Journal of Informatics Management and Information Technology
ISSN 2774-4744 (Media Online)
Vol 2, No 2, April 2022
Hal 73−77
https://hostjournals.com/jimat

Implementasi Algoritma Noekeon Untuk Mengamankan File Audio

Tita Azwinar Sarumaha

Program Studi Teknik Informatika STMIK Budi Darma, Medan, Indonesia1
Email: titaazwinarsarumaha@gmail.com

Abstrak−Seiring dengan perkembangan zaman yang semakin maju, serta didukung oleh perkembangan teknologi informasi yang sanagt pesat khususnya dalam menghasilkan file audio sekarang bisa dilakukan denagan perangakt smartphone. Dengan adanya aplikasi pada smarthone dengan perangkat membuat Audio baik untuk pribadi ataupun publik. File Audio perlu diamankan dengan pengamanan yang lebih baik, guna mengantisipasi Apbila akun jauh dari ke tangan orang yang tidak berwenang salah satu cara untuk mengamankan file audio adalah dengan teknik kriptografi, dengan teknik ini maka orang yang tidak berhak tidak dapat melihat informasi yang ada dalam Audio tersebut. Salah satu algoritma yang dapat digunakana dalam mengamankan *file audio* yaitu algoritma NOEKEON, Noekeon merupakan *cipher blok* berulang dengan panjang *blok* dan panjang kuncinya masing-masing 128 bit, yang terdiri dari aplikasi transpormasi round sederhana yang berulang, diikuti dengan sebuah trasformasi output. Noekeon memiliki 16 putaran (Nr) iterasi dalam setiap putarannya dilakukan empat buah trasformasi yaitu, Theta, *shift offset* yang terdiri dari dua buah transformasi Pi1 dan Pi2 dan gamma Kelebihan dari algoritma Noekeon tidak membatasi kunci yang digunakan ataupun pemenfatan kunci tersebut untuk melakukan eksploitasi ke dalam cipher teks dan efek avalanche yang diperoleh memenuhi Kriteria *strict Avalanche criterion.* Jika ada kesalahan pada satu blok *cipher* tidak dapat mempengaruhi blok lainya.

Kata Kunci : Kriptografi, Mengamankan, File Audio, Algoritma Noekeon

Abstract−Along with the development of an increasingly advanced era, and supported by the development of very rapid information technology, especially in producing audio files, it can now be done with smartphone devices. With the application on smartphones with devices to make audio both for private and public. Audio files need to be secured with better security, in order to anticipate if the account is far from being in the hands of unauthorized people, one way to secure audio files is by using cryptographic techniques, with this technique, unauthorized people cannot see the information contained in the audio. the. One of the algorithms that can be used to secure audio files is the NOEKEON algorithm, Noekeon is a repeating block cipher with a block length and key length of 128 bits each, which consists of a simple round transformation application that repeats itself, followed by an output transformation. Noekeon has 16 rounds (Nr) iterations in each round four transformations are carried out, namely, Theta, shift offset consisting of two transformations Pi1 and Pi2 and gamma The advantages of the Noekeon algorithm do not limit the keys used or use these keys to exploit into cipher text and avalanche effects obtained meet the strict Avalanche criterion. If there is an error in one block cipher it cannot affect the other blocks.

Keywords: Cryptography; Securing; Audio Files; Noekeon Algorithm

1. PENDAHULUAN

Di era yang serba digital banyak mengubah kebiasaan manusia dalam kehidupan sehari-hari. Sebelum era digital jika seseorang ingin mengirimkan pesan maka orang tersebut akan menuliskannya dalam bentuk surat dan mengirimkan surat tersebut melalui pos hal ini membutuhkan waktu yang relatif lama. Sekarang, jika ingin mengirimkan pesan kepada orang lain dapat langsung mengirimkan pesan tersebut melalui jaringan telekomunikasi dan dapat diterima oleh orang yang dituju hanya dalam hitungan detik saja. Bahkan pesan yang dikirimkan bukan hanya dalam bentuk teks saja, tetapi bisa juga dalam bentuk audio atau pun video.

Proses pengiriman *file audio* menggunakan jaringan telekomunikasi memiliki kelebihan yaitu waktu pengiriman yang sangat cepat. Banyak orang yang menggunakan saluran telekomunikasi untuk melakukan panggilan suara secara langsung atau pun mengirimkan pesan audio. Namun juga memiliki kelemahan yakni masalah keamanan data yang melewati jaringan telekomunikasi tersebut. Bisa saja data tersebut di sadap oleh orang yang tidak berhak sehingga informasi yang terdapat di dalamnya dapat bocor.

Untuk mengatasi hal tersebut, maka *file audio* atau pun *file audio* yang melewati jaringan telekomunikasi tersebut harus diamankan. Salah satu cara yang dapat digunakan untuk mengamankan *file audio* adalah dengan teknik kriptografi. Dalam kriptografi *file audio* yang melewati jaringan telekomunikasi dapat dienkripsi ataupun di acak sehingga ketika pesan audio tersebut berhasil disadap maka informasi yang terdapat dalam *file audio* tersebut tidak dapat dimengerti oleh pihak yang tidak berwenang ataupun pihak yang tidak memiliki kunci, hanya pihak yang memiliki kunci yang dapat mengetahui isi pesan dalam file audio tersebut.

Setiap file yang disimpan ke dalam media digital selalu di rubah ke dalam bentuk biner agar file tersebut dapat tersimpan di memori. Untuk dapat melakukan proses enkripsi terhadap file audio maka algoritma kriptografi yang dapat digunakan adalah algoritma kriptografi modern karena algoritma kriptografi modern beroperasi dalam mode bit. Salah satu algoritma kriptografi modern yang dapat digunakan untuk mengamankan *file audio* adalah algoritma noekeon. Pemilihan algoritma noekeon untuk mengamankan file audio karena algoritma ini memiliki beberapa kelebihan yang tidak dimiliki oleh algoritma kriptografi modern lainnya. Algoritma noekeon tidak memiliki kunci lemah sehingga tidak ada batasan terhadap penggunaan panjang kunci. Apabila terjadi kesalahan pada satu blok pesan suara maka tidak akan mempengaruhi blok lainnya. Serangan *brute force* membutuhkan waktu lebih dari 100 tahun untuk mendapatkan kunci dari algoritma noekeon ini [1].

Selain kelebihan yang telah disebutkan di atas juga terdapat beberapa kelebihan lain yang dimiliki oleh algoritma noekeon yang membuatnya cukup unik yaitu algoritma ini sangat cepat jika diimplementasikan pada perangkat keras

ataupun *hardware* khusus, memungkinkan untuk diimplementasikan pada perangkat lunak ataupun *software* yang tehan terhadap serangan DPA, penerapan algoritma noekeon membutuhkan penggunaan *Random Acces Memory* atau RAM yang sangat rendah, memiliki kode program yang sangat ringkas jika diimplemetasikan ke dalam perangkat lunak, dapat berjalan pada berbagai *platform* dan memiliki desain yang sederhana sehingga mudah untuk diingat oleh kebanyakan orang [2].

Berdasarkan kedua penelitian yang telah di sebutkan di atas, algoritma noekeon memiliki banyak kelebihan yang tidak dimiliki oleh algoritma kriptografi khusunya kriptografi *block cipher* maka algoritma ini cocok di terapkan untuk mengamankan file audio karena ukuran file audio yang tergolong besar sehingga proses enkripsi dan dekripsi file video tersebut dapat dilakukan dengan cepat.

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani *cryptos* artinya *secret* rahasia sedangkan *graphia* berarti *writing* tulisan [3]. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat lain sudah digunakan 400 tahun. yang dipergunakan untuk menandai aktivitas-aktivitas rahasia dalam mengirim pesan. Kriptografi pada awalnya dijabarkan sebagai ilmu yang mempelajari bagaimana menyembunyikan pesan, namun pada pengertian modern kriptografi adalah ilmu yang bersandarkan pada teknik matematika untuk berurusan dengan keamanan informasi [4]. Enkripsi dan proses menyandikan *plaintext* menjadi *ciphertext* sedangkan proses mengembalikan *ciphertext* menjadi *plaintext* seperti semula dinamakan dekripsi dapat diterapkan baik pada file audio *cipher* dan *key* kunci aturan untuk *enciphering* dan *deciphering* yang digunakan digunkan dalam relasi antara dua buah himpunan yang berisi elemen–elemen *plaintext* dan himpunan yang berisi *ciphertext*.

2.2 File Audio

Amr *(Adaptive multi rate)* merupakan file audio terkompresi, file ini beriteraksi AMR, dan berukuran sangat kecil [7]. file ini dirahasiakan dari sebuah *encoder* yang menyusuaikan denan kemampuan *processing* dan *streaming* MCU/CPU, sehingga file yang dihasilkan memiliki bit-rate yang sesuai dengan MCU/CPU/ Processor yang digunakan, file ini bisannya lebih banyak ditanamkan pada perangkat *mobile embeded file*, dan bisa ditransformasikan dalam bentuk file MP3

3. HASIL DAN PEMBAHASAN

Proses enkripsi dan dekripsi pada algoritma noekeon menggunakan proses pembangkitan atau penjadwalan kunci yang digunakan pada tiap putaran enkripsi dan dekripsi. Tahap- tahap penjadwalan kuunci pada algoritma noekeon adalah sebagai berikut:

1. input kunci pengguna.
2. Melakukan padding pada kunci pengguna jika panjang kunci kurang dari 16 karakter.
3. Membentuk blok A0-A3 masing-masing berukuran 32 bit atau 4 karakter.
4. Melakukan putaran penjadwalan kunci sebanyak 16 putaran (i) operasi pada tiap putaran adalah sebagai berikut:
   a. Melakukan operasi xor A0 dengan RC(i).
   b. Melakukan operasi theta inverse terhadap A0-A3.
   c. Melakukan operasi rotate_left A1<< 1
   d. Melakukan operasi rotate_left A2<< 5
   e. Melakukan operasi rotate_left A3<< 2
   f. Melakukan operasi gamma terhadap A0-A3
   g. Melakukan operasi rotate_right A1>> 1
   h. Melakukan operasi rotate_right A2>> 5
   i. Melakukan operasi rotate_right A3>> 2
5. Setelah operasi putaran selanjutnya meelakukan operasi xor A0 dan RC (16)
6. A0 –A3 akan menjadi kunci dekripsi DK (0)-DK (3).
7. Melakukan operasi theta inverse terhadap A0-A3.
8. A0-A3 akan menjadi kunci enkripsi EK (0) –EK (3).

Anlisis terhadap proses penjadwalan kunci pada algoritma Noekeon dapat dijabarkan sebagai berikut:
Penjadwalan Kunci:
Kunci Input :1002940000000000
Kunci (bit)
00110001;00110000;00110000;00110010
00111001;00110100;00110000;00110000
00110000;00110000;00110000;00110000

00110000;00110000;00110000;00110000
A0 = 00110001;00110000;00110000;00110000 = 31303032
A1 = 00111001;00110100;00110000;00110000 = 39343030
A2 = 00110000;00110000;001100000;00110000 = 30303030
A3 = 00110000;00110000;00110000;00110000 = 30303030

Putaran (0) Penjadwalan Kunci:
A0 = A0 Xor RC (0) = 313030B2
Theta Inv Proses:
A0 = 313030B2
A1 = 393430B0
A2 = 303030B0
A3 = 303030B0
T = T = A0 XOR A2 = 00000002

TEMP = T<<8 XOR T>>8 = 02000200
AI = T XOR TEMP XOR A1 = 3B343232
A3 = T XOR TEMP XOR A3 = 3D3D3439
T = A1 XOR A3 = 09040000

TEMP = T<<8 XOR T>>8 = 04090409
A0 = T XOR TEMP XOR A0 = 3C3D343B
A2 = T XOR TEMP XOR A2 = 3D3D3439
A1 = A1<<1 = 76686464
A2 = A2 <<5 = A7A68727
A3 = A3 <<2 =C8C0C8C8

GAMMA PROSES
A0 = 3C3D343B
A1 = 76686464
A2 = A7A68727
A3 = C8C0C8C8

A1 = A1 XOR ((NOT A3) AND (NOT A2)) = FFFFFFFF66715474
A0 = A0 XOR (A2 AND A1) = 1A1D301F
A0 = A3 = C8C0C8C8
A3 = A0 = 1A1D301F

A2 = A2 XOR A3 XOR A1 XOR A0 = FFFFFFFF130A2B84
A1 = A1 XOR (NOT A3 AND NOT A2) = FFFFFFFF82919014
A0 = A0 XOR (A2 AND A1) = FFFFFFFFCAC0C8CC

A1 = A1 >>1 = 7FFFFFFFC148C80A
A2 = A2 >>5 = 27FFFFFFF898515C
A3 = A3 >>2 = 1E874C07

Putaran Proses (1) Penjadwalan Kunci
A0=A0 Xor R (1) = FFFFFFFFCAC0C8D6
Theta inv proses
A0 = FFFFFFFFCAC0C8D6
A1 = 7FFFFFFFC148C80A
A2 = 2FFFFFFFF898515C
A3 = 1E874C07

T = A0 XOR A2 = D00000003258998A
TEMP = T<<8 XOR T>>8 = 8AD0003258ABD249
AI = T XOR TEMP XOR A1 = 252FFFCDABBB83C9
A3 = T XOR TEMP XOR A3 = 5AD00032747407C4
T = A1 XOR A3 = 7FFFFFFFDFCF840D
TEMP = T<<8 XOR T>>8 = 79000020305BC27B
A0 = T XOR TEMP XOR A0 = F900002025548EA0
A2 = T XOR TEMP XOR A2 = 500000002757D551

A1 = A1<<1 = A5FFF9B57770793
A2 = A2 <<5 = 4EAFAAA34
A3 = A3 <<2 = 6B4000C9D1D01F12

GEMMA PROSES
A0 = F900002025548EA0
A1 = A5FFF9B57770793
A2 = 4EAFAAA34
A3 = 6B4000C9D1D01F12

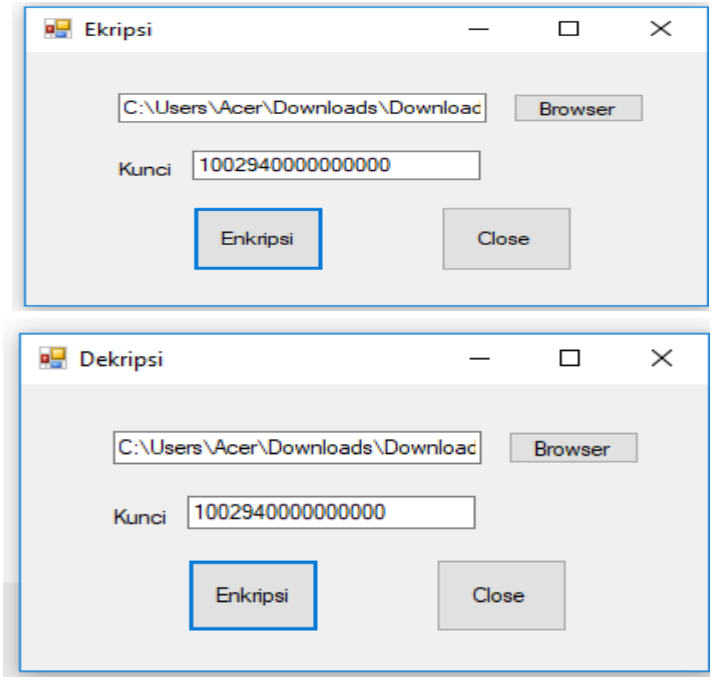
A1 = A1 XOR ((NOT A3) AND (NOT A2)) = 9EE000A95372475A
A0 = A0 XOR (A2 AND A1) = F900002067268CB0
A0 = A3 = 6B4000C9D1D01F12
A3 = A0 = F900002067268CB0

A2 = A2 XOR A3 XOR A1 XOR A0 = CA000440F7E7ECC
A1 = A1 XOR (NOT A3 AND NOT A2) = 9CBFFF32C3F34659
A0 = A0 XOR (A2 AND A1) = 67E000C9D2A2595A

A1 = A1 >>1 = CE5FFF9961F9A32C
A2 = A2 >>5 = 6650002207BF3F6
A3 = A3 >>2 = 3E40000819C9A32C
PUTARA PROSES (2) Penjadwalan Kunci
A0=A0 XOR R (2) = 67E000C9D2A2596E
A0 = 67E000C9D2A2596E

3.1 Pengujian Aplikasi

Pengujian aplikasi dimaksudkan untuk memastikan perintah yang di masukkan oleh *user* dapat dijelaskan dengan baik oleh aplikasi. Berikut ini adalah spesifikasi pengujian aplikasi pemograman *file audio* menerapkan algoritma *noekeon.*



Gambar 1. Pengujian Ekripsi dan Deskripsi

4. KESIMPULAN

Berdasarkan hasil penelitian disimpulkan pengamanan file audio dapat dilakukan dengan cara melakukan proses enkripsi pada file audio tersebut. Algoritma Noekeon dapat diterapkan untuk mengenkripsi file audio menggunakan 16 putaran. Aplikasi pengamanan file audio menerapkan algoritma noekeon dapat dirancang menggunakan visual basic.

ISSN 2774-4744 (Media Online)
Vol 2, No 2, April 2022
Hal 73−77
https://hostjournals.com/jimat

REFERENCES

[1] A. H. Lubis, "Enkripsi Data Dengan Algoritma Kriptografi Noekeon," *Journal of Computer Engineering System and Science,* pp. 22-26, 2017.
[2] J. Daemen, M. Peeters, G. V. Assche and V. Rijmen, "The Noekeon Block Cipher," Esat Cosic Kuleuven, Proton Worls Intl, Belgium, 2000.
[3] D. Ariyus, Pengantar Ilmu Kriptografi Teori dan Analisis dan Implementasinya, Yogyakarta: Andi, 2008
[4] R. Sadikin, Kriptografi Untuk Keamanan Jaringan dan Implementasinya Dalam Bahasa Java, A. Probawati, Ed., Yogyakarta: Andi, 2012
[5] R. Munir, Kriptografi, Yogyakarta: Andi, 2006.
[6] H. Mukhtar, Kriptografi Untuk Keamanan Data, Yogyakarta: Deepublish, 2018.
[7] J. Hermawan, Analisa dan Desain Pemrograman Berorientasi Objek Dengan UML dan Visual Basic.Net, Yogyakarta: Andi, 2005
[8] R. A. Sukamto and M. Shalahuddin, Rekayasa Perangkat Lunak, Yogyakarta: Andi, 2011