JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

Analisa Algoritma Noekeon Untuk Mengamankan File Video

Milawati, Natalia Silalahi, Kennedi Tampubolon

Teknik Informatika, Universitas Budi Darma, Medan, Indonesia
Email: milawatigayo1997@gmail.com
Submitted **16-02-2021**; Accepted **24-06-2021**; Published **29-06-2021**

Abstrak

Seiring dengan perkembangan zaman,kebutuhan manusian meningkat.termasuk akan kebutuhan imformasi .oleh sebab itu,pengiriman dan penyimpanan file melalui media eletronik memerlukan suatu proses yang mampu menjamin keaman dan keutuhan dari file tersebut.untuk menjamin keaman dan keutuhan dari suatu file,di butuhkan suatu proses penyandian.enkripsi dilakukan ketika file akan di kirim.proses ini akan mengubah suatau file asal menjadi file rahasia yang tidak dapat di baca. Sementara itu,proses dekripsi dilakukan oleh penerima file yang di kirim tersebut.file rahasia yang di terima akan di ubah kembali menjadi file asal.dengan cara penyandian tadi,file asli tidak akan terbaca oleh pihak yang tidak berkepentingan,melain kan haya oleh penerima yang memiliki kunci dekripsi. Saat ini,salah satu cara yang di gunakan untuk pengamanan file adalah menggunakan sistem kriptografi yaitu dengan menyandikan isi informasi (plainteks)tersebut menjadi isi yang tidak di pahami melalui proses enkripsi (enchiper),dan untuk memperoleh kembali informasi yang asli ,dilakukan proses dikripsi (dechiper).disertai dengan mengunakan kunci yang benar.namun dengan sejalan perkembangan ilmu penyandian atau kriptografi.usaha-usaha untuk memeroleh kunci tersebut dapat diakukan oleh siapa saja,termasuk yang tidak sah untuk memilih informasi tersebut .oleh karna itu, penelitian tentang kriptogafi akan selalu berkembang untuk memperoleh algoritma kriptografi yang semakin kuat, sehingga usaha-usaha untuk memecah kode kriptografi secara tidak sah menjadi lebih sulit.

Kata Kunci: Penyandian; File Video; Enkripsi; Dekripsi; Algoritma Nonkeon

Abstract

Along with the times, human needs are increasing, including the need for information. Therefore, sending and storing files via electronic media requires a process that is able to guarantee the safety and integrity of the file. To ensure the safety and integrity of a file, it requires a file. The encryption process is carried out when the file is sent. This process will change the original file into a secret file that cannot be read. Meanwhile, the decryption process is carried out by the recipient of the sent file. The secret file received will be changed back to the original file. By means of this encryption, the original file will not be read by unauthorized parties, but only by the recipient who has decryption key. Currently, one of the methods used to secure files is to use a cryptographic system by encoding the contents of the information (plaintext) into incomprehensible content through an encryption process (enchiper), and to retrieve the original information, a encryption process is carried out (dechiper). accompanied by using the correct key. However, in line with the development of encryption or cryptography, efforts to obtain this key can be done by anyone, including those who are not authorized to choose the information. Therefore, research on cryptography will always evolved to obtain ever stronger cryptographic algorithms, making attempts to illegally decode cryptography illegally become more difficult.

Keywords: Encoding; Video Files; Encryption; Decryption; Nonkeon Algorithm

1. PENDAHULUAN

Seiring dengan perkembangan zaman yang semakin maju, serta didukung oleh perkembangan teknologi yang sangat pesat khususnya dalam menghasilkan file video. Pembuatan video sekarang bisa dilakukan dengan perangkat smartphone. Dengan adanya aplikasi pada smartphone dengan mudah bisa membuat video baik untuk pribadi ataupun publik. File video perlu diamankan dengan pengamanan yang lebih baik, guna mengantisipasi apabila akun jatuh ke tangan orang yang tidak berwenang. Salah satu cara untuk mengamankan file video adalah dengan teknik kriptografi, dengan teknik ini maka orang yang tidak berhak tidak dapat melihat informasi [1]. yang ada dalam video tersebut.

Kriptografi merupakan ilmu sekaligus seni yang digunakan untuk menjaga kerahasiaan pesan dalam hal ini dapat berupa data ataupun informasi dengan cara menyamarkan informasi atau data tersebut dengan melakukan proses enkripsi menjadi bentuk yang tidak dapat dimengerti dengan menggunakan algoritma tertentu. Sistem keamanan data menggunakan aplikasi kriptografi dapat mengamankan file video dengan ekstensi mp4. Ada banyak algoritma dalam kriptografi yang dapat digunakan untuk mengamankan file video.

Salah satu algoritma yang dapat digunakan dalam mengamankan file video yaitu algoritma NOEKEON, Noekeon merupakan *cipher block* berulang dengan panjang *block* dan panjang kuncinya masing-masing 128 bit, yang terdiri dari aplikasi transpormasi *round* sederhana yang berulang, diikuti dengan sebuah transformasi output. Noekeon memiliki 16 putaran (Nr) iterasi, dalam setiap putarannya dilakukan empat buah transformasi yaitu, Theta, *Shift offset* yang terdiri dari dua buah transformasi Pi1 dan Pi2, da Gamma. Kelebihan dari algoritma Noekeon tidak membatasi kunci yang digunakan ataupun pemanfaatan kunci tersebut untuk melakukan eksploitasi ke cipher teks dan efek *avalanche* yang di peroleh memenuhi kreteria *strict Avalanche criterion*,jika ada kesalahan pada satu blok cipher tidak mempengaruhi blok lainya [2].

2. METODOLOGI PENELITIAN

2.1 Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua, yaitu kripto dan graphia. Kripto berarti secret (rahasia) dan graphia berarti writing (tulisan). Menurut terminologinya kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ketempat lain. Sebagai pembanding, selain definisi tersebut terdapat

JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

pula definisi yang lain yaitu, kriptografi adalah ilmu yang mempelajari teknik-teknik matematika yang berhubungan dengan aspek keamanan informasi seperti kerahasiaan, integritas data, serta otentikasi [3].

2.2 Video

Video adalah teknologi pemerosesan sinyal elektronik yang mewakilkan gambar bergerak. Video merupakan susunan beberapa frama dari cerita digital yang tersusun rapat sehingga menghasilkan gerakan berdurasi . Dalam 1 detik saja suatu video bisa ditemukan 20 frame atau gambar yang tersusun rapat didalamnya. Dengan kata lain video merupakan susunan dari banyak citra digital. Aplikasi umum dari teknilogi video adalah televise. Video juga bisa digunakan dalam aplikasi teknik, keilmuan, produksi dan keamanan. Istilah video juga digunakan sebagai singkatan videotape. Perekam video, dan pemutar video. Saat ini ada 2 kategori video yaitu, video analog dan video digital [5].

2.3 Algoritma Noekeon

Algoritma *Noekeon* adalah salah satu jenis algoritma kriptografi blok cipher 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[6]. 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 lakukan yang disebut dengan "*direct mode*" artinya *working-key* adalah *cipher-key* itu sendiri [6]. Mode yang kedua mode "*indirect mode*" yang melakukan proses penjadwalan kunci untuk mengeliminasi pola serangan *related-key*.
   Pada *indirect-key*, sebelum kunci diaplikasikan terhadap pesan pada oprasi *theta*, kunci dirubah dahulu menjadi sebuah kunci yang lain dengan tetap menggunakan fungsi yang sama dalam Noekeon. Kemudian baru kunci tersebut diaplikasikan pada pesan pada oprasi theta dan seterusnya sebanyak 16 putaran.
   a. *State*
      Setiap informasi round dioprasikan pada sebuah state yang terdiri dari empat buah 35-bit word yaitu [0] sampai [3].
   b. *Theta*
      Theta adalah pemetaan linier yang menggunakan *working-key k* dan dilakukan pada oprasi state a. tahap ini memerlukan 12 langkah dalam penyelesaiannya. Adapun langkah tersebut yaitu:
      Langkah pertama oprasi *xor* antara word a0 dan a2. Kemudian hasil oprasi dilakukan pergeseran bit, yaitu kekanan 8-bit dank e kiri 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 *plaintext* 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.
   c. *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:
      Pi1: A0 tidak bergeser
      A1 digeser 1 bit kekiri
      A2 digeser 5 bit kekiri
      A3 digeser 2 bit kekiri
      Pi2: A0 tidak bergeser
      A1 digeser 1 bit kekanan
      A2 digeser 5 bit kekanan
      A3 digeser 2 bit kekanan
   d. *Gamma*
      Gamma merupakan pemetaan non linier, dengan tiga langkah:
      1) Transformasi non linear sederhana
      2) Transformasi linier sederhana
      3) Transformasi non linear sederhana
      Dalam tahap ini Noekeon akan menghasilkan S-Box yang terdiri dari 4 buah *word* 32-bit (a0,a1,a2,a3).
   e. *Round Constant*
      Untuk menghilangkan sifat linear 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.
2. *Enkripsi dan Dekripsi*

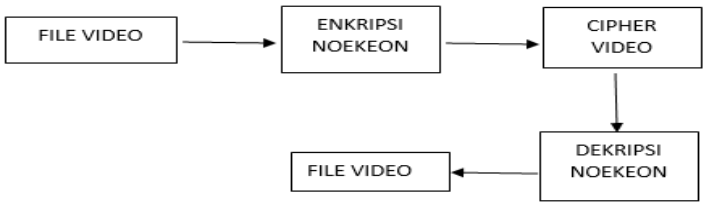
JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

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 denga langkah berikut:

1) *Enkripsi*
   Tahap ini diawali dengan adanya masukan dari pengguna berupa teks dan kunci. Lalu teks tersebut diubah menjadi bi-bit dan bentuk blok sepanjang 128 bit. Yang masing-masing blok dank kunci dibagi menjadi 4 buah word 32 bit (a0,a1,a2,a3) untuk *plaintext* 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.
2) *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*.

3. HASIL DAN PEMBAHASAN

Analisa dilakukan untuk mengetahui lebih dalam hal-hal yang berkaitan dengan suatu kejadian, dalam penelitian ini analisa dilakukan untuk mengetahui langkah-langkah dalam proses enkripsi dan dekripsi file video. Untuk melakukan proses enkripsi dan dekripsi file video, hal yang pertama dilakukan adalah mempersipkan sebuah file video dan mempersiapkan kunci yang akan digunakan pada saat enkripsi dan dekripsi. Proses enkripsi file video dilakukan untuk mengolah struktur file video tersebut, sehingga informasi yang ada dalam video tersebut dapat terlindungi atau tidak dapat dilihat oleh pihak yang tidak berwenang. Setelah melalui pakar enkripsi maka hasilnya adalah *cipher* video, untuk dapat dilihat kembali informasi yang ada dalam video tersebut perlu dilakukan proses dekripsi untuk mengubah struktur file *cipher* video kembali menjadi plain video semula menggunakan kunci yang dipakai saat proses enkripsi.



Gambar 1. Proses Pengamanan file Video

Proses enkripsi dan dekripsi pada algoritma Noekeon menggunakan proses pembangkitan atau penjadwalan kunci yang digunakan pada tiap putaran enkripsi dan dekripsi Tahap-tahap penjadwalan kunci 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 A1>>2
5. Setelah operasi putaran selanjutnya melakukan 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).

Tabel 1. Konstanta RC

I	Rumus	RC(i)
0	-	0×80
1	RC[0] And 0×80 != 0? Jika True Rc[1]= Rc [0]<< 1Xor 0×1B Jika False	0×1a

	RC[1]= Rc[0]<<1	
2	RC[1] And 0×80 != 0? Jika True Rc[2]= Rc [1]<< 1Xor 0×1B Jika False RC[2]= Rc[1]<<1	0×34
---	---	---
---	---	---
16	RC[15] And 0×80 != 0? Jika True Rc[16]= Rc [15]<< 1Xor 0×1B Jika False RC[16]= Rc[15]<<1	0×f8

Analisa 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 ; 00110010;
31303032
A1 : 00111001 ; 00110100 ; 00110000 ; 00110000;
39343030
A2 : 00110000 ; 00110000 ; 00110000 ; 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 = A0 XOR A2 = 00000002
TEMP = T<<8 XOR T>>8 = 02000200
AI = T XOR TEMP XOR A1 = 3B343232
A3 = T XOR TEMP XOR A3 = 32303232
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

JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

A0 = A0 XOR (A2 AND A1) = FFFFFFFFCAC0C8CC
A1 = A1 >>1 = 7FFFFFFFC148C80A
A2 = A2 >>5 = 27FFFFFFF898515C
A3 = A3 >>2 = 1E874C07

Sampai pada pada proses putran ke 16

Putaran Proses (16)Penjadwalan Kunci
A0=A0 Xor R(16) = 17FD259C7775035E
DK(0) = 17FD259C7775035E
DK(1) = C7413D441F2A31B
DK(2) =6772F14F8B5CF7AC
DK(3)= BFB30E7D04B3ED4C
Theta inv proses
A0 = 17FD259C7775035E
A1 = C7413D441F2A31B
A2 =6772F14F8B5CF7AC
A3 = BFB30E7D04B3ED4C
T = A0 XOR A2 = 708FD4D3FC29F4F2
TEMP = T<<8 XOR T>>8 = 76A45C28FA08DB15
AI = T XOR TEMP XOR A1 = A5F9B2F47D38CFC
A3 = T XOR TEMP XOR A3 = B99886860292C2AB
T = A1 XOR A3 = B3C71DA945414E57
TEMP = T<<8 XOR T>>8 = 90AE6E58E80B16FD
A0 = T XOR TEMP XOR A0 = 3494566DDA3F5BF4
A2 = T XOR TEMP XOR A2 = 441B82BE2616AF06
EK(0)= 3494566DDA3F5BF4
EK(1) = A5F9B2F47D38CFC
EK(2) = 441B82BE2616AF06
EK(3) = B99886860292C2AB

Analisa enkripsi pada algoritma Noekeon menggunakan blok-blok input dengan panjang masing-masing blok 32 bit. Berikut penjabaran operasi dan proses enkripsi pada algoritma Noekeon.

KUNCI ENKRIPSI:
EK(0)= 3494566DDA3F5BF4
EK(1) = A5F9B2F47D38CFC
EK(2) = 441B82BE2616AF06
EK(3) = B99886860292C2AB
KUNCI DEKRIPSI
DK(0) = 17FD259C7775035E
DK(1) = C7413D441F2A31B
DK(2) =6772F14F8B5CF7AC
DK(3)= BFB30E7D04B3ED4C
Analisa terhadap proses enkripsi pada algoritma Noekeon dapat dijabarkan sebagai berikut. Plainteks : 49;53;4F;20;4D;65;64;69;61;20;66;69;6C;65;20;70
Pembentukan Blok Input:
Blok input(0) : 01001001 ; 01010011 ; 01001111 ; 00100000
Blok input(1) : 01001101 ; 01100101 ; 01100100 ; 01101001
Blok input(2) : 01100001 ; 00100000 ; 01100110 ; 01101001
Blok input(3) : 01101100 ; 01100101 ; 00100000 ; 0 1110000
Enkripsi :
A0 = 49;53;4F;20
A1 = 4D;65;64;69
A2 = 61;20;66;69
A3 = 6C;65;20;70
Putaran (0) ENKRIPSI :
A0=A0 Xor R(0) = 49534FA0
A0=49534FA0
A1=4D656469
A2=61206669
A3=6C652070
K(0)= 3494566DDA3F5BF4

K(1)= A5F9B2F47D38CFC
K(2)= 441B82BE2616AF06
K(3)= B99886860292C2AB
T = A0 Xor A2 =287329C9
Temp = T<<Xor T>>8=141BA88
A1= T Xor Temp Xor A1=6457F728
A3= T Xor Temp Xor A3=4557B331
A0=A0 Xor kunci (0) =3494566D936C1454
A1=A1 Xor kunci (1) = A5F9B2F23847BD4
A2=A2 Xor kunci (2) =441B82BE4736C96F
A3=A3 Xor kunci (3) = B998868647C5719A
T = A1 Xor A3 = B3C71DA964410A4E
Temp = T<<Xor T>>8= 89AE6E79E86E0FB9
A0= T Xor Temp Xor A0=EFD25BD1F4311A3
A2= T Xor Temp Xor A2=7E72F16ECB19CC98
A1 = A1<<1= 4BF365E4708F7A9
A2 = A2<<5=4E5E2DD96339931F
A3 = A3<<2= E6621A191F15C66A

Gamma Proses :

A0= EFD25BD1F4311A3
A1=4BF365E4708F7A9
A2=4E5E2DD96339931F
A3= E6621A191F15C66A
A1 = A1 Xor ((Not A3) And (Not A2)) = A49F245E5B0CB3C9
A0 = A0 Xor (A2 And A1)= 41E245843089309
A0= A3= E6621A191F15C66A
A3= A0=41E245843089309
A2= A2 Xor A3 Xor A1 Xor A0 = EAC10987383520D6
A1 = A1 Xor (Not A3 And Not A2)= B5BFF67EDFCEFFE9
A0=A0 Xor (A2 And A1)= 46E31A1F0711E6AA
A1=A1 >> 1 = DADFFB3F6FE77FF4
A2=A2 >> 5 = B756084C39C1A906
A3= A3 >> 2=307891610C224C2
Sampai pada proses putaran ke 16
Putaran (16) ENKRIPSI :
A0=A0 Xor R(16) = E45DB201B76DE3BE
A0= E45DB201B76DE3BE
A1=76BD903DEBEEA710
A2= 1F701EFF00B329FD
A3= 77C336A4195CCC76
K(0)= 3494566DDA3F5BF4
K(1)= A5F9B2F47D38CFC
K(2)= 441B82BE2616AF06
K(3)= B99886860292C2AB
T = A0 Xor A2 =FB2DACFEB7DECA43
Temp = T<<Xor T>>8= 6E57D31B207D9D31
A1= T Xor Temp Xor A1= E3C7EFD87C4DF062
A3= T Xor Temp Xor A3=E2B949418EFF9B04
A0=A0 Xor kunci (0) =D0C9E46C6D52B84A
A1=A1 Xor kunci (1) = 7CE20B12AC3D2BEC
A2=A2 Xor kunci (2) =5B6B9C4126A586FB
A3=A3 Xor kunci (3) = CE5BB0221BCE0EDD
T = A1 Xor A3 = B2B9BB30B7F32531
Temp = T<<Xor T>>8= 8809890CC392C297
A0= T Xor Temp Xor A0= EA79D65019335FEC
A2= T Xor Temp Xor A2=61DBAE7D52C4615D
Hasil enkripsi = EA79D65019335FEC61DBAE7D52C4615D di rubah menjadi karakter yang dapat dilihat sebagai berikut:
Output(0) = EA =ê
Output(1) = 79 = y
Output(2) = D6 =Ö

JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

Output(3) = 50 =P
Output(4) = 19 =P
Output(5) = 33 =3
Output(6) = 5F =_
Output(7) = EC =ì
Output(8) = 61 =a
Output(9) = DB =Û
Output(10) = AE =®
Output(11) = 7D =}
Output(12) = 52 =R
Output(13) = C4 =Ä
Output(14) = 61 =a
Output(15) = 5D =]

Setelah melakukan proses enkripsi akan menghasilkan Chipervideo = êyÖPP3_ìaÛ®}RÄa]
Proses dekripsi pada algoritma Noekeon menggunakan blok-blok input dengan panjang masing-masing blok 32 bit. Berikut penjabaran oprasi dari proses enkripsi pada algoritma Noekeon.

DEKRIPSI PUTARAN (0)
A0= EA79D65019335FEC
A1=7CE20B12AC3D2BEC
A2=61DBAE7D52C4615D
A3= CE5BB0221BCE0EDD
DK(0) = 17FD259C7775035E
DK(1) = C7413D441F2A31B
DK(2) =6772F14F8B5CF7AC
DK(3)= BFB30E7D04B3ED4C
T = A0 Xor A2 =8BA2782D4BF73EB1
Temp = T<<Xor T>>8=13F38F33DA7546B5
A1= T Xor Temp Xor A1=E4B3FC0C3DBF53E8
A3= T Xor Temp Xor A3= 560A473C8A4C76D9
A0=A0 Xor kunci (0) =FD84F3CC6E465CB2
A1=A1 Xor kunci (1) = 709618C6EDCF88F7
A2=A2 Xor kunci (2) =6A95F32D99896F1
A3=A3 Xor kunci (3) = 71E8BE5F1F7DE391
T = A1 Xor A3 = 17EA699F2B26B66
Temp = T<<Xor T>>8= 6BE7542B99D4D4
A0= T Xor Temp Xor A0= FC91B201B76DE300
A2= T Xor Temp Xor A2=7BC1EFF00B32943
A0=A0 Xor RC(0)= FC91B201B76DE380
A1 = A1<<1=612C318DDB9F11EF
A2 = A2<<5= 783DFE01665287E
A3 = A3<<2=47A2F97C7DF78E47

Gamma Proses :

A0= FC91B201B76DE380
A1=612C318DDB9F11EF
A2= 783DFE01665287E
A3= 47A2F97C7DF78E47
A1 = A1 Xor ((Not A3) And (Not A2)) = D970318E5B97406F
A0 = A0 Xor (A2 And A1)= FD91A381A568E3EE
A0= A3= 47A2F97C7DF78E47
A3= A0= FD91A381A568E3EE
A2= A2 Xor A3 Xor A1 Xor A0 = 64C0B493956D05B8
A1 = A1 Xor (Not A3 And Not A2)= DB5E79E21105586E
A0=A0 Xor (A2 And A1)= 7E2C9FE6CF28E6F
A1=A1 >> 1 = 6DAF3CF10882AC37
A2=A2 >> 5 = 632605A49CAB682D
A3= A3 >> 2= BF6468E0695A38FB

Sampai pada putaran ke 16
PUTARAN (16) DEKRIPSI

JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

A0= ABFE0B71E33A1B77
A1= 36C3BA31D8B958E6
A2=8DAF0C1F6259E6B0
A3=73633438534F0115
DK(0) = 17FD259C7775035E
DK(1) = C7413D441F2A31B
DK(2) =6772F14F8B5CF7AC
DK(3)= BFB30E7D04B3ED4C
T = A0 Xor A2 =2651076E8163FDC7
Temp = T<<Xor T>>8=20E13F860D7CA464
A1= T Xor Temp Xor A1= 307382D954A60145
A3= T Xor Temp Xor A3=75D30CD0DF5058B6
A0=A0 Xor kunci (0) =BC032EED944F1829
A1=A1 Xor kunci (1) = 3AB7A9E5994BFBFD
A2=A2 Xor kunci (2) =EADDFD50E905111C
A3=A3 Xor kunci (3) = CCD03A4557FCEC59
T = A1 Xor A3 = F66793A0CEB717A4
Temp = T<<Xor T>>8= C365C75D17D913E1
A0= T Xor Temp Xor A0= 89017A104D211C6C
A2= T Xor Temp Xor A2= DFDFA9AD306B1559
A0=A0 Xor RC(16)= 89017A104D211C94

Hasil Dekripsi = 89017A104D211C6CDFDFA9AD306B1559 di rubah menjadi karakter yang dapat dilihat sebagai berikut:

Output(0) = 89 =]
Output(1) = 01 =SOH
Output(2) = 7A =z
Output(3) = 10 =DLE
Output(4) = 4D =M
Output(5) = 21 =!
Output(6) = 1C =FS
Output(7) = 6C =l
Output(8) = DF =ß
Output(9) = DF =ß
Output(10) = A9=I
Output(11) =AD=
Output(12) = 30 =0
Output(13) = 6B = k
Output(14) = 15 =NAK
Output(15) = 59 =Y
Setelah melakukan proses Dekripsi akan menghasilkan Chipervideo =
] SOH z DLEM!FS1 ß ßI0kNAKY.

3.1 Hasil Pengujian

Pengujian dilakukan untuk mengukur kinerja dari suatu algoritma, dalam penelitian ini pengujian dilakukan untuk mengukur kinerja algoritma noekeon berdasarkan parameter waktu. Sebagai bahan yang digunakan dalam pengujian digunakan file video dengan durasi yang sama, tetapi dengan format penyimpanan yang berbeda-beda berikut ini hasil pengujian yang telah dilakukan.

Tabel 1. Hasil Pengujian

File Video	Format Pengujian	Durasi (Detik)	Waktu Enkripsi (Detik)	Waktu Dekripsi (Detik)
	MP4	06:49	55,0	60,5
	WMV	06:49	52,5	53,0

JURIKOM (Jurnal Riset Komputer), Vol. 8 No. 3, Juni 2021
e-ISSN 2715-7393 (Media Online), p-ISSN 2407-389X (Media Cetak)
DOI 10.30865/jurikom.v8i3.2840
Hal 80−88

File Video	Format Pengujian	Durasi (Detik)	Waktu Enkripsi (Detik)	Waktu Dekripsi (Detik)
	FLV	06:49	51,0	52,3
	MOV	06:49	50,5	51,4
	Jumlah		52,25	54,3

Berdasarkan hasil pengujian di atas yang telah dilakukan nilai rata-rata enkripsi dijumlahakan kemudian dibagi 4 maka akan menghasilkan nilai rata-rata 52,25, dan nilai rata-rata dekripsi dijumlahkan kemudian dibagi 4 maka akan menghasilkan nilai rata-rata 54,3.

4. KESIMPULAN

Berdasarkan penelitian yang telah dilakukan dapat diambil beberapa kesimpulan bahwa dalam pengamanan file video dalam kriptografi dilakukan dengan cara mengacak atau enkripsi file video tersebut. File video hasil enkripsi dengan algoritma noekeon dapat mengamankan informasi yang ada dalam file video tersebut. Waktu yang dibutuhkan untuk melakukan proses enkripsi dan dekripsi pada berbagai format penyimpanan file video juga tidak terlalu jauh berbeda yaitu rata-rata 52,25 detik untuk enkripsi dan 54,3 detik untuk dekripsi.

REFERENCES

[1] F. Fernando, S. and E. Suryana, "Aplikasi Kriptografi Untuk Mengamankan File Audio Video Menggunakan Visual Basic. Net," Jurnal Media Infotama, vol. X, no. 1, pp. 27-34, 2014.
[2] A. h. Lubis, "ENKRIPSI DATA DENGAN ALGORITMA KRIPTOGRAFI NOEKEON," 2017.
[3] D. Ariyus, Pengantar Ilmu Kriptografi Teori, Analisis dan Implementasi, Yogyakarta: Andi Publisher, 2008.
[4] R. Sadikin, Kriptografi Untuk Keamanan Jaringan, Yogyakarta: Andi, 2012.
[5] T. D. Studio, Seri Pelajaran Komputer Mengoperasikan Software Video Editing, Jakarta: Alex Media Komputindo, 2006.
[6] K. and A. Koniyo, Tuntunan Praktis Membangun Sistem Informasi Akuntansi Dengan Visual Basic, Yogyakarta: Andi, 2007.
[7] R. Munir, Kriptografi, Bandung: Informatika, 2006.
[8] N. D. d. Anang, Kriptografi, 2011.
[9] S.M. Emy Setyningsih, Kriptografi & Implemetasinya Menggunakan Matlab,Yogyakarta, 2015