Algoritma Kriptografi Noekeon

Christopher Kurniawan – NIM : 13504117

Program Studi Teknik Informatika, Institut Teknologi Bandung
Jl. Ganesha 10, Bandung
E-mail : if114117@students.if.itb.ac.id

Abstraksi

Keamanan data merupakan hal yang sangat penting dalam menjaga kerahasiaan informasi terutama yang berisi informasi sensitive yang yhanya boleh diketahui isinya oleh pihak yang berhak saja, apalagi jika pengirimnya dilakukan melalui jaringan public, apabila data tersebut tidak diamankan terlebih dahulu, akan sangat mudah disadap dan diketahui isi informasinya oleh pihak yang tidak berhak.

Salah satu cara yang digunakan untuk pengamanan data adalah menggunakan system kriptografi yaitu dengan menyandikan isi informasi menjadi isi yang tidak dapat dipahami dengan melakukan enkripsi, dan untuk memperoleh kembali informasi yang asli, dilakukan proses sekripsi, disertai dengan menggunakan kunci yang tekah ditentukan. Namun usaha-usaha untuk memperoleh kunci tersebut dapat untuk dilakukan. Oleh karena itu, penelitian tentang kriptografi akan selalu berkembang untuk memperoleh algoritma yang makin kuat, untuk meningkatkan keamanan.

Melalui tugas ini akan dibahas mengenai algoritma kriptografi noekeon.

1 Dasar teori

1.1 Pengertian Kriptografi

Kriptografi aalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan seoerti inttegritas data, autentikasi data, dan kesahan.
Adapun 4 tujuan utama dari kriptografi adalah:

1 Kerahasiaan – hanya yang berwenang yang dapat informasi
2 Integritas data – penjagaan dari perubahan yang tidak sah, termasuk didalamnya penyisipan, penghapusan, dan penukaran data lain.
3 Autentikasi - identifikasi
4 Non-repudiasi – tidak dapat dibatalkan setelah dikirim

1.2 Dasar Matematis

Dasar matematis yang mendasari proses enkripsi dan dekripsi adalah relasi antara plainteks dan cipherteks. Dengan fungsi perantara enkripsi dan dekripsi. Apabila elemen plainteks adalah P dan elemen cipherteks adalah C, fungsi enkripsi adalah E dan dekripsi D, maka secara matematis proses kriptografi adalah:

$$\text{Enkripsi} : E(P) = C$$

Dekripsi : D(C) = P

Pada skema enkripsi konvensional atau symmetric key, digunakan sebuah kunci untuk melakukan proses enkripsi dan dekripsinya, kalau misalnya kuncinya dinotasikan dengan K, proses kriptografinya adalah:

Enkripsi : $E_K(P) = C$
Dekripsi : $D_K(C) = P$

Sedangkan pada system asymmetric key digunakan public key untuk proses enkripsi, dan private key untuk dekripsi. Sehingga proses enkripsinya adalah:

Enkripsi : $E_{PK}(P) = C$
Dekripsi : $D_{SK}(C) = P$

1.3 Teknik Kriptografi

Secara umum terdapat dua teknik yaitu symmetric key dan asymmetric key

1.3.1 Asymmetric key

Dalam skema ini, proses enkripsi dan dekripsi menggunakan kunci yang berbeda. Dan skema ini jg disebut public key karena kunci enkripsinya diberikan ke public, karena kunci sebenarnya adalah private key untuk mendekripsi.

Keuntungannya adalah jika pengguna banyak berinteraksi dengan berbagai pihak, sehingga cukup dibutuhkan dua buah kunci, yaitu public key dan private key.

1.3.2 Symmetric key

Skema enkripsi dalam bentuk symmetric key memiliki kunci yang sama dalam proses enkripsi dan dekripsinya. Dalam skema symmetric key, terdapat 2 jenis yaitu block cipher dan stream cipher.

Block cipher adalah skema enkripsi yang membagi2 pesan plainteks menjadi blok dengan suatu panjang tertentu dan di enkripsi perblok terlepas dari blok lain. Secara umum panjang bloknya lebih dari 64 bit. Dalam skema stream cipher, adalah pembagian blok dengan panjang satu bit.

1.4 Kriptografi Block cipher

1.4.1 Konsep dasar

Blok cipher merupakan sebuah fungsi yang memetakan n bit blok plainteks ke n bit blok cipherteks. Nilai n biasanya cukup besar beberapa teknik blok cipher modern diantaranya:

1.4.1.1 Cipher berulang

Pada teknik cipher berulang, blok plainteks mengalami pengulangan fungsi transformasi beberapa kali, dan secara umum merupakan gabungan dari proses subtitusi, kombinasi, penggeseran, xor dan lain sebagainya. Pada setiap pengulangan terdapa kunci yang dikombinasikan dengan teks. Parameter dalam cipher ini adalah jumlah pengulangan p, panjang blok n, dan kunci k, dan subkunci ki

1.4.1.2 Fiestel

Fiestel cipher beroperasi terhadap panjang blok data tetap sepanjang n, dan membagi 2 blok tersebut menjadi blok yang memiliki panjang n/2 dan dinotasikan menjadi L dan R. Fiestel cipher menerapkan

metode cipher berulang dengan masukan pada putaran ke i yang didapat dari keluaran sebelumnya. Secara sistematis dapat dinyatakan sebagai berikut:

Li =Ri -1
Ri=Li-1 (+) f(Ri-1,Ki) ; i=1,2,3,…,r

Ki adalah kunci untuk pengulangan ke i dan f adalah fungsi transformasi.

Blok plainteks adalah gabungan L dan R awal (Lo,Ro). Sedangkan cipherteks didapatkan dari L dan R putaran terakir (Rr,Lr).

1.4.1.3 Avalanche

Pada blok cipher, perubahan satu buah bit dapat byk menghasilkan perubahan yang besar, apalagi dalam pengulangan. Hasilnya disebut avalanche effect. Jadi jika ada satu buah bit input yang mengalami perubahan, maka kemungkinan besar setengah dari smua bit akan berubah dengan avalanche effect.

1.4.2 Mode Operasi

Ada beberapa mode operasi yang digunakan dalam kriptografi. Contohnya:

- Electronic codebook (ECB)
  Pada mode ini, blok plainteks yang menggunakan kunci yang sama, akan menghasilkan cipherteks yang sama pula.

Enkripsi : $Cj \leftarrow E_K(Pj)$; $1 \le j \le t$

Dekripsi : $Pj \leftarrow E_K^{-1}(Ck)$; $1 \le j \le t$

- Cipher-block Chaining (CBC)
  Pada prosesnya mode ini melibatkan penggunaan initializing vector, yang menyebabkan blok cipher apabila dienkripsi menggunakan kunci yang sama, cipherteksnya akan berbeda karena IV nya berubah.

Enkripsi : $Co \leftarrow IV$ untuk $1 \le j \le t$, $Cj \leftarrow E_K(Cj\text{-}1(+)Pj)$

Dekripsi : $Co \leftarrow IV$ untuk $1 \le j \le t$, $Pj \leftarrow Cj\text{-}1(+)E_K^{-1}(Cj)$

- Cipher feedback(CFB)
  Jika pada mode CBC plainteks dengan n bit diproses sekali waktu. Beberapa aplikasi mengharuskan r bit plainteks untuk dienkripsi duluan dan ditransmisikan bebas delay, untuk r<n. Dalam kasus ini CFB digunakan. CFB jg menggunakan IV

- Output feedback (OFB)
  Mode operasi ini digunakan apabila kesalahan propagasi sama sekali harus dihindari. Mirip dengan CFb, dan juga memungkinkan enkripsi menggunakan panjang blok yang berbeda.

1.4.3 Kunci lemah dan kunci Setengah lemah

Dalam Kriptografi dikenal istilah kunci lemah, dan kunci setengah lemah. Kunci lemah adalah kunci yang apabila dipakai untuk mengenkripsi plainteks menjadi cipherteks kemudian dienkripsi lagi, akan menghasilkan plainteks itu sendiri. Sedangkan kunci setengah lemah adalah sepasang kunci yang jika sebuah plainteks dienkripsi menjadi sebuah cipherteks, bias didekripsi dengan menggunakan kunci lain.

1.5 Enkripsi dan dekripsi

1.5.1 Enkripsi

Proses utama dalam algoritma kriptografi adalah enkripsi dan dekripsi. Enkripsi merubah plainteks menjadi cipherteks, pada mode ECBm sebuah blok pada plainteks dienkripsi kedalam blok cipherteks dengan panjang blok yang sama.

Blok cipher memiliki sifat bahwa setiap blok harus memiliki panjang yang sama(misalnya dalam contoh ini 128bit). Namun apabila plainteksnya kurang dari 128 bit, maka diperlukan adanya padding yaitu penambahan bit dummies untuk menambah bit hingga 128 bit.

1.5.2 Padding

Padding pada blok terakhir bias dilakukan dengan berbagai cara, misalnya penambahan bit bit tertentu. Misalnya penerapan padding dimana panjang blok adalah 128 bit, sedangkan yang baru terisi hanyalah 88 bit, maka diperlukan sekitar 40bit (5karakter). Sehingga kita masukkan padding yaitu karakter 0 sebanyak 5 buah.

1.5.3 Dekripsi

Dekripsi merupakan proses kebalikan dari enkripsi, dimana prosesnya merubah cipherteks menjadi plainteks.

1.6 Algoritma Noekeon

Noekeon merupakan cipher blok berulang dengan panjang blok dan panjang kuncinya 128 bit dan terdiri dari transformasi round berulang, diikuti transformasi output.

Noekeon memiliki 16 putaran pengulangan, dalam setiap putarannya dilakukan empat buah transformasi yaitu theta, shift offset Pi1 dan Pi2, dan gamma.

1.6.1 Penjadwalan kunci

Penjadwalan kunci dilakukan dengan mengkonversi kunci utama menjadi working key 128 bit, dan setiap roundnya menggunakan working key itu.

Dalam Noekeon ada mode penjadwalan kunci tidak dilakukan yang disebut direct key, namun dianggap kurang aman karena bias diserang memakai related key attack. Dalam mode indirect key, working keynya adalah kunci yang telah dienkripsi dengan menggunakan algoritma Noekeon itu sendiri.

1.6.2 State

Setiap transformasi round dioperasikan pada sebuah state yang terdiri dari empat buah 32 bit word yaitu a[0] sampai a[3]

1.6.3 Theta

Theta adalah pemetaan linear yang menggunakan working key k dan dilakukan operasi pada state a. pada tahap ini, terdapat 12 langkah operasi:

- Xor a0 dengan a2 (1)
- Geser (1) kekanan 8 bit(2)
- Geser (1) kekiri 8bit(3)
- Xor kan hasil 2 dengan 3 menjadi (4)
- Xor kan a1 dengan (4) lalu simpan sebagai a1
- Xor kan a3 dengan (4) lalu simpan sebagai a3
- Xor kan masing2 a0,a1,a2,a3 dengan kunci. Lalu simpan
- Xor a1 dengan a3(6)
- Geser(6) kekanan 8 bit (7)
- Geser (6) kekiri 8 bit (8)
- Xor kan a0 dengan (7) simpen sebagai a0
- Xor kan a2 dengan (8) simpan sebagai a2

1.6.4 Shift offset

Pergeseran ini terdiri dari 2 kali pergeseran yaitu Pi1 dan Pi2 yang masing2 berkebalikan arah dimana pergeseran pada Pi1 adalah:

- A0 tidak digeser
- A1 digeser 1 bit kekiri
- A2 digeser 5 bit kekiri
- A3 digeser 2 bit kekiri

Dan pergeseran pada Pi2:

- A0 tidak digeser
- A1 digeser 1 bit kekanan
- A2 digeser 5 bit kekanan
- A3 digeser 2 bit kekanan

1.6.5 Gamma

Gamma merupakan pemetaan non linear, dengan tiga langkah:

- Transformasi non linear sederhana
- Transformasi linear sederhana
- Transformasi non linear sederhana

Pada tahap ini Noekeon akan menghasilkan S-box yang terdiri dari 4 buah word 32 bit (a0,a1,a2,a3).

1.6.6 Round Constant

Untuk menghilangkan sifat linear tiap putaran Noekeon, dilakukan operasi round constants yang merupakan sebuah shift register (mod 0x80, untuk state[0]) yang dilaukan terhadap 8 bit terbawah dalam 32 bit word state awal.

1.6.7 Enkripsi dan Dekripsi

1.6.7.1 Enkripsi

Tahap ini diawali dengan adanya masukan dari pengguna berupa teks dan kunci. Lalu teks tersebut diubah menjadi bit-bit dan dibentuk blok sepanjang 128 bit. Yang masing-masing blok dan kunci dibagi menjadi 4 buah word 32bit (a0,a1,a2,a3) untuk plainteks dan (k0,k1,k2,k3) untuk kunci. Bila ternyata dalam suatu blok jumlah bitnya kurang dari 128, maka akan dilakukan padding dengan menambahkan bit dummies.

1.6.7.2 Dekripsi

Keunggulan algoritma Noekeon terletak pada kesederhanaan kode program dan sirkuit perangkat kerasnya. Kode atau sirkuit yang sama digunakan dalam enkripsi maupun dekripsinya, hanya penerapan pada theta yang berbeda. Pada enkripsi, theta adalah theta(k,a). namun pada dekripsi, menjadi theta(NullVektor,a). kebalikan dari theta adalah theta itu sendiri, namun dengan pengaplikasian null vector sebagai working key.

2 Pengamatan Simulasi Noekeon

2.1 Analisa system

Simulasinya terdiri dari 2 tahapan besar yaitu enkripsi dan dekripsi, yang masing2 pengulangannya tterdiri dari 4 prosedur, yaitu theta, Pi1, gamma dan Pi2. Pada implementasunya, data sebaai masukan akan dibagi2 menjadi beberapa blok yang masing2 blkok sepanjang 128 bit yang disebut state, baik sebagai plainteks maupun sebagai kunci, lalu blok tersebut akan dilakukan operasi dengan 4 prosedur tadi sehingga dapat menghasilkan cipherteks yang diharapkan.

Tujuan utama pada simulasi ini adalah memberikan penjelasan yang cukup baik dan mudah dipahami bagaimana proses atau langkah kriptografi Noekeon, mulai dari masukan data yang diberikan pengguna, sampai terjadi perubahan data tersebut menjadi bentuk yg terenkripsi, dan kembali jadi data semula.

2.2 Batasan pengamatan program simulasi

Dalam proses pengamatan program simulasi, akan ada pembatasan masalah yang diutamakan, untuk memudahkan pengamatan langkah kriptografi algoritma Noekeon ini, diantaranya:

1. Masukan berupa string baik untuk kunci maupun plainteks
2. Jumlah blok yang diamati satu blok

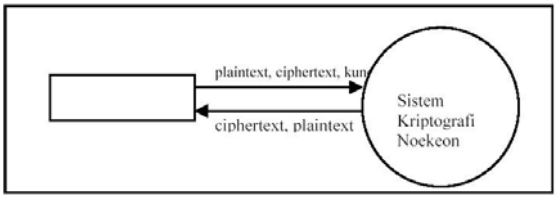
2.3 Pengamatan system

2.3.1 Model simulasi

Model simulasi yang digunakan adalah ada masukan dari pengguna, lalu visualisasi proses system dan keluaran yang ditampilkan untuk pengguna.

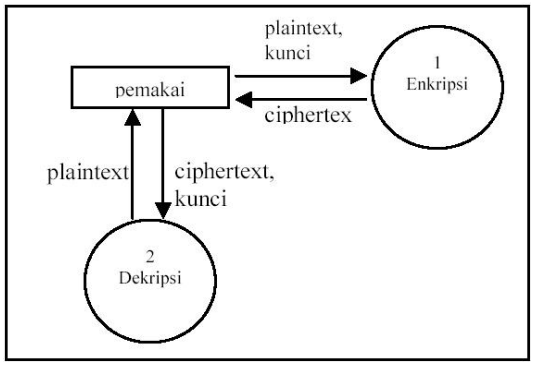
2.3.1.1 Diagram konteks

Pengamatan dimulai dengan mengamati diagram konteks, berupa penggambaran system penerapan algoritma Noekeon secara garis besar. Adapun diagram konteksnya adalah:



dari diagram konteks tersebut, terdapat DAD yg terdiri dari

- Proses enkripsi
- Proses dekripsi

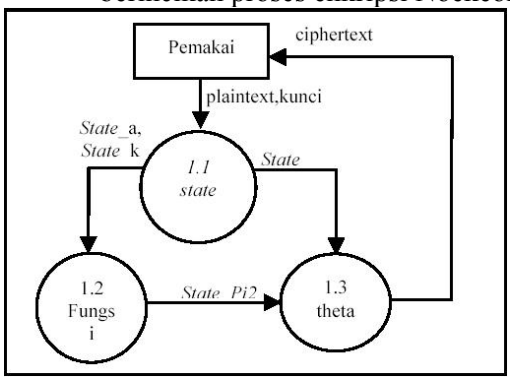


Untuk kedua proses enkipsi dan dekripsi yang masing2 putarannya terdiri dari theta, Pi1, Gamma, Pi2, dapat lebih dirinci nantinya.

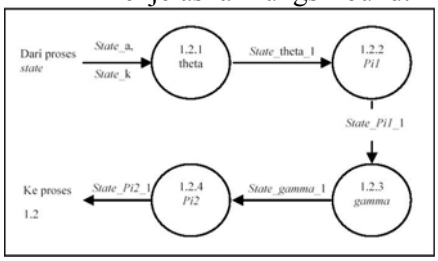
2.3.1.2 DAD

2.3.1.2.1 Proses Enkripsi

Dari DAD diatas, dapat diturunkan lagi DAD level bawah yang berincikan proses enkripsi Noekeon

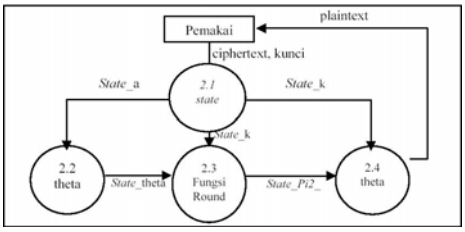


DAD pun diturunkan lagi untuk menjelaskan fungsi round:

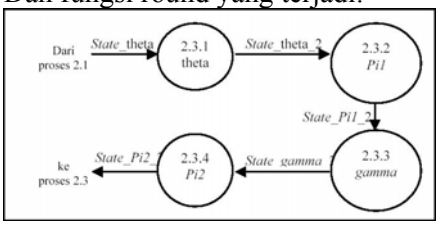


2.3.1.2.2 Proses Dekripsi

Analog dengan enkripsi, DAD level atas jg bias diturunkan menjadi:



Dan fungsi round yang terjadi:



2.3.1.3 Kamus Data

- Plainteks merupakan masukan dan keluaran dari proses system
  Plainteks = 0
  {Karakter ASCII} 16
- Cipherteks merupakan masukan dan keluaran dari proses system
  Cipherteks = 0
  {Karakter ASCII} 16
- State_a merupakan perubahan bentuk masukan (plainteks atau cipherteks) ke dalam bentuk state yaitu 4 buah 32 bit word
  State_a = 0
  {Karakter ASCII} 16
- State_k merupakan perubahan bentuk kunci ke dalam bentuk state yaitu 4 buah 32 bit word
  State_k = 0
  {Karakter ASCII} 16
- State_theta_1 merupakan state setelah hasil theta pada proses enkripsi
  State_theta_1 = 0
  {Karakter ASCII} 16

- State_theta_2 merupakan state setelah hasil theta pada proses enkripsi
  State_theta_2 = 0
  {Karakter ASCII} 16
- State_Pi1_1 merupakan state setelah hasil theta pada proses enkripsi
  State_Pi1_1 = 0
  {Karakter ASCII} 16
- State_Pi1_2 merupakan state setelah hasil theta pada proses enkripsi
  State_Pi1_2 = 0
  {Karakter ASCII} 16
- State_gamma_1 merupakan state setelah hasil theta pada proses enkripsi
  State_gamma_1 = 0
  {Karakter ASCII} 16
- State_gamma_2 merupakan state setelah hasil theta pada proses enkripsi
  State_gamma_2 = 0
  {Karakter ASCII} 16
- State_Pi2_1 merupakan state setelah hasil theta pada proses enkripsi
  State_Pi2_1 = 0
  {Karakter ASCII} 16
- State_Pi2_2 merupakan state setelah hasil theta pada proses enkripsi
  State_Pi2_2 = 0
  {Karakter ASCII} 16

2.3.1.4 Spesifikasi proses

Penggunaan algoritma Noekeon pada simulasi system kriptografi seperti telah disebutkan, menerapkan beberapa proses yang saling berhubungan sehingga akan menbentuk suatu system utuh yang diharapkan.

Nomor Proses	1.1,2.1
Masukan	Teks dari pengguna, Berupa plainteks, kunci
Keluaran	State_a,state_k
Logika	128 bit masukan data,dibagi kedalam empat buah word, masing-masing 32bit

Nomor Proses	1.2,2.3
Masukan	State_a,state_k,state_theta
Keluaran	State_Pi2,State_Pi2_2
Logika	Theta (k,a) Pi1(a) Gamma(a) Pi2(a)

Nomor Proses	1.3,1.2.1,2.2,2.4
Masukan	State_Pi2_1, State_a, State_k, State_a, State_Pi2_2
Keluaran	Cipherteks, State_theta_1, State_theta,plainteks
Logika	Temp = ao (+) a2 Temp = temp (+) (temp<<<8) (+) (temp >>>8) A1=a1(+)temp A3=a3(+)temp A0=a0(+)k0 A1=a1(+)k1 A2=a2(+)k2 A3=a3(+)k3 Temp = a1(+) a3 Temp=temp(+) (temp<<<8)(+)(temp>>>8) A0=a0(+)temp A2=a2(+)temp

Nomor Proses	1.2.2,2.3.2
Masukan	state_theta_1, state_theta_2
Keluaran	state_Pi1_1, state_Pi1_2
Logika	A1=a1<<<1 A2=a2<<<5 A3=a3<<<2

Nomor Proses	1.2.3,2.3.3
Masukan	state_Pi1_1, state_Pi1_2
Keluaran	state_gamma_1, state_gamma_2
Logika	A1=a1 (+) ¬ (a3 $_{v}$ a2)

	A0=a0 (+) (a2 $_{n}$ a1) Temp=a3 A3=a0 A0=temp A2=a2(+) a0(+)a1(+)a3 A1=a1 (+) ¬ (a3 $_{v}$ a2) A0=a0 (+) (a2 $_{n}$ a1)

Nomor Proses	1.2.4,2.3.4
Masukan	state_gamma_1, state_gamma_2
Keluaran	state_Pi2_1, state_Pi2_2
Logika	A1=a1>>>1 A2=a2>>>5 A3=a3>>>2

3 Hasil pengamatan Algoritma Noekeon

3.1 Hasil simulasi

3.1.1 Proses Enkripsi

Pada proses ini dibatasi masukan berupa 16 buah karakter bertipe string, dan kuncinya 16 karakter.

3.1.2 Proses Dekripsi

Proses dekripsi dilakukan untuk mendapatkan plainteks dari cipherteks, dengan masukan cipherteks dan menggunakan kunci yang sama pada saat menenkripsi.

3.2 Analisa Algoritma Noekeon

3.2.1 Struktur cipher

Struktur cipher pada Noekeon ditekankan pada kesederhanaan transformasi, yaitu komposisi desainnya terdiri dari transformasi linear theta,Pi1,Pi2, dan transformasi non linear gamma. Operasi diimplementasikan dengan operasi bitwise dan pergeseran bit.

Suatu cipher akan memiliki tingkat keamanan yang bagus jika antara plainteks dan cipherteks tidak ada hubungannya sama sekali. Untuk Noekeon telah dilakukan pengujian dengan kunci yang berbeda pada sebuah plainteks.

3.2.2 Proses Enkripsi dan Dekripsi

Struktur enkripsi dan dekripsi dirancang menggunakan kode maupun rangkaian yang sama. Sehingga menghasilkan kesederhanaan dalam implementasinya.

3.2.3 Penjadwalan kunci

Penjadwalan kunci pada Noekeon digunakan pada mode indirect key. Metode ini akan lebih memperkuat tingkat keamanan algoritma terhadap serangan, khususnya serangan related key. Penjadwalan kunci dilakukan melalui proses yang sama dengan Noekeon itu sendiri, yaitu proses Theta,Pi1,gamma,Pi2.

3.2.4 Sifat simetris, kunci lemah, kunci setengah lemah

Sifat simetri setiap putaran pada tiap algoritma kriptografi memberikan peluang untuk diserang kriptanalis. Pada Noekeon hal ini bias terjadi jika dalam setiap round tidak ditambahkan round constant, sehingga sifat-sifat simetrisnya dihilangkan termasuk didalamnya kemungkinan timbulnya kunci lemah dan kunci setengah lemah seperti pada DES.

3.2.5 Efek Avalanche

Suatu Algoritma Kriptografi memenuhi criteria Strict Avalanche Criterion (SAC) apabila rata-rata perubahan bit keluaran terhadap satu bit masukan setidaknya 50%. Dan Noekeon memenuhi criteria itu, karena rata-rata perubahan bit keluaran terhadap bit satuan pada masukan yaitu : 52.78% untuk plainteks, dan 52.37% untuk kunci.

3.2.6 Kesalahan Propagasi

Dimungkinkan terjadi kesalahan baik pada proses enkripsi maupun pada saat proses pertukaran data melalui media tertentu yang bias saja disebabkan oleh interferensi ataupun penyadap, sehingga terjadi perubahan informasi pada cipherteks.Untuk melihat sejauh mana kesalahan tersebut berpengaruh pada plainteks hasil dekripsi, dicobakan dilakukan perubahan pada cipherteks pada beberapa bit blok pertama. Yang kemudian didekripsi kembali menjadi plainteks.

Dari hasil yang diperoleh, ternyata plainteks yang diperoleh hanya mengalami kerusakan pada blok pertama saja, karena Noekeon merupakan algoritma dengan bentuk Block cipher, dengan pengenkripsian secara independent. Sehingga kesalahan pada satu blok tidak mempengaruhi blok lainnya.

3.2.7 Kekuatan terhadap serangan Brute Force

Serangan Bruteforce merupakan serangan dengan melakukan percobaan satu persatu kunci yang mungkin sampai diperoleh plainteks yang benar. Waktu yang diperlukan berbanding lurus dengan panjang kunci yang dipakai. Dengan panjang kunci 128 bit, dengan kemampuan computer yang sekarang, dibutuhkan kira-kira 100 tahun untuk dapat memecahkan kuncinya.

4 Kesimpulan

Dari hasil pengamatan pada tugas ini, dapat diambil beberapa kesimpulan:

- Semua kunci lemah dan kunci setengah lemah yang dimiliki oleh DES tidak terjadi pada Noekeon, sehingga pada Noekeon tidak ada pembatasan kunci yang digunakan ataupun pemanfaatan kunci tersebut untuk melakukan eksploitasi ke cipherteks.
- Efek avalanche yang diperoleh memenuhi criteria Strict Avalanche Criterion
- Kesalahan pada satu blok cipherteks tidak mempengaruhi blok lainnya
- Serangan Brute Force pada algoritma Noekeon membutuhkan waktu 100 tahun

5. Daftar Pustaka

- http://en.**wikipedia**.org/wiki/**Noekeon**
- Brickell Ernest F, Odlyzko, Andrew M. Cryptanalysis: A survey of recent result
- Daemen,Joan,Peeters,Michael, Van Assche,Gilles,and Rijmen,Vincent. NOEKEON Block cipher, Nessie Proposal, October 27,2000
- Daemen,Joan,Peeters,Michael, Van Assche,Gilles,and Rijmen,Vincent. NOEKEON slide. September 13,2000
- I Made ari, Penyandian data dengan Algoritma Kriptografi Noekeon
- Mohammad Sbastian Widodo, "Simulasi Algoritma Kriptografi Noekeon dalam penyandian data", Tugas akhir STT Telkom 2002