IMPLEMENTASI ALGORITMA KRIPTOGRAFI HC-128 PADA VIDEO ON DEMAND (VOD) BERBASIS DIGITAL RIGHTS MANAGEMENT (DRM) IMPLEMENTATION OF CRYPTOGRAPHIC ALGORITHM HC-128 IN VIDEO ON DEMAND (VOD) BASED DIGITAL RIGHTS MANAGEMENT (DRM)

[1]Rifkha Junianty Arief **[2]Surya Michrandi N., S.T, M.T** **[3]Tito Waluyo Purboyo, S.T, S.Si., M.Pmat**

1104110054 **13861155-1** **14731529-1**

[123]Prodi S1 Teknik Komputer, Fakultas Teknik Elektro, Universitas Telkom
Jl. Telekomunikasi, Dayeuh Kolot, Bandung 40257, Indonesia

[11]rifkha.arief@gmail.com, [2]michrandi@telkomuniversity.ac.id, [3]titowaluyo@telkomuniversity.ac.id

ABSTRAK

Perkembangan teknologi saat ini berkembang sangat pesat khususnya penyebaran konten digital seperti video khususnya video on demand di internet. Hal tersebut memungkinkan masyarakat mengakses konten digital tersebut kapanpun dan dimanapun masyarakat berada. Konten digital tersebut tidak lepas dari pembajakan atau penggandaan oleh orang-orang yang tidak memiliki akses untuk memilikinya, oleh karena itu dibutuhkan system keamanan seperti ilmu kriptografi dan DRM (Digital Right Management) yang berguna untuk melindungi hak akses, mencegah suatu konten digital dari pembajakan dan membantu dalam proses penyembunyian pesan atau data. Dalam penilitan ini, akan menggunakan algoritma kriptografi HC-128. Algoritma kriptografi HC-128 adalah salah satu dari empat algoritma yang dipilih di kompetisi eStream untuk aplikasi perangkat lunka. Algoritma HC-128 menghasilkan sebuah keystream dengan 128 bit kunci dan 128 bit kunci inisasi vektor.
Tugas Akhir ini meneliti tentang performansi dari algoritma kriptografi HC-128 pada Video on Demand. Proses penelitian dilakukan dengan membuat program menggunakan Netbeans IDE 8.0.2.

Kata Kunci : Kriptografi, HC-128 Video on Demand, DRM (Digital Right Management)

ABSTRACT

The development of technology is developing very rapidly especially to disseminate content such as digital video especially video on demand in the internet. It allows people to access digital content was whenever and wherever they are. Digital content is not free from the hijacking or cloning by those who do not have access to possess, because they are needed security system such as knowledge cryptography and DRM (Digital Rights Management) which is useful to protect the rights access, to prevent a digital content from piracy and help in the process concealment message or data. In this research, will use crypthography algorithm HC-128. Crypthography algorithm HC-128 is one of the four algorithm that was chosen in the competition eStream for the application software. Algorithm HC-128 results in a 128-bit keystream with key and 128-bit initialisation key vector.
This final project examines about performance of crypthography algorithm HC-128 in Video on Demand. The research was done to make programs using Netbeans IDEAS 8.0.2.

Keywords : Criptography, HC-128, *Video on Demand, DRM (Digital Right Management)*

1. PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi saat ini berkembang sangat pesat khususnya penyedia informasi seperti internet. Dengan adanya internet, memudahkan masyarakat untuk memperoleh dan berbagi informasi kapanpun dan dimanapun masyarakat berada. Di sisi lain, penyebaran internet membuat data multimedia seperti musik , gambar, dan khususnya video menyebar dengan begitu banyak dan menimbulkan ancaman bagi pihak-pihak tertentu. Ancaman yang timbul adalah masalah hak cipta, status kepemilikan, dan HAKI (Hak Kekayaan Intelektual). Masalah tersebut muncul diakibatkan oleh pembajakan atau penggandaan video tanpa izin dari pihak terkait dalam hal ini adalah Video On Demand. Karena video tersebut bisa diakses oleh siapa saja maka dibutuhkan suatu teknologi yang disebut DRM (Digital Right Management) dan kriptografi untuk mencegah pembajakan hak cipta, menyalin secara ilegal [1], dan mengatur hak akses yang diberikan kepada mahasiswa ataupun dosen serta membantu dalam proses penyembunyian pesan. Teknologi DRM berfungsi untuk mengontrol penggunaan media digital dengan mencegah akses, menyalin, dan tindakan yang melanggar hak cipta lainnya. Sedangkan kriptografi merupakan salah satu teknologi dalam keamanan suatu sistem yang bertujuan untuk membantu dalam proses penyembunyian pesan atau data dengan cara mengenkripsi dan mendekripsi data tersebut dengan syarat memiliki kunci yang sama untuk mendekripsinya.

Tugas Akhir ini meneliti tentang performansi dari algoritma kriptografi HC-128 pada Video on Demand. Algoritma kriptografi HC-128 adalah salah satu dari empat algoritma yang dipilih di kompetisi eStream untuk aplikasi perangkat lunak. Algoritma HC-128 menghasilkan sebuah keystream dengan 128 bit kunci dan 128 bit kunci inisiasi vektor. HC-128 stream cipher [2] terdiri dari dua tabel rahasia, masing-masing dengan 512 bit untuk masing-masing elemen terdiri dari 32-bit. Setiap langkah memperbarui satu elemen dari tabel dengan fungsi umpan balik non-linear. Semua elemen dari dua tabel diupdate setiap 1.024 langkah. Pada setiap langkah, satu output 32-bit yang dihasilkan dari non-linear fungsi output filtering [3]. Proses penelitian dilakukan dengan membuat program menggunakan Netbeans IDE 8.0.2. Hasil keluaran dari implementasi ini adalah data uji performansi menggunakan lima parameter, yaitu avalanche effect, waktu proses enkripsi dan dekripsi, pengujian waktu normal video asli pada aplikasi, dan kualitas dari video yang kemudian akan dianalisis.

1.2 Perumusan Masalah

Penelitian Tugas Akhir ini berkonsentrasi pada implementasi algoritma kriptografi HC-128 pada Video on Demand yang terdiri dari permasalahan-permasalahan berikut:

1. Bagaimana mengimplementasikan algoritma kriptografi HC-128 pada konten digital seperti Video on Demand berbasis DRM (Digital Right Management)?
2. Bagaimana pengimplementasian DRM pada Video on Demand?
3. Bagaimana performansi algoritma HC-128 pada Video on Demand berbasis DRM?

1.3 Tujuan

Tujuan penulis membuat Tugas Akhir ini adalah sebagai berikut:

1. Mengetahui cara untuk mengimplementasikan algoritma kriptografi HC-128 pada konten digital seperti Video on Demand berbasis DRM,
2. Mengimplementasikan DRM pada konten digital seperti Video on Demand.
3. Mengetahui performansi algoritma kriptografi HC-128 pada Video on Demand berbasis Digital Right Management.

1.4 Batasan Masalah

Hal-hal yang dibatasi dalam penelitian Tugas Akhir ini adalah :

1. Algoritma yang digunakan adalah algoritma kriptografi HC-128
2. Client tidak terlibat dalam memasukkan kunci
3. Client terdiri dari client member dan client non member
4. Tipe data yang digunakan adalah video
5. Video yang digunakan berformat .mp4
6. Performansi yang diukur adalah alanisa avalanche effect, waktu proses enkripsi dan dekripsi, dan kualitas video
7. Pembobolan akun client member, server, dan database tidak dibahas
8. Video yang digunakan video tanpa suara

1.5 Metodologi Penyelesaian Masalah

Metodologi penelitian yang digunakan adalah:

1. Studi literatur, yaitu mempelajari literatur-literatur yang ada sesuai dengan permasalahan yang akan dibahas meliputi, konsep Video on Demand, konsep Digital Right Management (DRM), konsep kriptografi, teori algoritma kriptografi HC-128.
2. Konsultasi dengan dosen pembimbing terkait permasalahan dan kemungkinan solusi yang ditawarkan.
3. Perancangan sistem dan perancangan fungsionalitas serta pembuatan desain antarmuka bagi user dengan menggunakan bahasa pemograman java, Netbeans IDE 8.0.2.

4. Melakukan uji coba aplikasi yang telah dibuat, serta menganalisa masalah-masalah yang muncul, serta melakukan perbaikan terhadap masalah-masalah tersebut. Uji performansi menggunakan parameter waktu enkripsi dan dekripsi, avalanche effect dan kualitas video.
5. Pembuatan laporan dari hasil penelitian

2. DASAR TEORI

2.1 Video

Video merupakan suatu teknologi yang berfungsi untuk menangkap, merekam, memproses, ataupun mentransmisikan dan menata ulang gambar bergerak yang biasa disebut gambar-gambar mati yang dibaca berurutan dalam suatu waktu dan dalam kecepatan tertentu. Video terbagi atas dua jenis, yaitu:

1. Video Analog, Analog video tersusun dari gelombang bersambung yang bervariasi, dengan kata lain nilai sinyal akan memiliki angka yang beragam tetapi terbatas pada batas maksimum dan minimum yang diijinkan
2. Video Digital, digital video ditransmisikan hanya berupa titik presisi yang dipilih pada interval dalam kurva. Tipe sinyal digital yang dapat dipakai oleh komputer kita adalah tipe *binary*. Data *binary* diwakili dengan angka 1 dan 0, angka 1 mewakili nilai maksimum dan angka 0 mewakili nilai minimum.

2.2 Video on Demand (VoD)

Video On Demand adalah sebuah penyajian video yang bisa diakses secara *online* melalui jaringan dimana pengguna dapat melihat video dimana saja dan kapan saja. video bisa disajikan secara *streaming* ataupun di *download*. Selain itu, pengguna dapat memilih untuk menghentikan sementara (*pause*), *play*, *fast forward*, atau *rewind video*. Pengguna juga dapat memilih untuk melewatkan (*skip*) adegan-adegan (*scenes*) tertentu.

2.3 Digital Right Management (DRM)

Digital Rights Management (DRM) adalah suatu sistem pengamanan untuk mencegah penggandaan secara ilegal musik yang telah di-download. Apabila pemegang hak cipta mempunyai hak eksklusif untuk suatu file, seperti hak untuk mendistribusikan suatu file kepada publik, DRM mengatur pula bagaimana file itu akan digunakan. DRM beroperasi dalam mengontrol hak cipta untuk suatu isi file dan mengatur distribusi dari isi file yang dilindungi tersebut

2.4 Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu crypto yang berarti rahasia dan graphia yang berarti tulisan. menurut terminologinya kriptogtafi adalah ilmu dan sen untuk mejaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain [4]. dengan kata lain kriptografi memastikan agar informasi atau pesan rahasia yang dikirimkan tidak diketahui oleh orang lain. Kriptografi terdiri dari beberapa komponen, yaitu:

1. Enkripsi - Dekripsi, merupakan proses mengamankan informasi atau pesan dengan mengubah pesan atau informasi yang asli menjadi kode-kode yang tidak dimengerti oleh orang lain. Sedangkan dekripsi merupakan kebalikan dari enkripsi yaitu proses mengembalikan kode-kode yang tidak dimengerti tersebut menjadi bentuk asalnya yaitu informasi yang utuh, sehingga penerima informasi bisa mengetahui informasi apa yang diterima.
2. Kunci (Key), merupakan kunci yang dipakai untuk melakukan proses enkripsi dan dekripsi. kunci terdiri dari 2 bagian yaitu:
    a. kunci rahasia (private key)
    b. kunci umum (public key)
3. Ciphertext – Plaintext, ciphertext merupakan hasil dari proses enkripsi yang merupakan kode-kode yang terdiri dari karakter-karakter yang tidak memiliki arti atau makna. Sedangkan plaintext merupakan hasil dari proses dekripsi yaitu pesan atau informasi utuh yang memiliki arti atau makna. Untuk melakukan proses tersebut menggunakan algoritma kriptografi.

2.4.1. Algoritma Kriptografi HC-128

Kode aliran HC-128 adalah salah satu algoritma empat yang dipilih dalam kompetisi eStream untuk aplikasi perangkat lunak [5]. HC--128 menghasilkan sebuah keystream algoritma dengan panjang hingga 2^{64} bit dengan 128 bit untuk kunci dan 128 bit untuk initialitation vector. HC-128 kode aliran terdiri dari dua tabel rahasia, masing-masing dengan 512 bit untuk elemen-elemen 32-bit. Setiap langkah-langkah akan memperbarui elemen tabel menggunakan non-linear fungsi umpan balik. Semua elemen-elemen kedua loh diperbarui setiap 1024 langkah-langkah-langkah, dan masing-masing akan menghasilkan 32 bit output dari non-linear fungsi penyaringan keluaran.

2.4.2.1. Operasi, Variable dan Fungsi

Operasi ini digunakan dalam HC-128:

+ : x + y berarti x + y mod 232, where $0 \le x < 232$ and $0 \le y < 232$
$\boxminus$: x $\boxminus$ y berarti x − y mod 512
$\oplus$: operasi XOR
$\|$: concatenation
>> : bergeser ke kanan. x >> n berarti x digeser ke kanan sebanyak n bit.
<< :bergeser ke kiri. x << n berarti x digeser ke kiri sebanyak n bit.
>>> : putar ke kanan. x >>> n artinya ((x >> n) $\oplus$ (x << (32−n)), dimana $0 \le n < 32$, $0 \le x < 2^{32}$.

<<< : putar ke kiri. x <<< n artinya ((x << n) ⊕ (x >> (32−n)), dimana $0 \leq n < 32$, $0 \leq x < 2^{32}$.

Ada dua S-box dalam HC-128 rahasia yang dipegang, P dan Q. masing-masing berisi 512 32-bit elemen yang digunakan sebagai langkah internal HC-128.

P : tabel dengan 512 32-bit elemen. Setiap elemen atau unsur ditandai sebagai P[i], dengan $0 \leq i \leq 511$.

Q : tabel dengan 512 32-bit elemen. Setiap elemen atau unsur ditandai sebagai Q[i], dengan $0 \leq i \leq 511$.

K : 128-bit kunci dari HC-128.

IV : 128-bit inisialisasi vektor dari HC-128.

s : hasil keystream dari HC-128. keluaran 32-bit dari langkah ke-i ditandai dengan si. dimana s = s0 ‖ s1 ‖ s2 ‖ ⋯

128-bit kunci array K[0, . . . , 3] dan 128-bit inisialisasi vector IV [0, . . . , 3] digunakan, di mana setiap masukan dari array merupakan elemen dari 32-bit. st ditandai sebagai keystream yang dibuat oleh langkah ke-i, i = 0, 1, 2, . . .

Berikut fungsi yang digunakan dalam HC-128:

f1(x) = (x >>> 7) ⊕ (x >>> 18) ⊕ (x >> 3) (1)

f2(x) = (x >>> 17) ⊕ (x >>> 19) ⊕ (x >> 10) (2)

g1(x, y, z) = ((x >>> 10) ⊕ (z >>> 23)) + (y <<< 8) (3)

g2(x, y, z) = ((x <<< 10) ⊕ (z <<< 23)) + (y <<< 8) (4)

h1(x) = Q[x0] + Q[256 + x2] (5)

h2(x) = P[x0] + P[256 + x2] (6)

f1(x) dan f2(x) adalah sama dengan σ0{256}(x) dan σ1{256}(x) yang digunakan pada penjadwalan pesan dari SHA-256. Untuk h1(x), tabel Q digunakan di S-box. For h2(x), tabel P digunakan di S-box. Dimana x = x3 ‖ x2 ‖ x1 ‖ x0, x adalah 32-bit kata, x0, x1, x2 dan x3 merupakan empat byte. x3 dan x0 menunjukkan Most Significant Byte dan Least Significant Byte dari x.

2.4.2.2. Inisialisasi Proses

Dalam proses inisialisasi HC-128 terdiri dari perluasan kunci dan inisialisasi vector ke P dan Q menjalankan kode 1024 langkah:

1. Tentukan K = K0 ‖ K1 ‖ K2 ‖ K3 dan IV = IV0 ‖ IV1 ‖ IV2 ‖ IV3, dimana setiap Ki dan IVi terdiri dari 32-bit angka. Tentukan Ki+4 = Ki, dan IVi+4 = IVi untuk $0 \leq i < 4$. Key dan IV diperluas ke dalam array Wi ($0 \leq i \leq 1279$) yaitu:.

$$W_i = \begin{cases} Ki & 0 \leq i \leq 7 \\ IVi - 8 & 8 \leq i \leq 15 \\ f2(Wi-2) + Wi-7 + f1(Wi-15) + Wi-16 + i & 16 \leq i \leq 1279 \end{cases} \quad (7)$$

2. Memperbarui table P dan Q ke dalam array W.
   P[i] = Wi+256 for $0 \leq i \leq 511$ (8)
   Q[i] = Wi+768 for $0 \leq i \leq 511$
3. Menjalankan 1024 langkah dan menggunakan keluaran untuk mengganti elemen-elemen tabel.
   for i = 0 to 511, do (9)
   P[i] = (P[i] + g1(P[i ⊟ 3], P[i ⊟ 10], P[i ⊟ 511]))⊕ h1(P[i ⊟ 12]);
   for i = 0 to 511, do
   Q[i] = (Q[i] + g2(Q[i ⊟ 3], Q[i ⊟ 10], Q[i ⊟ 511])) ⊕ h2(Q[i ⊟ 12]);

2.4.2.3. Pembangkitan Kunci

Setelah initialisasi dilakukan, keystream siap untuk dibangkitkan atau dibuat. Di setiap langkah, satu elemen tabel diperbarui dan satu keluaran 32-bit dibuat. Setiap S-box digunakan untuk menghasilkan hanya 512 keluaran, kemudian S-box diperbarui dalam 512 langkah-langkah berikutnya.

i = 0; (10)

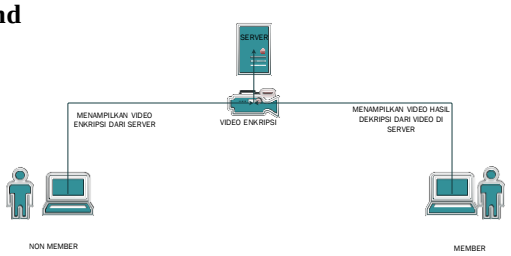
berulang sampai keystream sudah cukup untuk diubah.{
j = i mod 512;
if (i mod 1024) < 512
{
P[j] = P[j] + g1(P[j ⊟ 3], P[j ⊟ 10], P[j ⊟ 511]);
si = h1(P[j ⊟ 12]) ⊕ P[j];
}
else
{
Q[j] = Q[j] + g2(Q[j ⊟ 3], Q[j ⊟ 10], Q[j ⊟ 511]);
si = h2(Q[j ⊟ 12]) ⊕ Q[j];
}
end-if
i = i + 1;
}
end

2.4.2.4. Enkripsi dan Dekripsi

Untuk enkripsi, dapat dilakukan dengan melakukan XOR antara pesan yang ingin dienkripsi dengan keystream yang telah dihasilkan. Untuk dekripsi, dilakukan dengan melakukan XOR antara chipertext yang ingin didekripsi dengan keystream yang dihasilkan.

3. ANALISA DAN PERANCANGAN SISTEM

3.1 Sistem Aplikasi Video on Demand



Gambar 3.1 Sistem Aplikasi Video on Demand

Pada aplikasi Video on Demand berbasis Digital Right Management yang dibuat terdapat perbedaan hak akses dari segi pengguna yaitu terdapat dua pengguna antara lain adalah pengguna non-member dan pengguna member. pengguna non-member hanya bisa mengakses video yang sudah terenkripsi karena pengguna non-member tidak memiliki hak penuh untuk melihat video secara utuh. Sedangkan pengguna member dapat mengakses dan menampilkan video yang sudah terdekripsi. Untuk melakukan proses enkripsi dan dekripsi terhadap video tersebut, penulis menggunakan algoritma kriptografi HC-128.

3.2 Proses Enkripsi dan Dekripsi

Untuk melakukan proses enkripsi pada file video menggunakan algoritma HC-128, tahap pertama yang dilakukan adalah memecah video asli menjadi frame-frame sesuai dengan frame yang dimiliki video tersebut. Proses enkripsi kemudian dilakukan dengan melakukan proses XOR dari keystream yang dihasilkan dari algoritma HC-128 dengan frame-frame yang sudah dipecah dari bentuk video asli. Setelah proses enkripsi selesai, tahap selanjutnya yang dilakukan adalah menggabungkan frame yang sudah terenkripsi menjadi video kembali dan begitupun sebaliknya.

3.3 Skenario Pengujian

Skenario pengujian dibagi menjadi 5 yaitu, pengujian waktu enkripsi, pengujian waktu dekripsi, dan pengujian keamanan sistem. keamanan sistem diukur berdasarkan Avalance Effect, pengujian waktu normal video pada aplikasi, dan pengujian kualitas video. Adapun skenario pengujian yang akan dilakukan pada aplikasi ini adalah:

1. Skenario pengujian waktu enkripsi dan dekripsi
   5 file video berekstensi .MP4 dienkripsi menggunakan panjang kunci 128 bit dengan melakukan 15 kali percobaan, dan 5 file video terenkripsi di dekripsi menggunakan panjang kunci 128 bit dengan melakukan pengujian berulang sebanyak 15 kali
2. Skenario pengujian Avalanche Effect
   Avalanche Effect dihitung menggunakan panjang kunci 128 bit dengan ketentuan waktu dalam menit.
3. Skenario pengujian waktu normal video asli pada aplikasi
   Pengujian waktu normal video asli pada aplikasi yaitu waktu yang dibutuhkan aplikasi untuk menjalankan video yang diterima dari server.
4. Skenario pengujian kualitas video
   Pengujian kualitas video yaitu pengujian yang bertujuan untuk membandingkan kualitas video asli, video terenkripsi dan video yang telah terdekripsi.

4. Pengujian dan Analisis

Pengujian dilakukan dengan berbagai skenario untuk mengetahui dan menganalisis apakah metode yang digunakan dapat diimplementasikan pada aplikasi Video on Demand. Pengujian dilakukan untuk dapat mengetahui dan menganalisis performansi algoritma kriptografi HC-128 pada video.

4.1 Pengujian Sistem

Pengujian dilakukan dengan berbagai skenario untuk mengetahui dan menganalisis apakah metode yang digunakan dapat diimplementasikan pada aplikasi Video on Demand. Pengujian dilakukan untuk dapat mengetahui dan menganalisis performansi algoritma kriptografi HC-128 pada video**.**

4.1.1. Pengujian Performansi

4.1.1.1. Pengujian Waktu Enkripsi dan Dekripsi

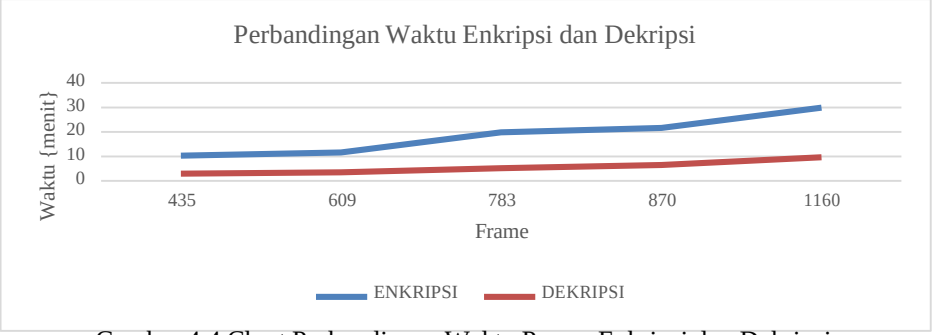
Untuk mengetahui performansi dari algoritma kriptografi HC-128 yang diimplementasikan ke Video on Demand adalah dengan mengukur hasil waktu enkripsi dari video tersebut. Berikut hasil rata-rata waktu enkripsi dari 5 video yang telah disediakan dengan melakukan pengujian berulang sebanyak 15 kali.:

Tabel 4. 1 Hasil Pengukuran Waktu Enkripsi

No	Nama Video	Ukuran	Durasi (*second*)	fps	Total *Frame*	Waktu Enkripsi (Menit)	Waktu Dekripsi
1.	Mad Max- Fury Road.mp4	1.95 MB	15	29	435	10,26	2,93
2.	batman vs supermen.mp4	1.39.MB	21	29	609	11,62	3,44
3.	Shia LaBeouf Mad Max JUST DO IT Motivational.mp4	2.83 MB	27	29	783	19,82	5,24
4.	Os Vingadores Kids - Comercial de Os Vingadores com Crianças.mp4	4.23 MB	30	29	870	21,63	6,45
5.	Smyths Toys Superstores mini-avengers TV commercial.mp4	6.05 MB	40	29	1160	29,88	9,69

Berdasarkan tabel pengujian waktu enkripsi HC-128 yang diimplementasikan pada Video on Demand, terlihat bahwa besar total frame suatu video mempengaruhi lama atau cepatnya waktu enkripsi. Semakin besar jumlah frame suatu video, maka semakin lama pula waktu yang dibutuhkan untuk mengenkripsi video tersebut. Hal ini dikarenakan oleh data yang dienkripsi dari video tersebut adalah data yang berupa frame, dan bukan data video secara keseluruhan.Dalam hal ini dapat disimpulkan bahwa perbandingan waktu proses enkripsi dan dekripsi adalah proses enkripsi dari video tersebut membutuhkan waktu yang lebih lama dibandingkan dengan waktu untuk melakukan proses dekripsi dari video tersebut.

Berikut perbandingan antara hasil proses waktu enkripsi dan dekripsi pada Video on Demand menggunakan algoritma kriptografi HC-128:



Gambar 4.4 Chart Perbandingan Waktu Proses Enkripsi dan Dekripsi

4.1.1.2. Pengujian Waktu Video pada Non Member dan Member

Pengujian waktu video untuk non member ada waktu yang dibutuhkan aplikasi menjalankan video dari server. Berikut hasil pengujian terhadap waktu video untuk non member:

Tabel 4.3 Hasil Pengujian Waktu Video pada Non Member

No	Nama *Video*	Waktu Normal (menit)
1.	Mad Max- Fury Road.mp4	1,31
2.	Batman vs Superman.mp4	1,32
3	Shia LaBeouf Mad Max JUST DO IT Motivational	1,37
4.	Os Vingadores Kids.mp4	1,32
5.	Smyths Toys Superstores mini.mp4	1,34

Pada Tabel 4.3 diatas, waktu yang diperlukan untuk memutar video dari aplikasi yang dijalankan membutuhkan waktu kurang lebih 1 menit, sehingga pengguna non-member dapat memutar video dengan cepat dan tidak harus menunggu lama. Sedangkan waktu yang dibutuhkan dalam memutar video dari aplikasi yang dijalankan memiliki waktu proses yang sama dengan waktu dekripsi dalam program.

4.1.1.3. Pengujian Avalanche Effect

Setelah pelaksanaan dan algoritma pengujian HC-128 pada Video on Demand Avalanche Effect dihitung dengan menggunakan 2 bahan uji, yaitu:

1. pengujian Avalanche Effect yang pertama menggunakan 128 bit kunci dan 128 bit inisialisasi vektor (iv) untuk digunakan pada 15 video yang berberda. Kunci yang digunakan adalah 4F 46 12 9B 1A DF AD 32 5B 5C CB 46 9D 1A FB 87 sedangkan untuk iv yang digunakan adalah 11 81 BC A5 AD 1E 17 B4 45 24 83 85 36 BA AC 21

Tabel 4.4 Hasil pengukuran Avalance Effect dengan Menggunakan Kunci Sama

No.	Video	Jumlah bit beda	Avalanche Effect
1.	Mad Max- Fury Road	541	47,17%
2.	batman vs supermen.mp4	541	47,17%
3.	Shia LaBeouf Mad Max JUST DO IT Motivational.mp4	541	47,17%
4.	Os Vingadores Kids - Comercial de Os Vingadores com Crianças.mp4	541	47,17%
5.	Smyths Toys Superstores mini-avengers TV commercial.mp4	541	47,17%

Pada pengujian avalanche effect diatas dapat disimpulkan bahwa meskipun video yang diujikan berbeda-beda dengan meggunakan Key dan IV yang sama tetapi ciphertext yang dihasilkan berbeda-beda, meskipun seperti itu hasil dari avalanche effet akan tetap sama yaitu 47,17 %. Dengan kata lain algoritma HC-128 masih termasuk baik dan aman untuk diimplementasikan ke Video on Demand.

2. Pengujian Avalanche Effect yang kedua menggunakan 128 bit kunci yang berbeda pada setiap percobaannya dan 128 bit inisialisasi vektor (iv) dan video yang sama.

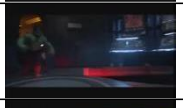
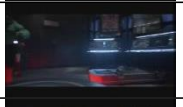
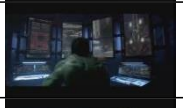
Tabel 4.5 Hasil pengukuran Avalance Effect dengan Menggunakan Kunci Berbeda

No	Key	Avalanche Effect
1	ED 35 76 DD 9F 6E 51 77 99 5B AF 33 AC AE 66 77	51% 499 bit changed
2	ED 35 76 DE 9F 6E 51 77 94 5B AF 33 AC AE 66 77	50,68% 505 bit changed
3	ED 35 76 DE 9F 6E 51 77 99 5C AF 33 AC AE 66 77	50% 512 bit changed
4	ED C5 76 DD 9F 6E 41 77 99 5B AF 33 AC AE 66 77	51,17% 500 bit changed
5	EE 35 76 DD 9F 6E 51 77 99 5B AF 33 AC AE 66 77	51,07% 501 bit changed
6	E0 35 76 DE 9F 6E 51 77 94 5B AF 33 AC AE 66 77	49,90% 513 bit changed
7	E0 35 76 DE 9F 6E 51 78 94 5B AF 33 AC AE 66 77	50,29% 509 bit changed
8	E0 35 76 DE FF 6E 51 7A 94 5B AF 33 AC AE 66 77	50,20% 510 bit changed
9	E0 35 76 DE FF 6E 51 7A 95 5B AF 33 AC AE 66 77	51,37% 498 bit changed
10	E0 35 76 DE FF 6E 51 7A 95 5B A3 A3 AC AE 66 77	50,29% 509 bit changed

4.1.1.4. Pengujian Kualitas Video

Pengujian kualitas video bertujuan untuk membandingkan hasil frame video yang telah diproses oleh algoritma HC-128 yaitu frame asli, frame hasil enkripsi dan frame dekripsi. Untuk membandingkan hasil gambar enkripsi dan dekripsi diambil beberapa sampel dari video "Os Vingadores Kids - Comercial de Os Vingadores com Criançasl.mp4" seperti pada tabel dibawah ini

Tabel 4.6 Perbandingan Frame Video Asli, Enkripsi, dan Dekripsi

Frame	Asli	Enkripsi	Dekripsi
41			
54			
61			
100			
120			

Dari perbandingan frame asli, enkripsi, dan dekripsi di atas, dapat dilihat frame hasil enkripsi tidak jelas dalam menampilkan gambar hal itu dikarenakan oleh hasil dari enkripsi algoritma yang telah dijalankan. Sedangkan untuk perbandingan frame asli dengan frame hasil dekripsi sudah menyerupai bentuk video aslinya, tetapi terjadi penurunan kualitas gambar dan warna. Pada frame 41 dan frame 54 terjadi penurunan kualitas gambar sebasar 25,51%, sedangkan untuk frame 61 dan frame 100 mengalami penurunan kualitas gambar sebesar 21.17%, dan pada frame 120 mengalami penurunan kualitas gambar sebesar 22,71%. Nilai penurunan kualitas gambar dan warna didapatkan dengan cara membandingkan nilai biner RGB frame asli dengan biner RGB pada frame dekripsi.

5. Kesimpulan

Dari hasil pengujian di atas, dapat diambil kesimpulan berikut ini.

1. Berdasarkan hasil pengujian waktu proses enkripsi dapat disimpulkan bahwa besar total frame suatu video mempengaruhi lama atau cepatnya waktu enkripsi. Semakin besar jumlah frame suatu video, maka semakin lama pula waktu yang dibutuhkan untuk mengenkripsi video tersebut. Sama halnya dengan waktu proses dekripsi
2. Hasil pengujian Avalanche Effect berdasarkan kunci dan iv yang sama pada video yang berbeda adalah menghasilkan ciphertext yang berbeda-beda setiap videonya tetapi menghasilkan Avalanche Effect yang sama yaitu 47,71 %. Hal ini dikarenakan tidak adanya perubahan kunci dari masing-masing video. Hasil pengujian Avalanche Effect berdasarkan video dan iv yang sama adalah menghasilkan ciphertext yang berbeda-beda setiap pergantian kuncinya dan menghasilkan Avalanche Effect yang berbeda-beda yaitu berada di range 47% - 52% . Hal ini dikarenakan adanya perubahan kunci dari pada setiap percobaan yang dilakukan
3. Perbandingan frame asli dengan frame hasil dekripsi sudah menyerupai bentuk video aslinya, tetapi terjadi penurunan kualitas gambar dan warna. Pada frame 41 dan frame 54 terjadi penurunan kualitas gambar sebasar 25,51%, sedangkan untuk frame 61 dan frame 100 mengalami penurunan kualitas gambar sebesar 21.17%, dan pada frame 120 mengalami penurunan kualitas gambar sebesar 22,71%.
4. Dari hasil pengujian tersebut dapat disimpulkan bahwa algoritma kriptografi HC-128 baik dan aman untuk diimplementasikan kedalam Video on Demand dengan waktu untuk melakukan enkripsi memerlukan waktu selama 10-29 menit, sedangkan waktu yang diperlukan untuk melakukan dekripsi adalah selama 2-9 menit, dan rata-rata avalanche effect yang dihasilkan 50,59%, serta kualitas video yang dihasilkan memiliki rata-rata penurunan kualitas sebesar 23,214%

Daftar Pustaka:

[1] T. M. Thanh dan M. Iwakiri, “An Incomplete Cryptography based Digital Right Management with DCFF,” *The International of Soft Computing and Software Engineering, Vol.3, No. 3,*, 2013.

[2] G. Paul, S. Maitra dan S. Raizada, “A Combinatorial Analysis of HC-128,” *Statistic Unit, Indian Statistican Institute, Kolkata 700 108, India.*.

[3] H. Wu, “ecrypt.eu.org,” [Online]. Available: http://www.ecrypt.eu.org/stream/hcp3.html. [Diakses 3 June 2015].

[4] D. Ariyus, Pengantar Ilmu Kriptografi, Yogyakarta: C.V ANDI OFFSET, 2008.

[5] M. Asghar dan M. Ghanbari, “Cryptographic Keys Management for H.264 Scalable Coded Video Security,” *International ISC Conference on Information Security and Cryptology (ISCISC),* 2011.

[6] D. F., “Simulasi Penerapan Metoda Elliptic Curve Cryptogaphy (ECC) Untuk Mengatasi Kelemahan Sistem Keamanan Jaringan GSM,” *Journal Terra Hertz, ICT Research Center UNAS,* vol. vol. 2 No.2, Agustus 2008.

[7] H. O. P. ST, M. Dr. Ir. Sholeh Hadi P. dan S. M. Rusmi Ambarwati, “PERFORMANSI VIDEO ON DEMAND (VOD) PADA VIRTUAL PRIVATE NETWORK (VPN) MENGGUNAKAN OpenVPN”.