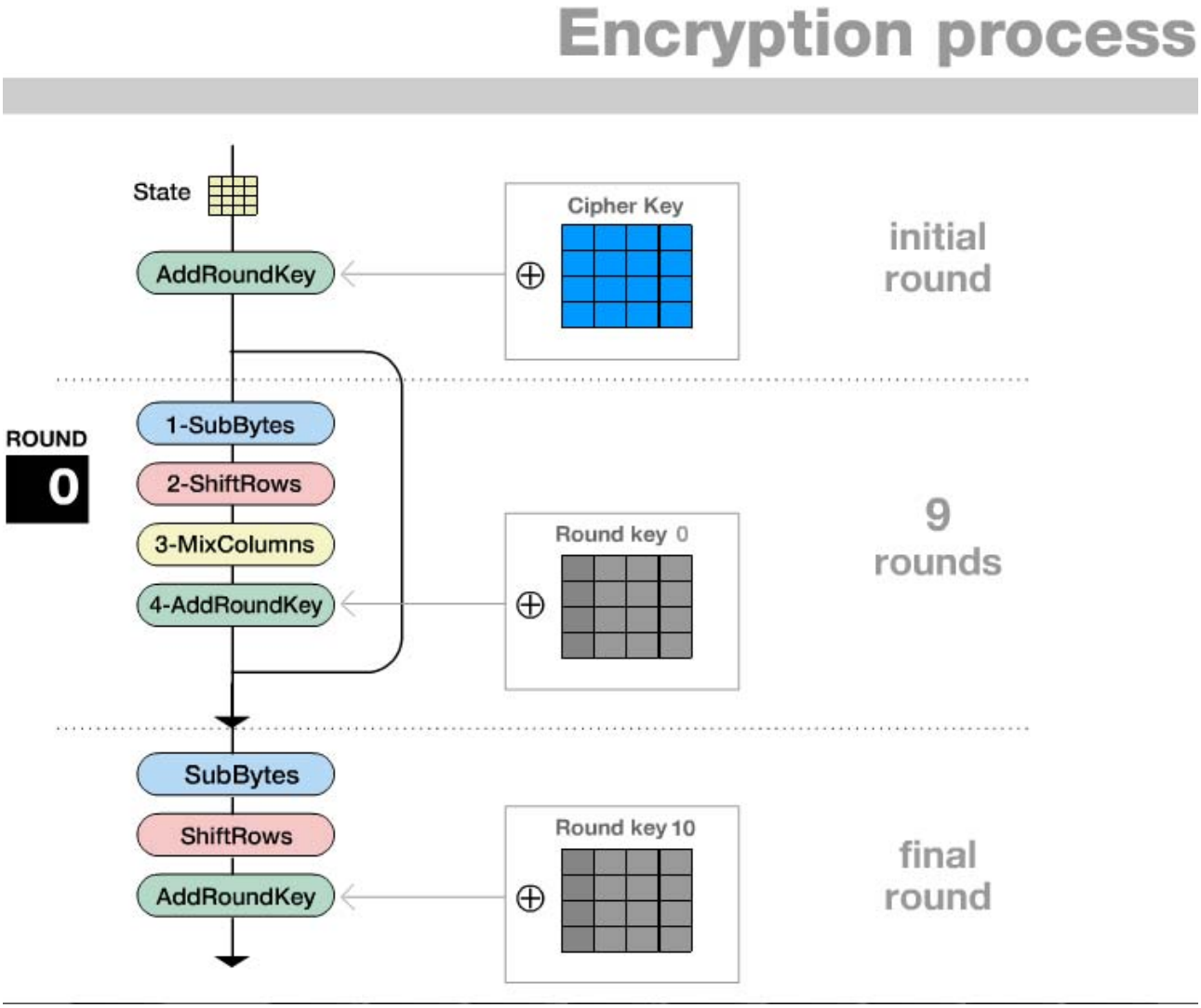



**Gambar 7. Transformasi *AddRoundKey***

Untuk proses dekripsi, dilakukan secara kebalikannya menggunakan inversi dari masing-masing transformasi dengan properti sebagai berikut :

- Transformasi *SubBytes* dan *ShiftRows* bersifat komutatif, demikian pula berlaku terhadap inversinya.
- Baik Transformasi *MixColumns* maupun inversinya adalah lanjar terhadap input kolom sehingga berlaku hukum distributif terhadap Transformasi *RoundKey*.

Secara umum, skema enkripsi AES ditunjukkan oleh Gambar 8 di bawah ini.




**Gambar 8. Skema Enkripsi**

Seperti yang terlihat pada gambar, putaran final adalah sama seperti transformasi putaran tanpa transformasi MixColumns.

Untuk pembangkitan kunci internal menggunakan penjadwalan kunci, dilakukan hal-hal sebagai berikut ini terhadap kolom terpilih –pertama kali dipilih kolom ke-4 dari matriks kunci untuk pengisian kolom ke-5– :

- *RotWord*
  pergeseran kolom secara siklis ke atas.
- *SubBytes*
  substitusi sel kunci seperti substitusi sel data menggunakan S-Box.
- XOR
  operasi ini melakukan XOR terhadap hasil operasi sebelumnya dengan kolom ke-(*n-4*) dan kolom pertama dari Rcon yang tersisa, dan membuang kolom tersebut dari Rcon.

Operasi ini dilakukan secara berulang untuk mendapatkan kolom ke-(*4m+1*) dari kunci. Sementara kolom lainnya didapatkan dengan melakukan operasi XOR kolom ke-(*n-1*) dan kolom ke-(*n-4*) dari kunci.

## VII. SERANGAN PADA **AES** [5], [6], [7]

Secara matematis berbagai pembuktian telah dilakukan dan ditunjukkan bahwa AES dapat bertahan menghadapi serangan-serangan berikut ini :

- *Differential Cryptanalisis* dan *Linear Cryptanalysis*,
- *Truncated Differentials*,
- *The Square Attacks, dan*
- *Interpolation Attacks*,

serta lulus uji terhadap sifat simetrik dan kunci lemah. Sekalipun demikian, berbagai serangan secara praktis dan teoritis dicoba dilakukan dengan berbagai klain yang hingga saat ini masih tidak terbukti efektif menghadapi AES putaran kunci penuh.

Kendatipun demikian, sebuah serangan terhadap cipher blok dengan sistem persamaan *overdefined*, XSL, tidak dapat dibuktikan tidak efektif terhadap algoritma Rijndael. Bahkan percobaan pada *baby* Rijndael, sebuah semi cipher putaran tidak penuh dibuktikan berhasil. Dikatakan pula, dengan metoda tersebut, Rijndael terbukti menjadi yang terlemah dari kelima kandidat AES.

## VIII. ANALISIS

### *A. Karakteristik DES*

Ukuran *block* adalah 64 bit dan bekerja pada mode bit. Operator yang digunakan adalah XOR sehingga menjamin keterbatasan ruang lingkup area medan interval biner.

Penerapan prinsip *diffusion* dari Shanon pada DES akan bergantung kepada mode dimana DES dijalankan. Sementara penerapan prinsip *confussion* dilakukan dengan cara substitusi seleksi maupun transposisi permutasi dan pengacakan penerapan fungsi dimana kelakuan terhadap masing-masing bit yang berbeda tidak persis tepat selalu sama.

- Jumlah transposisi permutasi yang dialami oleh satu bit pada data adalah 1 + 16 * 2 + 1 = 34x.
- Jumlah sustitusi seleksi yang dialami oleh satu bit data adalah 16 * 1 = 16x.
- Jumlah operasi XOR pada satu bit data adalah 16 * 2 = 32x.
- Jumlah transposisi permutasi yang dialami oleh satu bit pada kunci adalah 3x.
- Tingkat ketergantungan satu bit data terhadap kunci adalah 16 operasi.

Prinsip cipher berulang diterapkan dalam iterasi sejumlah 16 kali dengan memanfaatkan jaringan feistel.

i. Kekuatan DES

Kekuatan DES terletak pada pemilihan matriks ekspansi *E*, matriks substitusi seleksi $S_{i,1\leq i\leq 16}$, dan matriks transposisi permutasi *P*. Dasar pemilihan pada DES sampai saat ini masih tidak dipublikasikan akan tetapi ternyata telah terbukti secara praktis efektif. Pemilihan yang salah dapat saja menjadi bumerang dan menyebabkan kelemahan terbesar untuk algoritma kriptografi modern berbasis transposisi dan substitusi terdefinisi yang dikenal sebagai karakteristik kunci lemah.

ii. Kelemahan DES

Kelemahan utama DES terletak pada panjang kuncinya yang relatif pendek dan sifat properti komplemen yang mana $E_k(P) = C \Leftrightarrow E_{\bar{k}}(\bar{P}) = \bar{C}$ yang berarti reduksi kemungkinan kunci menjadi setengahnya saja. DES juga dcatat memiliki 4 kunci lemah yang mana $E_k\big(E_k(P)\big) = P \Leftrightarrow E_k = D_k$ selain daripada 6 kunci semi-lemah yang mana $E_{k1}\big(E_{k2}(P)\big) = P \Leftrightarrow E_{k2} = D_{k1}$.

### *B. Karakteristik AES*

Ukuran *block* berkisar antara 128 bit hingga 256 bit dengan variasi pada angka 32 bit dan bekerja pada mode byte. Operator yang digunakan adalah operator penjumlahan, perkalian, dan perkalian dengan konstanta pada medan GF($2^8$) yang merupakan sebuah medan berhingga dengan koefisien derajat polinomial kurang dari 8.

Penerapan prinsip *diffusion* dari Shanon pada AES akan bergantung kepada mode dimana AES dijalankan. Sementara penerapan prinsip *confussion* dilakukan dengan cara substitusi pada ranah hexa maupun trasnposisi permutasi dan pengacakan penerapan fungsi dimana kelakuan terhadap masing-masing byte yang berbeda tidak persis tepat selalu sama.

- Jumlah transposisi permutasi yang dialami oleh satu byte pada data adalah minimum 9 * 1 + 1 = 10x.
- Jumlah sustitusi seleksi yang dialami oleh satu byte data adalah minimum 9 * 1 + 1 = 10x.
- Jumlah operasi penjumlahan pada satu byte data adalah minimum 1+ 9 * 1 + 1 = 11x.
- Jumlah operasi perkalian pada satu byte data adalah minimum 9 * 1 = 9x.
- Jumlah transposisi permutasi yang dialami oleh satu byte pada kunci adalah maksimum 1x.
- Jumlah substitusi seleksi yang dialami oleh satu byte pada kunci adalah maksimum 1x.
- Jumlah operasi pada satu byte kunci adalah maksmimum 2x.
- Tingkat ketergantungan satu byte data terhadap kunci adalah minimum 10 operasi.

Prinsip cipher berulang diterapkan dalam iterasi sejumlah minimum 9 kali tanpa memanfaatkan jaringan feistel.

i. Kekuatan AES

Kekuatan AES terletak pada karakteristik sifat dari medan GF($2^8$) dimana untuk setiap bilangan prima selalu terdapat sebuah medan tunggal terbatas yang unik sehingga seluruh representasi dari GF($2^8$) bersifat *isomorphic* dan pemilihan polinomial biner berderajat 8 m(x) bersifat ireducible –yakni tidak dapat dibagi oleh bilangan lain pada medan selain 1 dan dirinya sendiri, relatif prima terhadap medan–. Kekuatan ini didasari oleh operasi matematis yang kompleks dan membutuhkan sumber daya yang tidak sedikit untuk melakukan komputasi. Karena didasarkan pada persamaan matematis, AES dapat dengan mudah dibuktikan keamanannya. Akan tetapi pula, hal ini sekaligus adalah kelemahan terbesar dari AES karena dengan berhasilnya dipecahkan persamaan matematis yang mendasarinya secara otomatis seluruh sistem di dalam AES dapat ditembus dan dengan demikian barisan pertahanannya dapat dikatakan hancur berantakan, luluh lantak.

Berbeda dengan DES yang tidak diketahui dasar pemilihan berbagai fungsinya, AES menyediakan pembuktian yang lengkap mengenai dasar-dasar matematis atas pemilihan yang dilakukan sehingga menunjukkan kekuatannya dalam menghadapi berbagai serangan.

### *C. Perbandingan DES dan AES*

Berdasarkan hasil analisis yang dilakukan, dapat dibuat sebuah hipotesis yaitu bahwa hal yang paling berdampak terhadap tingkat keamanan kriptografi modern berbasis blok dengan karakteristik kunci simetri adalah panjang

dari kunci itu sendiri mengingat algoritma pada kriptografi jenis ini tidaklah dirahasiakan sehingga keamanan sepenuhnya bergantung kepada kunci. Karakteristik lainnya seperti prinsip *diffusion* dan *confusion* dari Shannon hanyalah berlaku untuk mempersulit cryptanalysis yang sebenarnya sudah sulit secara praktis. Dengan kata lain, kejaran utama dari suatu algoritma yang baik bukanlah kompleksitas strukturnya dan jumlah transposisi permutasi serta substitusi selektif yang dilakukan terhadap data maupun jumlah operasi dan kebergantungan kunci. Hal ini dapat dilihat dari kemenangan mutlak DES terhadap AES dari segi struktur dan kompleksitas. Adalah penting untuk dicatat bahwa terdapat struktur dan kompleksitas minimum yang harus dipenuhi oleh suatu algoritma tetapi bukan berarti algoritma yang mudah dan sederhana pasti tidak kuat.

### *D. Perbandingan Rijndael dan Kandidat AES, serta DES dan Turunannya*

Beberapa situs mencatat bahwa Rijndael tergolong sebagai yang terlemah di antara kelima kandidat AES akan tetapi merupakan yang paling baik dalam segi komleksitas waktu dan ruang karena sifatnya yang sederhana.

Sementara itu dikatakan DES menurunkan jumlah bit kunci untuk mengejar implementasi yang mangkus dan sangkir pada sepotong chip.

## IX. KESIMPULAN

Tingkat keamanan kriptografi modern berbasis blok dengan karakteristik kunci simetri terletak pada panjang kunci yang digunakan.

Untuk kriptografi komersil, performansi juga harus diperhitungkan tetapi tidak boleh menekan tingkat keamanan. Jika tingkat keamanan yang ditawarkan tidak berbeda jauh, algoritma yang paling cepat secara praktis, selain terbukti kokoh secara teoritis, akan menjadi pilihan yang lebih diutamakan.

## X. LAMPIRAN

**IP**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 58 | 50 | 42 | 34 | 26 | 18 | 10 | 2 |
| 60 | 52 | 44 | 36 | 28 | 20 | 12 | 4 |
| 62 | 54 | 46 | 38 | 30 | 22 | 14 | 6 |
| 64 | 56 | 48 | 40 | 32 | 24 | 16 | 8 |
| 57 | 49 | 41 | 33 | 25 | 17 | 9 | 1 |
| 59 | 51 | 43 | 35 | 27 | 19 | 11 | 3 |
| 61 | 53 | 45 | 37 | 29 | 21 | 13 | 5 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 | 7 |

**Gambar X-1. IP**

**$IP^{-1}$**

| | | | | | | | |
|---|---|---|---|---|---|---|---|
| 40 | 8 | 48 | 16 | 56 | 24 | 64 | 32 |
| 39 | 7 | 47 | 15 | 55 | 23 | 63 | 31 |
| 38 | 6 | 46 | 14 | 54 | 22 | 62 | 30 |
| 37 | 5 | 45 | 13 | 53 | 21 | 61 | 29 |
| 36 | 4 | 44 | 12 | 52 | 20 | 60 | 28 |
| 35 | 3 | 43 | 11 | 51 | 19 | 59 | 27 |
| 34 | 2 | 42 | 10 | 50 | 18 | 58 | 26 |
| 33 | 1 | 41 | 9 | 49 | 17 | 57 | 25 |

**Gambar X-2. $IP^{-1}$**

**E BIT-SELECTION TABLE**

| | | | | | |
|---|---|---|---|---|---|
| 32 | 1 | 2 | 3 | 4 | 5 |
| 4 | 5 | 6 | 7 | 8 | 9 |
| 8 | 9 | 10 | 11 | 12 | 13 |
| 12 | 13 | 14 | 15 | 16 | 17 |
| 16 | 17 | 18 | 19 | 20 | 21 |
| 20 | 21 | 22 | 23 | 24 | 25 |
| 24 | 25 | 26 | 27 | 28 | 29 |
| 28 | 29 | 30 | 31 | 32 | 1 |

**Gambar X-3. E**

**P**

| | | | |
|---|---|---|---|
| 16 | 7 | 20 | 21 |
| 29 | 12 | 28 | 17 |
| 1 | 15 | 23 | 26 |
| 5 | 18 | 31 | 10 |
| 2 | 8 | 24 | 14 |
| 32 | 27 | 3 | 9 |
| 19 | 13 | 30 | 6 |
| 22 | 11 | 4 | 25 |

**Gambar X-4. P**

**$S_1$**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 14 | 4 | 13 | 1 | 2 | 15 | 11 | 8 | 3 | 10 | 6 | 12 | 5 | 9 | 0 | 7 |
| 0 | 15 | 7 | 4 | 14 | 2 | 13 | 1 | 10 | 6 | 12 | 11 | 9 | 5 | 3 | 8 |
| 4 | 1 | 14 | 8 | 13 | 6 | 2 | 11 | 15 | 12 | 9 | 7 | 3 | 10 | 5 | 0 |
| 15 | 12 | 8 | 2 | 4 | 9 | 1 | 7 | 5 | 11 | 3 | 14 | 10 | 0 | 6 | 13 |

**$S_2$**

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 15 | 1 | 8 | 14 | 6 | 11 | 3 | 4 | 9 | 7 | 2 | 13 | 12 | 0 | 5 | 10 |
| 3 | 13 | 4 | 7 | 15 | 2 | 8 | 14 | 12 | 0 | 1 | 10 | 6 | 9 | 11 | 5 |
| 0 | 14 | 7 | 11 | 10 | 4 | 13 | 1 | 5 | 8 | 12 | 6 | 9 | 3 | 2 | 15 |
| 13 | 8 | 10 | 1 | 3 | 15 | 4 | 2 | 11 | 6 | 7 | 12 | 0 | 5 | 14 | 9 |

$S_3$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 10 | 0 | 9 | 14 | 6 | 3 | 15 | 5 | 1 | 13 | 12 | 7 | 11 | 4 | 2 | 8 |
| 13 | 7 | 0 | 9 | 3 | 4 | 6 | 10 | 2 | 8 | 5 | 14 | 12 | 11 | 15 | 1 |
| 13 | 6 | 4 | 9 | 8 | 15 | 3 | 0 | 11 | 1 | 2 | 12 | 5 | 10 | 14 | 7 |
| 1 | 10 | 13 | 0 | 6 | 9 | 8 | 7 | 4 | 15 | 14 | 3 | 11 | 5 | 2 | 12 |

$S_4$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 7 | 13 | 14 | 3 | 0 | 6 | 9 | 10 | 1 | 2 | 8 | 5 | 11 | 12 | 4 | 15 |
| 13 | 8 | 11 | 5 | 6 | 15 | 0 | 3 | 4 | 7 | 2 | 12 | 1 | 10 | 14 | 9 |
| 10 | 6 | 9 | 0 | 12 | 11 | 7 | 13 | 15 | 1 | 3 | 14 | 5 | 2 | 8 | 4 |
| 3 | 15 | 0 | 6 | 10 | 1 | 13 | 8 | 9 | 4 | 5 | 11 | 12 | 7 | 2 | 14 |

$S_5$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 2 | 12 | 4 | 1 | 7 | 10 | 11 | 6 | 8 | 5 | 3 | 15 | 13 | 0 | 14 | 9 |
| 14 | 11 | 2 | 12 | 4 | 7 | 13 | 1 | 5 | 0 | 15 | 10 | 3 | 9 | 8 | 6 |
| 4 | 2 | 1 | 11 | 10 | 13 | 7 | 8 | 15 | 9 | 12 | 5 | 6 | 3 | 0 | 14 |
| 11 | 8 | 12 | 7 | 1 | 14 | 2 | 13 | 6 | 15 | 0 | 9 | 10 | 4 | 5 | 3 |

$S_6$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 12 | 1 | 10 | 15 | 9 | 2 | 6 | 8 | 0 | 13 | 3 | 4 | 14 | 7 | 5 | 11 |
| 10 | 15 | 4 | 2 | 7 | 12 | 9 | 5 | 6 | 1 | 13 | 14 | 0 | 11 | 3 | 8 |
| 9 | 14 | 15 | 5 | 2 | 8 | 12 | 3 | 7 | 0 | 4 | 10 | 1 | 13 | 11 | 6 |
| 4 | 3 | 2 | 12 | 9 | 5 | 15 | 10 | 11 | 14 | 1 | 7 | 6 | 0 | 8 | 13 |

$S_7$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 4 | 11 | 2 | 14 | 15 | 0 | 8 | 13 | 3 | 12 | 9 | 7 | 5 | 10 | 6 | 1 |
| 13 | 0 | 11 | 7 | 4 | 9 | 1 | 10 | 14 | 3 | 5 | 12 | 2 | 15 | 8 | 6 |
| 1 | 4 | 11 | 13 | 12 | 3 | 7 | 14 | 10 | 15 | 6 | 8 | 0 | 5 | 9 | 2 |
| 6 | 11 | 13 | 8 | 1 | 4 | 10 | 7 | 9 | 5 | 0 | 15 | 14 | 2 | 3 | 12 |

$S_8$

| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 13 | 2 | 8 | 4 | 6 | 15 | 11 | 1 | 10 | 9 | 3 | 14 | 5 | 0 | 12 | 7 |
| 1 | 15 | 13 | 8 | 10 | 3 | 7 | 4 | 12 | 5 | 6 | 11 | 0 | 14 | 9 | 2 |
| 7 | 11 | 4 | 1 | 9 | 12 | 14 | 2 | 0 | 6 | 10 | 13 | 15 | 3 | 5 | 8 |
| 2 | 1 | 14 | 7 | 4 | 10 | 8 | 13 | 15 | 12 | 9 | 0 | 3 | 5 | 6 | 11 |

**Gambar X-5. S**

PC-1

| | | | | | | |
|---|---|---|---|---|---|---|
| 57 | 49 | 41 | 33 | 25 | 17 | 9 |
| 1 | 58 | 50 | 42 | 34 | 26 | 18 |
| 10 | 2 | 59 | 51 | 43 | 35 | 27 |
| 19 | 11 | 3 | 60 | 52 | 44 | 36 |
| 63 | 55 | 47 | 39 | 31 | 23 | 15 |
| 7 | 62 | 54 | 46 | 38 | 30 | 22 |
| 14 | 6 | 61 | 53 | 45 | 37 | 29 |
| 21 | 13 | 5 | 28 | 20 | 12 | 4 |

**Gambar X-6. PC-1**

PC-2

| | | | | | |
|---|---|---|---|---|---|
| 14 | 17 | 11 | 24 | 1 | 5 |
| 3 | 28 | 15 | 6 | 21 | 10 |
| 23 | 19 | 12 | 4 | 26 | 8 |
| 16 | 7 | 27 | 20 | 13 | 2 |
| 41 | 52 | 31 | 37 | 47 | 55 |
| 30 | 40 | 51 | 45 | 33 | 48 |
| 44 | 49 | 39 | 56 | 34 | 53 |
| 46 | 42 | 50 | 36 | 29 | 32 |

**Gambar X-7. PC-2**

| Iteration Number | Number of Left Shifts |
|---|---|
| 1 | 1 |
| 2 | 1 |
| 3 | 2 |
| 4 | 2 |
| 5 | 2 |
| 6 | 2 |
| 7 | 2 |
| 8 | 2 |
| 9 | 1 |
| 10 | 2 |
| 11 | 2 |
| 12 | 2 |
| 13 | 2 |
| 14 | 2 |
| 15 | 2 |
| 16 | 1 |

**Gambar X-8. Shift Table**

## REFERENCES


http://www.itl.nist.gov/fipspubs/fip46-2.htm; Selasa, 22 Maret 2011 : $07^{00}$.

http://en.wikipedia.org/wiki/Data_Encryption_Standard; Selasa, 22 Maret 2011 : $07^{30}$.

http://csrc.nist.gov/publications/fips/fips197/fips-197.pdf; Selasa, 01 Maret 2011 : $22^{55}$.

http://csrc.nist.gov/archive/aes/rijndael/Rijndael-ammended.pdf; Selasa, 01 Maret 2011 : $22^{55}$.

http://orion.math.iastate.edu/dept/thesisarchive/MS/EKleimanMSSS05.pdf; Selasa, 01 Maret 2011 : $22^{55}$.

http://www.artofhacking.com/tucops/etc/crypto/044.PDF; Selasa, 01 Maret 2011 : $22^{55}$.

http://en.wikipedia.org/wiki/Advanced_Encryption_Standard#Known_attacks; Selasa, 22 Maret 2011 : $20^{15}$.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 23 Maret 2011

Michell Setyawati Handaka / 135 08 045