CESS (Journal Of Computer Engineering, System And Science) **p-ISSN :2502-7131**
Vol 2, No 1, Januari 2017 **e-ISSN :2502-714x**

ENKRIPSI DATA DENGAN ALGORITMA KRIPTROGRAFI NOEKEON

Aidil Halim Lubis
Teknik Informatika, Fakultas Ilmu Komputer dan Teknologi Informasi, Universitas Sumatera Utara
Jalan Universitas No.24A, Kampus USU Medan

***Abstrak*— Dalam kemajuan teknologi komputer saat ini berkembang sangat cepat seiring dengan makin kompleksnya sistem komputer dan kemampuan komputer untuk berkomunikasi dengan komputer lain dengan adanya jaringan. Distribusi file menggunakan jaringan antar komputer yang bersifat rahasia sangat memerlukan teknik untuk mengamankan file tersebut. Oleh karena itu diperlukan teknik pengaman dengan menggunakan algoritma kriptografi. Salah satu algoritma kriptografi adalah algoritma noekeon. Algoritma ini termasuk dalam algoritma blok cipher. Dengan algoritma ini data akan dienkrip sehingga aman untuk di distribusikan dalam jaringan.**

***Keywords*— Kriptografi, file, algoritma noekeon**

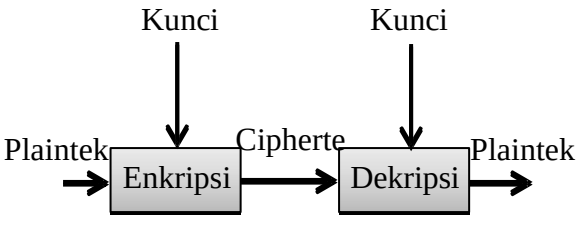
I. PENDAHULUAN

Kriptografi dalam sejarahnya tercatat dipergunakan secara terbatas oleh bangsa mesir 4000 tahun lalu. Kriptografi *(Crypthography)* berasal dari dua kata yaitu *"Crypto & Graphy"* yang dapat diartikan dalam bahasa yaitu *Crypto* artinya rahasia dan *Graphy* artinya tulisan. Dalam definisi lain kriptografi adalah ilmu dan seni untuk menjaga kerahasiaan pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknannya. Adapun tujuan dalam kriptografi tersebut yaitu :

1. *Kerahasiaan (Confidentially)* yaitu layanan yang digunakan untuk menjaga isi pesan dari siapapun yang tidak berhak untuk membacanya.
2. *Integritas Data (Data Integrity)* yaitu layanan yang menjamin bahwa pesan masih asli/utuh atau belum dimanipulasi selama pengiriman berlangsung.
3. *Otentikasi (authentication)* yaitu layanan dimana pihak-pihak yang berkomunikasi diidentifikasi dan juga mengidentifikasi sumber pesan *(data origin authentication)*.
4. *Nirpenyangkal (Non-repudiation)* yaitu layanan untuk mencegah entitas yang berkomunikasi *melakukan* penyangkalan, yaitu pengirim pesan menyangkal melakukan pengiriman atau penerima pesan menyangkal telah menerima pesan.

Kriptogrfi bukan satu-satunya cara untuk mengamankan informasi, melainkan teknik dalam melakukan kriptrografi tersebut. Kriptografi sendiri mulai terasa penting sejak berakhirnya perang dunia ke-2. Sejarahnya sejak masa perang dunia ke-2 pemerintahan jerman telah membuat mesin enkripsi yang bernama enigma. Namun enigma cipher berhasil dipecahkan oleh pihak sekutu sehingga perang dunia ke-2 tidak berlangsung lama. Konsep informasi diambil untuk memahami tentang kuantititas. Untuk memahami kriptografi, pengetahuan dan pemahaman tentang isu-isu yang terkait dengan keamanan informasi sangat diperlukan.

Selama bertahun-tahun satu set protokol yang rumit dibuat untuk menangani isu-isu tentang keamanan informasi ketika informasi tersebut dibuat menjadi sebuah dokumen atau data. Isu keamanan informasi tidak hanya dicapai melalui algoritma matematika dan protokol saja tapi memerlukan teknik prosedural. Kriptografi telah ada selama berabad-abad yang lalu,namun dimasa transisi sejak dua puluh tahun yang lalu dan kebaradaan tersebtu telah menjadi sebuah bidang ilmu. Sekarang di beberapa konfrensi ilmiah internasional dibuat khusus membahas tentang kriptografi, dan organisasi ilmiah internasional tersebut bernama *International Association for Cryptologic Research (IACR)* yang mendorong untuk penelitian-penelitian tentang kriptografi.
Pada gambar berikut ini dapat di definisikan mengenai alur kriptografi.



Gbr. 1 Proses Enkripsi/Dekripsi

II. TINJAUAN PUSTAKA

A. Dasar Matematis

Seperti yang diketahui bahwa kriptografi pada dulunya adalah sebuah seni,namun sekarang telah menjadi ilmu tentang mengamankan sebuah informasi didalamnya. Oleh karena perkembangan tersebut kriptografi saat perkembangan tersebut banyak

mengandung unsur matematis dalam hal enkripsi dan dekripsinya. Proses tersebut memiliki relasi antara plainteks dan cipherteks. Melalui perantara fungsi tersebut menjadikan elemen plainteks menjadi P dan elemen cipherteks menjadi C, sedangkan fungsi enkripsi adalah E dan dekripsi yaitu D, sehingga secara matematis didapatlah dasar proses kriptografi dengan fungsi :

Enkripsi = E(P) = C

Dekripsi = D(C) = P

Pada fungsi diatas adalah proses dasar kriptografi untuk enkripsi dan dekripsi, namun pada sistem yang konvesional akan didapati perubahan fungsi enkripsi dan dekripsinya. Hal ini terjadi pada sistem kunci simetris. Dalam prosesnya proses enkripsi dan dekripsi harus menggunakan sebuah kunci, dan elemen dari kunci tersebut adalah K. adapun proses kriptografi di definisikan dengan fungsi :

Enkripsi = EK(P) = C

Dekripsi = DK(C) = P

Sementara itu untuk sistem kunci asimetris akan didapati fungsi enkripsi dan dekripsi yang lain lagi dikarenakan adanya kunci public yang digunakan untuk enkripsi dan kunci private pada proses dekripsinya. Sehingga proses tersebut dapat di definisikan dengan fungsi :

Enkripsi : EK1(P) = C

Dekripsi : DK2(C) = P

Dimana :
K1 = Kunci Publik
K2 = Kunci Private

B. Dasar Matemaris

Dalam kriptografi teknik untuk enkripsi dan dekripsi yang menggunakan kunci terbagi menjadi 2 (dua) yaitu symmetric-key dan asymmetric-key (public key).Symmetric-key adalah proses enkripsi dan dekripsinya bila dilakukan akan memiliki pasangan kunci yang sama. Dan dalam symmetric-key skema enkripsi dibedakan menjadi dua kelas yaitu block cipher dan stream cipher.

Block cipher adalah algoritma enkripsi yang membagi-bagi plainteks yang akan dikirimkan dengan ukuran tertentu dalam hal ini dibuat menjadi blok-blok dengan panjang t, dan setiap blok dienkripsi dengan menggunakan kunci yang sama. Umumnya block cipher memporoses plainteks dengan blok yang relatif panjang lebih dari 64 bit, untuk mempersulit pola-pola penyerangan kunci bila data dicuri atau dibongkar oleh pihak yang tidak berkepentingan. Sedangkan Stream cipher adalah algoritma enkripsi yang mengenkripsikan data persatuan data, seperti bit, byte, nible atau per 5 bit. Setiap mengenkripsi satu satuan data digunakan kunci yang merupakan hasil pembangkitan dari kunci sebelumnya.

Asymmetric-key adalah algoritma yang menggunakan kunci yang berbeda pada proses enkripsi dan dekripsi. Sistem ini disebut juga dengan Public key karena kunci untuk enkripsi dibuat secara umum (public-key) atau dapat diketahui oleh orang lain, tapi untuk proses dekripsinya dibuat hanya satu saja oleh orang yang berwenang, dan ini disebut sebagai private-key. Dalam segi keunggulan atau keuntungan pada asymmetric-key ini yaitu untuk berkorespondensi secara rahasia dengan pihak lain tidak diperlukan kunci rahasia sebanyak jumlah pihak tersebut, cukup membuat dua buah kunci yaitu public-key bagi para koresponden untuk mengenkripsi pesan, dan private-key untuk mendekripsi pesan.

C. Dasar Matematis

Konsep Dasar

Blok cipher merupakan sebuah fungsi yang memetakan n-bit blok-blok plainteks ke n-bit blok-blok cipherteks, dengan n adalah panjang blok. Umumnya proses memblok-blok plainteks cukup besar yaitu (n > 64). Dalam penggunaannya metode blok cipher modern terbagi menjadi beberapa teknik.

1. Cipher berulang

Pada teknik cipher berulang (iterated cipher), blok plainteks mengalami perulangan fungsi transformasi beberapa kali untuk mendapatkan blok cipherteks. Dalam proses tersebut umumnya menggunakan gabungan proses substitusi, permutasi, kompresi dan ekspansi terhadap blok plainteks. Dalam proses kunci di kombinasikan dengan plainteks dalam round key. Untuk elemennya putaran adalah r, besar blok adalah n dan kunci besar adalah k serta sub-kunci berelemen Ki.

2. Fiestel Cipher

Fiestel cipher beroperasi terhadap panjang blok data tetap sepanjang n (genap), kemudian dibagi 2 blok dengan panjang masing-masing n/2, kedua blok tersebut dielemenkan menjadi L dan R. fiestel menerapakan metode cipher berulang dengan masukkan pada putara ke-i yang didapat dari output sebelumnya. Secara matematis dinyatakan dengan :

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

Ki adalah kunci putaran ke- I dan f adalah transformasi. Pada blok plainteks awal dinyatakan dalam bentuk (Lo, Ro) sedangakan cipherteks akhir dinyatakan dalam (Rr, Lr).

3. Avalanche

Pada cipher blok perubahan satu bit akan menghasilkan perubahan lebih dari satu bit setelah satu putaran. Hasil perubahannya itu disebut avalanche effect. Setiap algoritma harus memenehi kriteria avalanche effect.

Mode Operasi

Dalam kriptografi ada beberapa mode operasi yang digunakan untuk blok cipher diantaranya :

1. Electronic Codebook (ECB)

Dalam mode ini, blok-blok plainteks (x) yang identik (menggunakan kunci yang sama) akan menghasilkan cipherteks (c) yang identik juga. Dalam matematis dinyatakan :

Enkripsi : $cj \leftarrow E_K(x_j);\ 1 \leq j \leq t$
Dekripsi : $xj \leftarrow E_K(c_j);\ 1 \leq j \leq t$

2. *Cipher blok chaining (CBC)*

Dalam proses cipher blok chaining harus menggunakan *initializing vector (IV)* yang menyebabkan blok-blok cipherteks yang identik bila dienkripsi dengan kunci dan *IV* yang sama. Perubahan *IV,kunci* dan *plainteks* pertama akan menghasilkan cipherteks yang berbeda. Dalam matematis dinyatakan :

Enkripsi : $c_o \leftarrow IV$, untuk $1 \leq j \leq t$,
$c_j \leftarrow E_K(c_j - 1\ (+)\ x_j)$

Dekripsi : $co \leftarrow IV$, untuk $1 \leq j \leq t$,
$x_j \leftarrow c_j - 1\ (+) E_K^{-1}\ (c_j)$

3. *Cipher feedback (CFB)*

Dalam mode ini tidak perlu menunggu pembagian data menjadi blok-blok yang memiliki ukuran, sehingga mode ini dapat diimplementasikan secara real time.

4. *Output feedback (OFB)*

Mode operasi ini digunakan bila kesalahan propagasi sama sekali harus dihindari. OFB hampir mirip dengan CFB dan juga memungkinkan enkripsi menggunakan variasi blok.

Kunci Lemah dan Setengah Lemah

Didalam istilah kriptografi dikenal adanya kunci lemah dan setengah lemah. Kunci lemah adalah apabila mengenkripsi suatu plainteks kemudian di enkripsi lagi menggunakan kunci yang sama maka hasil cipherteksnya adalah plainteks itu sendiri. Kunci setengah lemah adalah sepasang kunci yang mempunyai sifat jika sebuah plainteks dienkripsi dengan suatu kunci, akan didapat dekripsi dengan kunci yang lain.

D. Enkripsi dan Dekripsi

Enkripsi

Enkripsi adalah proses utama dalam suatu algoritma kriptografi. Enkripsi adalah merubah sebuah plainteks ke dalam bentuk cipherteks. Proses enkripsi tersebut telah dijelaskan berdasarkan dasar matematis yang ada.

Blok cipher memiliki sifat bahwa panjang blok harus sama (misal 128 bit). Namun apabila pesan yang dienkripsi memiliki panjang blok terakhir tidak tepat 128 bit, maka diperlukan mekanisme yang dinamakan padding. Padding adalah proses penambahan bit-bit dummies agar blok tersebut terpenuhi atau sesuai. Padding ini dilakukan pada blok terakhir plainteks.

Mekanisme padding dapat dilakukan dengan berbagai macam cara diantaranya menambahkan bit-bit tertentu. Contohnya ada sebuah plainteks dengan panjang blok 128 bit (16 byte) dan pada blok terakhir plainteks tersebut hanya terdiri dari 88 bit (11 byte), sehingga jumlah padding yang dibutuhkan adalah 5 byte yaitu dengan menambahkan angka nol sebanyak 4 byte kemudian angka 5 sebanyak 1 byte.

Dekripsi

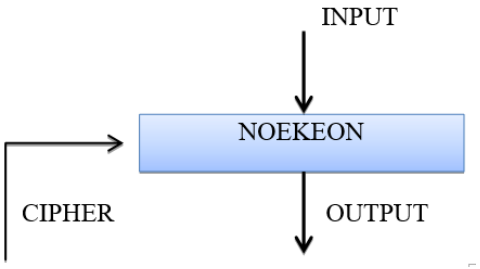
Dekripsi adalah proses kebalikan dari proses enkripsi yaitu merubah cipherteks menjadi plainteks. Untuk menghilangkan padding pada proses enkripsi dilakukan berdasarkan informasi jumlah padding yaitu angka pada byte terakhir.

E. Algoritma Noekon

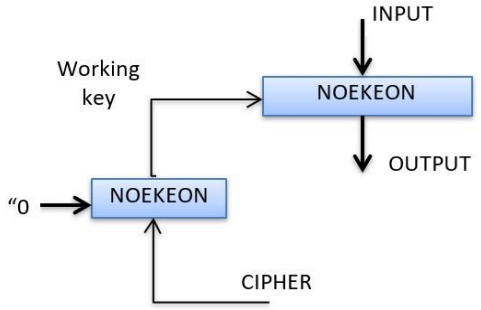
Salah satu jenis algoritma kriptografi blok cipher adalah noekeon. Algoritma noekeon ini termasuk keluarga dua cipher blok yang dirancang oleh Joan Daemen, Michael Peeters, Gilles Van Assche dan Vinjent Rijmen yang dibuat pada proyek Nessie pada September 2000. Dua cipher tersebut adalah direct mode dan indirect mode. Noekeon juga merupakan cipher blok berulang dengan panjang blok dan panjang kunci masing-masing 128 bit, terdiri dari transformasi round sederhana yang berulang, diikuti dengan transformasi output. Algoritma noekeon memiliki 16 putaran (Nr) iterasi, dalam setiap putarannya dilakukan empat buah transformasi yaitu theta, shift offset yang terdiri dua buah transformasi Pi1 dan Pi2 dan gamma.

1. Penjadwalan Kunci

Penjadwalan kunci dilakukan dengan cara mengkonversi kunci utama *(cipher key)* 128 bit menjadi sebuah *working-key* 128 bit. Karena sifat Noekeon yang simetri, maka setiap roundnya menggunakan working-key yang sama. Dalam Noekeon ada mode saat penjadwalan kunci tidak dilakukan yang disebut dengan "direct mode" artinya working-key adalah cipher-key itu sendiri. Mode yang kedua mode "indirect mode"yang melakukan proses penjadwalan kunci untuk mengeliminasi pola serangan related-key. Adapun alur dari mode-mode tersebut seperti gambar berikut :



Gbr. 2 Mode Direct-key



Gbr. 3 Mode Indirect-key

Pada indirect-key, sebelum kunci diaplikasikan terhadap pesan pada operasi theta, kunci dirubah dahulu menjadi sebuah kunci yang lain dengan tetap menggunakan fungsi yang sama dalam Noekeon. Kemudia baru kunci tersebut diaplikasikan pada pesan pada operasi theta dan seterusnya sebanyak 16 putaran.

2. State

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

3. Theta

Theta adalah pemetaan linier yang menggunakan working-key *k* dan dilakukan pada operasi *state a*. tahap ini memerlukan 12 langkah dalam penyelesaiannya. Adapun langkah tersebut yaitu :
Langkah pertama operasi *xor* antara word a0 dan a2. Kemudian hasil operasi dilakukan pergeseran bit, yaitu kekanan 8-bit dan kekiri 8-bit. Hasil pergeseran tersebut di-*xor*dengan hasil langkah pertama. Berikutnya yaitu proses perubahan word a1 dan a3,dengan meng-*xor*-kan a1 dengan langkah kedua. Setelah itu keempat word dari plainteks masing-masing di-*xor*-kan dengan keempat buah kunci word dan akan menghasilkan word [a0,a1,a2,a3] baru. Dari word baru tersebut, a1 dan a3 di-*xor* dan hasilnya dilakukan dua buah pergeseran 8-bit masing-masing kekanan dan kekiri. Terakhir a0 dan a2 masing-masing akan di-*xor* dengan hasil pergeseran tersebut. Dari proses Theta ini akan dihasilkan word [a0,a1,a2,a3] yang baru untuk proses selanjutnya.

4. Shift Offset

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

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

Pergeseran pada Pi2 :

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

5. Gamma

Gamma merupakan pemetaan non linier, dengan tiga langkah :

- Transformasi non linier sederhana
- Transformasi linier sederhana
- Transformasi non linier sederhana

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

6. Round Constant

Untuk menghilangkan sifat linier pada setiap putaran Noekeon, dilakukan operasi round constant yang merupakan shift register (mod 0x80, untuk state [0]) yang dilakukan terhadap 8-bit terbawah dalam 32-bit word state awal.

7. Enkripsi dan Dekripsi

Seperti yang diketahui dalam setiap algoritma kriptografi akan melakukan proses enkripsi dan dekripsi pada data yang akan diproses. Adapun di algoritma Noekeon proses enkripsi dan dekripsi tersebut dengan langkah berikut :

Enkripsi

Tahap ini diawali dengan adanya masukkan 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 32 bit (a0,a1,a2,a3) untuk plainteks dan (k0,k1,k2,k3) untuk kunci. Bila ternyata dalam suatu blok jumlah bitnya kurang dari 128 bit, maka akan dilakukan padding dengan menambahkan bit dummies.

Dekripsi

Proses selanjutnya yang dilakukan oleh Noekeon adalah 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 (k,a). namun pada dekripsi, menjadi theta (NullVektor,a). kebalikan dari theta adalah theta itu sendiri, namun dengan pengaplikasian null vector sebagai working-key.

III. ANALISA ALGORIMTA NOEKEON

Struktur cipher pada Noekeon ditekankan pada kesederhanaan transformasi, yaitu komposisi desainnya terdiri dari transformasi linier theta, Pi1,Pi2 dan transformasi non linier gamma. Suatu cipher akan memilikit tingkat keamanan yang bagus jika antara plainteks dan cipherteks tidak ada hubungan sama sekali.

Penjadwalan kunci pada Noekeon digunakan pada mode indirect key. Metode ini akan lebih memperkuat tingkat keamanan algoritma terhadap serangan, khususnya serangan related-key.

Suatu algoritma kriptografi memenuhi criteria Strict Avalanche Criterion (SAC) apabila rata-rata perubahan bit keluaran terhadap satu bit masukkan setidaknya 50%. Noekeon rata-rata perubahan bit keluaran terhadap bit satuan pada masukkan yaitu 52.78% untuk plainteks dan 52.37% untuk kunci.

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

Kekuatan terhadap serangan Brute Force. Serangan brute force merupakan serangan dengan melakukan percobaan satu persatu terhadap 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 komputer sekarang dibutuhkan waktu kira-kira 100 tahun untuk dapat memecahkan kuncinya.

IV. KESIMPULAN

Pada algoritma Noekeon ini dapat disimpulkan bahwa jika dalam pengamanan sebuah data yang menggunakan algoritma kriptografi Noekeon akan didapat beberapa kesimpulan yaitu :

1. Noekeon tidak membatasi kunci yang digunakan ataupun pemanfaatan kunci tersebut untuk melakukan eksploitasi ke cipherteks.
2. Efek avalanche yang diperoleh memenuhi kriteria Strict Avalanche Criterion.
3. Kesalahan pada satu blok cipher tidak mempengaruhi blok lainnya.
4. Serangan brute force membutuhkan waktu yang lama untuk dipecahkan.

REFERENSI

[1] http://en.wikipedia.org/wiki/Noekeon
[2] Daemon,Joan,Peeters,Michael, Van Assche, Gilles, and Rijmen, Vincent. Noekeon slide. September 13,2000
[3] Daemon,Joan,Peeters,Michael, Van Assche, Gilles, and Rijmen, Vincent. Noekeon blok cipher, Nessie proposal, October 27,2000
[4] Ebook.Menezes, Handbook of Applied Cryptography