APLIKASI PENGAMANAN VIDEO DENGAN FORMAT 3GP MENGGUNAKAN ALGORITMA NOEKEON

I Putu Herryawan
Program Studi Teknik Informatika, Jurusan Ilmu Komputer
Fakultas Matematika dan Ilmu Pengetahuan Alam
Universitas Udayana
Email : putu.herry@cs.unud.ac.id

Abstrak: Keamanan data adalah hal yang kritis dalam pengelolaan informasi pribadi terutama untuk informasi yang hanya bias diakses oleh seseorang yang memiliki hak. pengiriman data atau informasi tanpa pengamanan sangat beresiko penyadapan dan dapat dengan mudah diketahui oleh orang yang tidak memiliki hak.

Kriptografi adalah jalan keluar untuk kepastian keamanan data dengan jalan mengkodekan informasi menjadi bentuk yang sulit atau bahakan tidak dimengerti melalui proses enkripsi, kemudian untuk mendapatkan kembali bentuk semula diperlukan kunci yang tepat.

Keamanan format 3gp mengunakan algoritma kriptografi noekeon bertujuan untuk memberikan keamanan pada *content* video dan membatasi dari orang yang tidak berhak. Disamping itu aplikasi keamanan ini juga bertujuan untuk mempelajari bagaimana algoritma tersebut bekerja dan keuntungan atau kelebihan algoritma tersebut.

Kunci : kriptografi, enkripsi, descripsi, 3gp, nokeon

APPLICATION SECURITY WITH VIDEO FORMAT 3GP ALGORITHM USING NOEKEON

Abstract: *Data security is a critical in maintaining information privacy, mainly for the information that just can be accessed by someone who reserve the right. Data or information sending without securing is risky in tapping and the information content can be known easily by people who are not eligible.*

Cryptography is a solution to ensure data security by encode the information content into difficult or even can not be understood through encryption process, then to get back the original one is passed through by decryption process, using the correct key.

".3gp" video format security using Noekeon cryptography algorithm is expected to give the video content is secure from the people who are not eligible. Beside that, by this ".3gp" video format security application is also expected for learning how a cryptography algorithm working especially the Noekoen cryptography algorithm and also the advantages by using this algorithm from research.

Keywords : Cryptography, encryption, decryption, 3gp video format, Noekeon Cryptography Algorithm

I. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi dari waktu ke waktu kian meningkat. Kebutuhan manusia akan perangkat informasi dan komunikasi seakan menjadi kebutuhan yang tidak terpisahkan dalam kehidupan sehari-hari. Inovasi yang terjadi dalam bidang ini senantiasa berkembang secara dinamis. Salah satu contohnya adalah pada saat mengirimkan data berupa video yang berekstensi *"3gp"* pada jaringan komputer, dimana video yang berekstensi *"3gp"* sudah umum digunakan tidak hanya pada komputer tetapi juga pada perangkat mobile dan *size* video yang berekstensi *"3gp"* lebih kecil di bandingkan *size* video yang lainnya.

Jaringan komputer pada awalnya dikembangkan untuk menghubungkan antar pihak yang saling mempercayai, dengan tujuan untuk saling menukar informasi (data). Dengan seiring berjalannya waktu dan berkembangnya teknologi dan komunikasi sehingga menyebabkan tingkat ancaman dalam keamanan informasi dan komunikasi menjadi semakin tinggi yaitu masalah keamanan data. Keamanan dari suatu data merupakan hal yang perlu diperhatikan dalam menjaga kerahasiaan informasi terutama yang berisi informasi yang hanya boleh diketahui isinya oleh pihak yang berhak saja. Pengiriman data atau informasi tanpa dilakukan pengamanan akan beresiko terhadap penyadapan dan informasi yang ada di dalamnya dapat mudah diketahui oleh pihak-pihak yang tidak berhak.

Hingga saat ini kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu data yaitu dengan menyandikan isi informasi menjadi isi yang sulit bahkan tidak dipahami dengan cara melalui proses enkripsi *(encryption)*, dan untuk memperoleh kembali informasi yang asli dilakukan proses dekripsi *(decryption)*, disertai dengan menggunakan kunci yang benar. Namun sejalan dengan perkembangan ilmu penyandian atau kriptografi, usaha - usaha untuk memperoleh kunci tersebut dapat dilakukan oleh siapa saja, termasuk pihak yang tidak sah untuk memiliki informasi tersebut.

Adapun macam-macam algoritma kriptografi seperti algoritma *Noekeon*, algoritma *RSA*, algoritma *ElGamal*, algoritma *DES*, dll, dimana salah satu contoh algoritma kriptografi adalah algoritma kriptografi *Noekeon*, algoritma kriptografi *Noekeon* merupakan *block cipher* berulang dengan panjang blok dan panjang kunci masing-masing 128 bit yang berjalan dalam 16 putaran, Dalam setiap putarannya dilakukan empat buah transformasi yaitu *theta*, *shift operations* yang terdiri dari dua buah transformasi *Pi1* dan *Pi2*, dan *gamma*, algoritma kriptografi *Noekeon* ini juga jarang digunakan untuk mengamankan video yang berekstensi *"3gp"*. Oleh karena masalah keamanan yang masih kurang pada saat pengiriman data atau informasi terutama untuk video yang berekstensi *".3gp"*, maka peneliti mengambil judul "Pengamanan Video Format 3gp Menggunakan Algoritma Kriptografi *Noekeon*", dimana program aplikasi ini menggunakan algoritma kriptografi *Noekeon* untuk mengamankan data berupa video yang berekstensi *".3gp"* sehingga video yang berekstensi

".3gp" tersebut tidak dapat di pahami dan pihak yang tidak berhak atas video tersebut tidak dapat mengetahui isi dari video tersebut.

II. METODA PENELITIAN

Untuk dapat mengimplementasikan sistem diatas, maka secara garis besar di gunakan beberapa metode sebagai berikut :

1. Studi Literatur dan Teori Penunjang
   Untuk memperoleh informasi dengan mempelajari buku-buku literatur atau karya lainnya yang membahas tentang kriptografi atau untuk menunjang pembuatan perangkat lunak yang berhubungan dengan materi penulisan.

2. Penerapan metode algoritma Noekeon dalam perancangan sistem.

3. Analisa permasalahan
   Untuk mengetahui dan menentukan metode algoritma yang digunakan sehingga dapat menentukan cara yang paling efektif dalam penyelesaian suatu permasalahan dalam proses enkripsi maupun dekripsi.

4. Pembuatan aplikasi pengaman suatu file

Setelah menganalisa permasalahan, selanjutnya dilakukan perancangan atau pembuatan sistem dengan menggunakan model perancangan sistem yang telah diterapkan agar sistem hasilnya akan maksimal dan dapat digunakan oleh *user* dengan mudah

III. PEMBAHASAN DAN HASIL

3.1 *Third Generation Project* (3GP)

Format video 3GP merupakan format video untuk *mobile phone* dengan kompresi yang tinggi sehingga memiliki ukuran yang kecil namun dengan kualitas gambar yang cukup lumayan.

3.2 Proses Enkripsi *Noekeon*

Berikut merupakan tahapan dari proses enkripsi dengan menggunakan algoritma kriptografi *Noekeon* :

1. Ubah *plaintext* dan kunci menjadi blok biner dengan panjang 128 bit atau dalam heksadesimal sebanyak 32 karakter. Untuk panjang blok yang tidak sesuai 128 bit lakukan proses padding yaitu dengan menambahkan bit "0".

2. *State*
   Pembagian blok biner *plaintext* dan kunci 128 bit menjadi empat buah 32 bit *word* yaitu a[0], a[1], a[2] dan a[3] dan k[0], k[1], k[2], k[3]
3. Untuk i = 0 sampai 15 lakukan proses 4,5,6,7 dan 8.
4. a0 = a0 xor rc[i]
5. *Theta(k,a)*
   Temp = a0 ⊕ 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
6. *Pi1(a)*
   a1 = a1 <<< 1
   a2 = a2 <<< 5
   a3 = a3 <<< 2
7. *Gamma(a)*
   a1 = a1 ⊕ ¬ (a3 v a2)
   a0 = a0 ⊕ (a2 ^ a1)
   temp = a3
   a3 = a0
   a0 = temp
   a2 = a2 ⊕ a0 ⊕ a1 ⊕ a3
   a1 = a1 ⊕ ¬ (a3 v a2)
   a0 = a0 ⊕ (a2 ^ a1)
8. *Pi2(a)*
   a1 = a1 >>> 1
   a2 = a2 >>> 5
   a3 = a3 >>> 2
9. a0 = a0 xor rc[16]
10. *Theta(k,a)*
    Temp = a0 ⊕ 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

11. Dari nilai a0,a1,a2 dan a3 yang baru ubah kedalam bentuk karakter dan akan menghasilkan sebuah *ciphertext* atau karakter baru hasil enkripsi dari *plaintext.*

3.3 Proses Dekripsi *Noekeon*

Berikut merupakan tahapan dari proses dekripsi dengan menggunakan algoritma kriptografi *Noekeon* :

1. Ubah *ciphertext* dan kunci menjadi blok biner dengan panjang 128 bit atau dalam heksadesimal sebanyak 32 karakter. Untuk panjang blok yang tidak sesuai lakukan proses *padding* yaitu dengan menambahkan bit "0".

2. *State*
   Pembagian blok biner *plaintext* dan kunci 128 bit menjadi empat buah 32 bit *word* yaitu a[0], a[1], a[2] dan a[3] dan k[0], k[1], k[2], k[3]

3. *Theta(NullVector,k)*
   Dari proses *Theta(NullVector,k)* ini akan dihasilkan nilai kunci yang baru *(k')*.
   Temp = a0 ⊕ 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

4. Untuk i = 16 sampai 1 lakukan proses 5,6,7,8 dan 9.

5. *Theta(k',a)*
   Temp = a0 ⊕ a2
   Temp = temp ⊕ (temp <<< 8) ⊕ (temp >>> 8)
   a1 = a1 ⊕ temp
   a3 = a3 ⊕ temp
   a0 = a0 ⊕ k'0
   a1 = a1 ⊕ k'1

a2 = a2 ⊕ k'2
a3 = a3 ⊕ k'3
temp = a1 ⊕ a3
temp = temp ⊕ (temp <<< 8) ⊕ (temp >>> 8)
a0 = a0 ⊕ temp
a2 = a2 ⊕ temp

6. a0 = a0 xor rc[i]

7. *Pi1(a)*
   a1 = a1 <<< 1
   a2 = a2 <<< 5
   a3 = a3 <<< 2

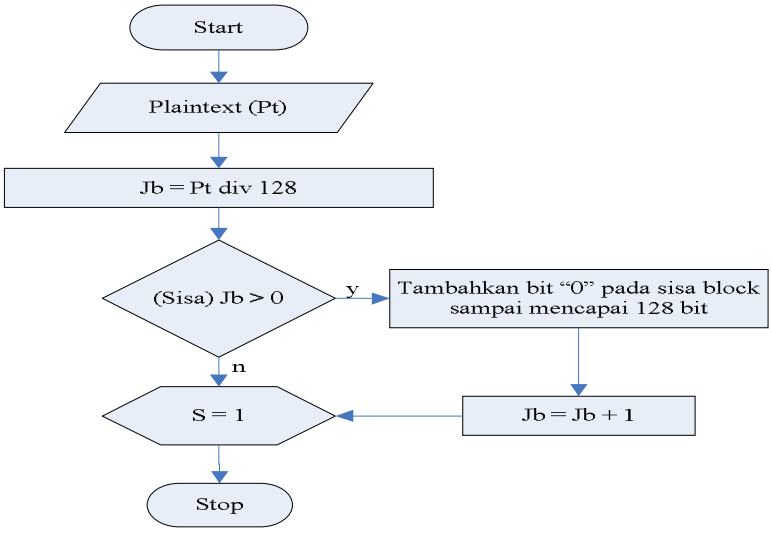
8. *Gamma(a)*
   a1 = a1 ⊕ ¬ (a3 v a2)
   a0 = a0 ⊕ (a2 ^ a1)
   temp = a3
   a3 = a0
   a0 = temp
   a2 = a2 ⊕ a0 ⊕ a1 ⊕ a3
   a1 = a1 ⊕ ¬ (a3 v a2)
   a0 = a0 ⊕ (a2 ^ a1)

9. *Pi2(a)*
   a1 = a1 >>> 1
   a2 = a2 >>> 5
   a3 = a3 >>> 2

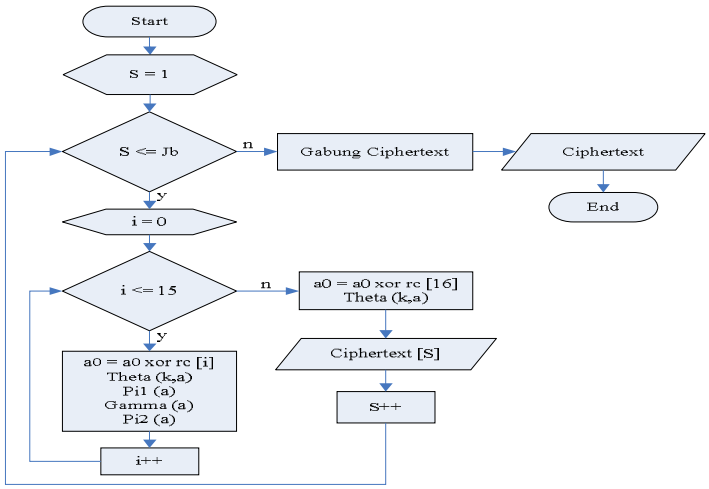
10. *Theta(k',a)*
    Temp = a0 ⊕ a2
    Temp = temp ⊕ (temp <<< 8) ⊕ (temp >>> 8)
    a1 = a1 ⊕ temp
    a3 = a3 ⊕ temp
    a0 = a0 ⊕ k'0
    a1 = a1 ⊕ k'1
    a2 = a2 ⊕ k'2
    a3 = a3 ⊕ k'3
    temp = a1 ⊕ a3
    temp = temp ⊕ (temp <<< 8) ⊕ (temp >>> 8)
    a0 = a0 ⊕ temp
    a2 = a2 ⊕ temp

11. a0 = a0 xor rc[0]

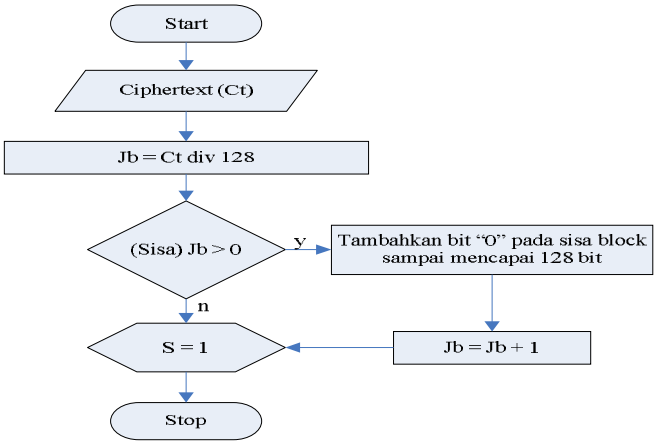
Dari nilai a0,a1,a2 dan a3 yang baru ubah kedalam bentuk karakter dan akan menghasilkan sebuah *plaintext* atau karakter baru hasil dekripsi dari *cipher*



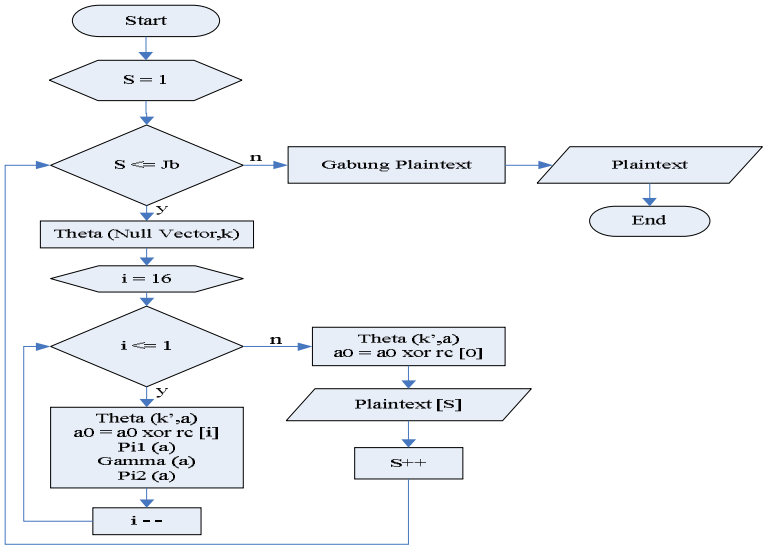
Gambar 1 Flowchart Pembentukan Jumlah Blok Pada Proses Enkripsi Algoritma Kriptografi *Noekeon*



Gambar 1 Flowchart Pembentukan Ciphertext Pada Proses Enkripsi Algortima Kriptografi *Noekeon*



Gambar 3 Flowchart Pembentukan Jumlah Blok Pada Proses Dekripsi Algoritma Kriptografi *Noekeon*

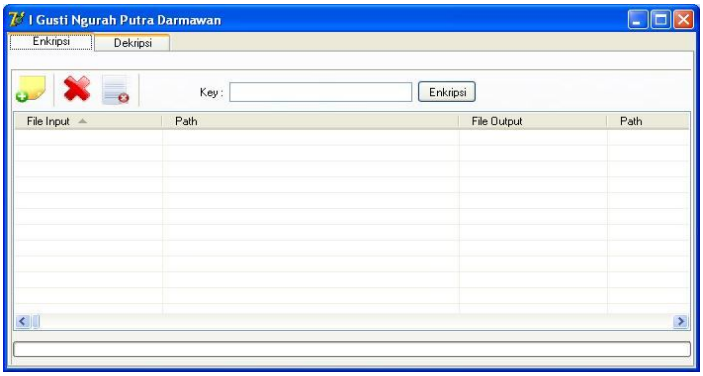


Gambar 4 Flowchart Pembentukan *Plaintext* Pada Proses Dekripsi Algortima Kriptografi *Noekeon*

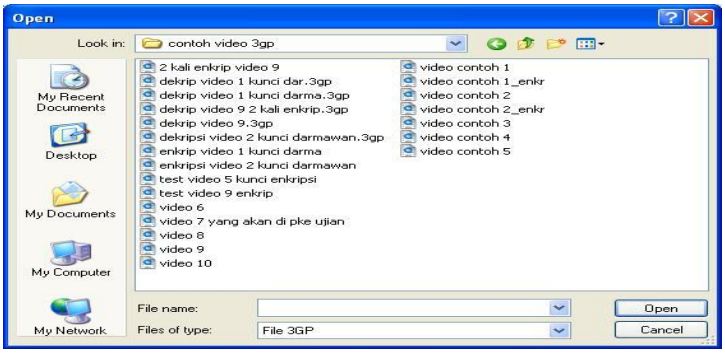
IV. IMPELEMENTASI HASIL

4.1 Tampilan Utama

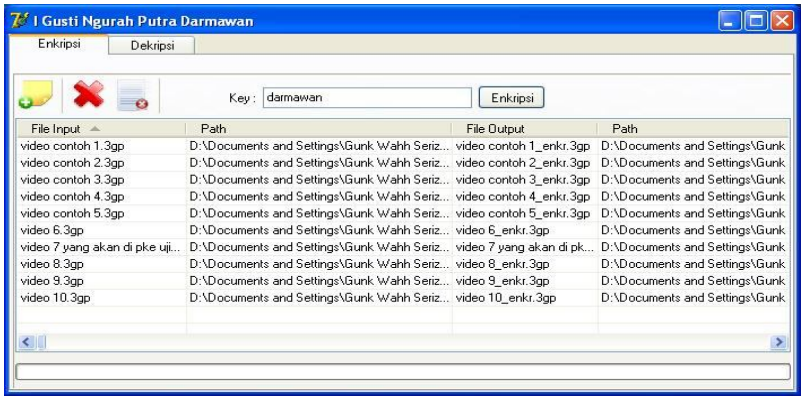
Berikut merupakan tampilan utama dari pengamanan video format *".3gp"* menggunakan algoritma kriptografi *Noekeon*



Gambar 5 Tampilan Utama Program Enkripsi

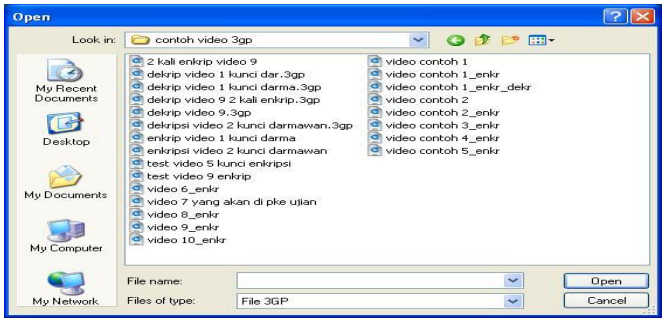


Gambar 6 Pemilihan File



Gambar 7 Proses Enkripsi

Hasil dari proses enkripsi akan tetap tersimpan dalam format *".3gp"* dan akan tersimpan dengan nama *file "nama file_enkr.3gp"* sebagai penanda bahwa video tersebut hasil telah dilakukan proses enkripsi.



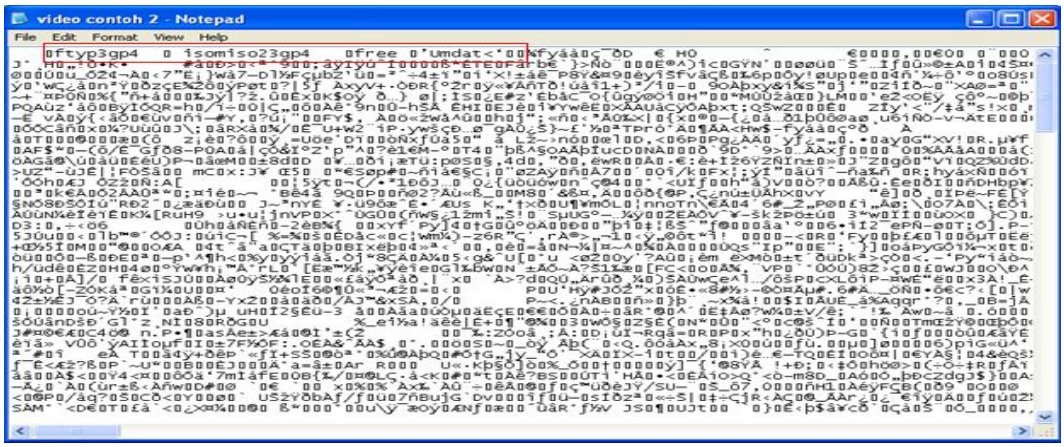
Gambar 8 Tampilan Utama Program Dekripsi

jika tidak memilih video yang akan diproses dan *list* masih kosong tidak terdapat video yang akan diproses dan langsung mengklik tombol dekripsi akan tampak pemberitahuan seperti pada gambar 13.

Gambar 9 Kotak Dialog Tidak Terdapat Video yang Akan Diproses

Penanda bahwa video tersebut hasil telah dilakukan proses enkripsi dan dekripsi.

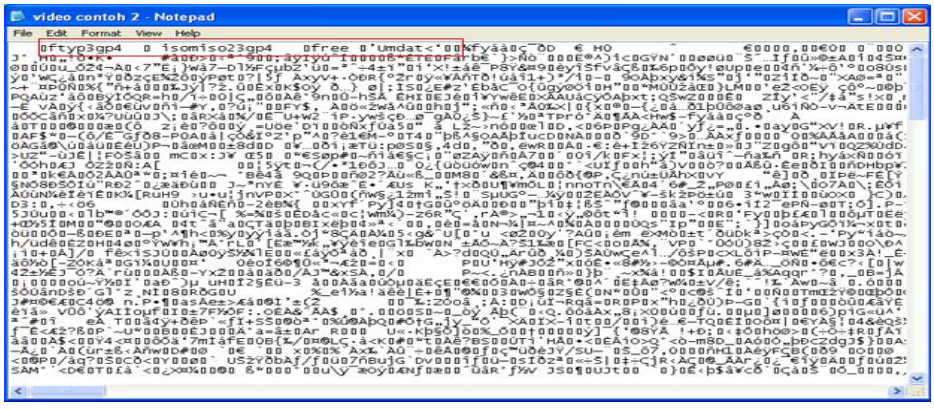
4.2.1 Video Hasil Enkripsi dan Video Hasil Dekripsi



Gambar 10 Isi Dari Video Asli

Gambar 11 Isi Dari Video Hasil Enkripsi

4.2.2 Video Asli dan Video Hasil Dekripsi



Gambar 12 Isi Dari Video Asli

Gambar 13 Isi Dari Video Hasil Dekripsi

V. SIMPULAN

Adapun kesimpulan yang dapat diambil dari penelitian pengamanan video berekstensi *".3gp"* dengan menggunakan algoritma kriptografi *Noekeon* adalah Aplikasi yang sudah dikembangkan dapat menyandikan informasi dari video berekstensi *".3gp"* menjadi *".3gp"* yang tidak dapat dipahami sehingga pihak yang tidak berhak atas video tersebut tidak dapat mengetahui isi dari video tersebut, disamping itu aplikasi ini juga mampu mengembalikan hasil video yang tidak dapat dipahami tersebut menjadi dapat dipahami kembali

5.1 SARAN PENULIS

Adapun saran untuk pengembangan sistem yang dibuat antara lain :

1. Sistem yang dibuat diharapkan dapat diimplementasikan dalam sebuah pengiriman data pada jaringan komputer.
2. Sistem dapat memberikan informasi mengenai *file ciphertext* yang dihasilkan sehingga nantinya penerima pesan dapat memastikan keaslian pengirimnya.
3. Diharapkan kedepannya aplikasi ini dapat dikembangkan sehingga dapat berjalan pada system operasi lain, seperti : Linux atau Solaris.

VI DAFTAR PUSTAKA

[1] Bahri, Kusnassriyanto Saiful dan Wawan Sjachriyanto, 2008 "Teknik Pemrograman DELPHI", Bandung, Informatika

[2] Budiono, Avon, "Keamanan Sistem Lanjut", 2004 Bandung

[3] Daemen, Joan., Peeters, Michaël., Van Assche, Gilles., and Rijmen, Vincent. "*NOEKEON block cipher, Nessie proposal*",

[4] HM, Jogiyanto. 2005. *Analisis & Desain Sistem Informasi: Pendekatan Terstruktur Teori dan Praktek Aplikasi Bisnis*. Yogyakarta: CV Andi Offset.

[5] Kurniawan, Yusuf, 2004. "KRIPTOGRAFI : Keamanan Internet dan Jaringan Komunikasi", Bandung, Informatika,