Perancangan dan Implementasi *Algoritma Elgamal* untuk Keamanan Data pada Video *Streaming*

Muhammad Rofiq
Dosen STMIK AsiA Malang

ABSTRAK

Dalam aplikasi video streaming tertentu dibutuhkan suatu keamanan data yang mengharuskan tidak semua pengguna dapat mengetahui isi data tersebut. Beberapa contoh aplikasi dari video streaming yang membutuhkan kerahasiaan data antara lain aplikasi video on demand, program pay per view, dan pada aplikasi video conferencing. Dalam proses enkripsi data khususnya data multimedia, ada dua hal yang harus diperhatikan. Pertama, ukuran data multimedia yang biasanya sangat besar, dan kedua, data multimedia harus diproses secara real-time.

Dalam perancangan dan implementasi metode enkripsi video streaming ini dikembangkan dengan menggunakan algoritma ElGamal. Hal ini bertujuan untuk pengembangan aplikasi algoritma dengan basis blok chipper ke dalam aplikasi yang berbasis stream. Umumnya enkripsi berbasis stream memiliki algoritma tersendiri yang berbasis stream chiper dan block chiper misalnya Video Encryption Algorithm (VEA), CR4, DES atau AES dan lain. Dalam proses perancangan dan implementasinya melalui beberapa tahap yaitu capture frame, enkripsi frame, dan proses streaming pada sisi server sedangkan pada sisi client dilakukan proses pengambilan data stream, dekripsi data, serta menampilkannya sebagai output video.

Hasil penelitian menunjukkan keakurasian data video (frame) mencapai 100%. Time delay enkripsi frame pada video standar (MPEG) sebesar 0,775 detik dan dekripsi sebesar 1,027 detik. Time delay enkripsi frame pada webcam standar (640x480) sebesar 1,797detik dan dekripsi sebesar 2,860 detik. Nilai entropy frame untuk video standar sebesar 7,680 dan webcam standar sebesar 7,595. Rata-rata bandwidth yang dibutuhkan dalam aplikasi video streaming sebesar 55,1 kbps.

***Kata kunci**: Video Streaming, ElGamal, enkripsi, dekripsi*

ABSTRACT

In particular streaming video application requires a data security requires all users can not know the contents of the data. Some examples of video streaming applications that require confidentiality of data between other video applications on demand, pay per view programs, and video conferencing applications. In the process of encryption of data, especially multimedia data, there are two things to note. First, the size of multimedia data is usually very large, and second, multimedia data must be processed in real-time.

In the design and implementation of streaming video encryption method is developed using the ElGamal algorithm. It is intended for application development on the basis of the block cipher algorithm in a stream-based applications. Generally, stream-based encryption has its own algorithm based stream ciphers and block ciphers such as Video Encryption Algorithm (VEA), CR4, DES or AES, and others. In the design and implementation through several stages, frame capture, frame encryption and streaming process on the server side, while on the client side do the data retrieval process stream, decrypt the data, and display it as a video output.

The results show the accuracy of the video data (frame) to 100%. Time delay in the video frame encryption standard (MPEG) of 0.775 seconds and 1.027 seconds for decryption. Time delay on the webcam frame encryption standard (640x480) by 1.797 seconds and 2.860 seconds for decryption. Entropy values for the standard video frame of 7.680 and 7.595 of a standard webcam. Average bandwidth required for video streaming applications for 55.1 kbps.

***Keywords:** Video Streaming, ElGamal, Encryption, Decryption*

PENDAHULUAN

Streaming adalah pengiriman data secara terus-menerus yang dilakukan secara *broadcast* melalui internet maupun intranet untuk ditampilkan pada komputer. Dalam aplikasi video *streaming* tertentu dibutuhkan suatu keamanan data yang mengharuskan tidak semua pengguna dapat mengetahui isi data tersebut. Beberapa contoh aplikasi dari *video streaming* yang membutuhkan kerahasiaan data adalah aplikasi *video on demand*, program *pay per view* serta v*ideo conferencing* yang bersifat rahasia.

Proses untuk mengamanakan dan menjadi kerahasiaan data ini dikenal dengan istilah proses enkripsi dan dekripsi. Proses enkripsi

merupakan suatu proses yang mengubah atau memodifikasi suatu data sehingga sebagian atau seluruh data sudah berbeda dengan data aslinya. Sedangkan proses dekripsi adalah suatu proses untuk mengubah atau memodifikasi data sehingga sebagian atau seluruh data yang telah berubah kembali ke data aslinya

Dalam perancangan dan implementasi metode enkripsi video streaming ini dikembangkan dengan menggunakan algoritma ElGamal. Hal ini bertujuan untuk pengembangan aplikasi algoritma dengan basis blok chipper ke dalam aplikasi yang berbasis stream. Seperti diketahui bahwa algoritma ElGamal digunakan untuk proses enkripsi citra (image). Sehingga untuk aplikasi yang berbasis streaming masih jarang penggunaannya. Umumnya enkripsi berbasis stream memiliki algoritma tersendiri yang berbasis stream chiper dan block chiper misalnya Video Encryption Algorithm (VEA), CR4, DES atau AES dan lain sebagainya. Selain itu algoritma ElGamal memiliki metode yang berbeda dengan algoritma untuk streaming. Metode algoritma ElGamal menggunakan analisis matematis dalam enkripsinya sedangkan algoritma berbasis stream menggunakan metode logika. Dari perbedaan karakteristik ini diharapkan algoritma ElGamal dapat memberikan kontribusi dalam pengembangan metode baru untuk memenuhi kebutuhan akan keamanan dan kerahasiaan data pada aplikasi berbasis stream misalnya video streaming Algoritma ElGamal dikembangkan pertama kali oleh Taher ElGamal pada tahun 1985. Algoritma ElGamal mempunyai kunci publik berupa tiga pasang bilangan dan satu bilangan sebagai kunci rahasia. Algoritma ElGamal melakukan proses enkripsi dan dekripsi pada blok-blok plainteks dan dihasilkan blok-blok cipherteks yang masing-masing terdiri dari dua pasang bilangan.

Dalam penelitian ini akan diterapkan algoritma ElGamal dalam aplikasi video streaming sebagai salah satu pengembangan metode standar yang berbasis stream.

Berdasarkan pada permasalahan tersebut diatas, maka rumusan masalah nya adalah:

1. Bagaimana tingkat keakurasian algoritma ElGamal terhadap data video;
2. Berapa *time delay* yang dibutuhkan dalam proses mengenkripsi atau mendekripsi file video;
3. Seberapa besar tingkat kekuatan penyandian algoritma ElGamal pada aplikasi video streaming.

Batasan masalah dalam penelitian ini adalah sebagai berikut:

1. Dalam penelitian ini algoritma yang digunakan adalah algoritma ElGamal.
2. Fokus penelitian ini adalah enkripsi dan dekripsi data video.
3. Format atau tipe data video yang digunakan yaitu 3G2, avi, mp4, mpeg serta input dari kamera.
4. Dalam penelitian ini tidak dibahas metode streaming video.
5. Implementasi enkripsi dan dekripsi algoritma ElGamal dibangun dengan menggunakan pemrograman berbasis object.

Tujuan dari penelitian ini adalah untuk merancang dan mengimplementasikan algoritma ElGamal untuk keamanan data dalam video streaming. Penggunaan algoritma ElGamal ini sebagai pengembangan dari metode kriptografi yang berbasis stream misalnya AES, VEA, CR4, Rijdnael.

Manfaat dari penelitian yang akan dilakukan adalah:

1. Penerapan algoritma baru yang diharapkan dapat memberikan kontribusi dalam khazanah pengembangan penelitian yang telah dilakukan sebelumnya khususnya yang berkaitan dengan penelitian dalam tesis ini.
2. Sebagai alternatif referensi pada pihak-pihak yang ingin melakukan penelitian lebih lanjut dalam kajian keilmuan yang berkaitan dengan kriptografi..

KAJIAN TEORI

Kajian teori dalam penelitian perancangan dan implementasi algoritma elgamal ini meliputi teori video *digital*, *video streaming*, algoritma ElGamal, *Entropy*.

Video *Digital*

Video *digital* pada dasarnya merupakan *array* tiga dimensi. Dua dimensi digunakan untuk menggambarkan ruang pergerakan citra (*spatial*) dan satu dimensi lainnya menggambarkan waktu. Video *digital* tersusun atas serangkaian *frame* yang ditampilkan dengan kecepatan tertentu (*frame*/detik). Jika laju *frame* cukup tinggi, maka mata manusia akan melihatnya sebagai rangkaian yang kontinyu. Setiap *frame* merupakan gambar atau citra *digital*. Suatu citra *digital* direpresentasikan dengan sebuah matriks yang masing-masing elemennya merepresentasikan nilai intensitas atau kedalaman warna. (Tekalp, 1995)

Beberapa aspek yang terkait dengan video *digital* antara lain:

Karakteristik Video *Digital*

Karakteristik yang dimiliki oleh sebuah video *digital* akan menentukan kualitas dari

video tersebut. Adapun karakteristik yang dimiliki oleh sebuah video *digital* adalah sebagai berikut :

a. **Resolusi**

Resolusi atau dimensi *frame* merupakan ukuran sebuah *frame* yang dinyatakan dalam piksel x piksel. Semakin tinggi resolusi maka akan semakin baik tampilan video tersebut, namun resolusi yang tinggi akan membutuhkan jumlah *bit* yang besar.

b. **Kedalaman *Bit***

Kedalaman *bit* akan menentukan jumlah *bit* yang digunakan untuk merepresentasikan tiap piksel di dalam sebuah *frame*. Sama halnya dengan resolusi, semakin besar kedalaman *bit* yang digunakan akan membutuhkan jumlah *bit* yang semakin besar.

c. **Laju *Frame***

Laju *frame* merupakan banyaknya *frame* yang bergerak tiap detik. Karakteristik ini berkaitan dengan kehalusan gerakan (*smoothness of motion*) sebuah objek di dalam video. (Riyanto, 2007)

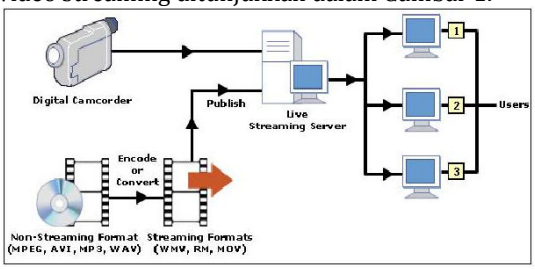
Teknik Kompresi

Terdapat dua teknik kompresi yang umum digunakan berdasarkan ada atau tidaknya penghapusan *bit*. Pertama, teknik kompresi yang mengambil X sebagai masukan dan menghasilkan Xc sebagai keluaran, dimana Xc memiliki jumlah *bit* yang lebih sedikit dibanding X. Kedua, teknik kompresi yang mengambil X sebagai masukan dan menghasilkan Y sebagai keluaran, dimana X dan Y identik. Teknik kompresi pertama disebut sebagai teknik kompresi *array* dan teknik kompresi kedua disebut sebagai teknik kompresi loseless.

Video *stream*ing

Beberapa istilah tentang *video streaming* adalah *video* yang berarti tampilan berupa gambar secara visual dan *streaming* yang berarti pengaliran atau mengalirkan. Dalam perkembangan teknologi informasi, *streaming* lebih mengarah kepada sebuah teknologi yang mampu melakukan kompresi terhadap ukuran file baik *audio* maupun *video* dengan tujuan agar mudah ditransfer melalui jaringan lokal area atau pun jaringan *internet*. Proses pengiriman file *audio* dan *video* tersebut dilakukan secara "*stream*" yang berarti proses berlangsung secara terus menerus.

Proses pengiriman file berlangsung dari sebuah *server* ke *client* melalui jaringan lokal maupun *internet*. Dimana file yang dikirimkan tersebut berupa paket time stamped atau biasa yang disebut sebagai *stream* media file. Proses video streaming ditunjukkan dalam Gambar 1.



Gambar 1: Proses video streaming
Sumber: Desk Share Website. *Understanding Video Streaming*. 24 Nov 2010

Karakteristik dari aplikasi streaming adalah sebagi berikut:

a. Distribusi data berupa audio, video, dan multimedia pada jaringan secara *real time live casting* atau *video on demand*.
b. Transfer media *digital* oleh *server* dan diterima oleh *client* sebagai *real time stream simultan*.
c. *Client* tidak perlu menunggu keseluruhan data di *download* karena *server* mengirimkan *data* yang diperlukan setiap selang waktu tertentu.
d. Terdapat komponen tambahan yang digunakan untuk melakukan *encoding* dan *decoding* terhadap aplikasi *streaming*.
e. Pada aplikasi *stream* melibatkan jaringan, dan interaksi *client* dan *server.*

Model pengiriman file multimedia *streaming* dibagi menjadi 2 yaitu:

a. *Live*, dimana pada model pengiriman file multimedia ini *server* mengcapture dan *encode* serta mengirim *stream* secara *real time*.
b. *Pre-Recorded / On Demand,* dimana pada model ini *server* melakukan *pre-encoded* dan menyimpan *content* (*file media stream*) lalu mengirim pada *client* saat ada permintaan. (Bojnord, 2005)

Kriptografi ElGamal

Algoritma ElGamal merupakan algoritma kriptografi asimetris. Pertama kali dipublikasikan oleh Taher ElGamal pada tahun 1985. Algoritma ini didasarkan atas masalah logaritma diskret pada grup $Z_p{}^*$.

Algoritma ElGamal terdiri dari tiga proses, yaitu proses pembentukan kunci, proses enkripsi dan proses dekripsi. Algoritma ini merupakan cipher blok, yaitu melakukan proses enkripsi pada blok-blok plainteks dan menghasilkan blok-blok cipherteks yang kemudian dilakukan proses dekripsi, dan hasilnya digabungkan kembali menjadi pesan yang utuh dan dapat dimengerti. Untuk membentuk system kriptografi ElGamal,

dibutuhkan bilangan prima p dan elemen primitif grup Z_p^*.

Untuk lebih jelasnya mengenai algoritma ElGamal, berikut ini diberikan suatu sistem kriptografi ElGamal, yaitu sistem kriptografi yang menggunakan algoritma ElGamal, definisi himpunan-himpunan plainteks, cipherteks dan kunci, serta proses enkripsi dan dekripsi.

Diberikan bilangan prima p dan sebuah elemen primitive $\alpha \in Z_p^*$, ditentukan

$\rho = Z_p^*, C = Z_p^* \; x \; Z_p^* \; dan \; \alpha \in \{0,1, \dots, p-2\}.$

Didefinisikan

$K = \{ (p, \alpha, a, \beta) : \beta = \alpha^a \; mod \; p \}$ …….. (2.12)

Nilai $p, \alpha, dan \; \beta$ dipublikasikan, dan nilai a dirahasiakan. Untuk $K = \{(p, \alpha, a, \beta)\}$, plainteks $m \in Z_p^*$, dan untuk suatu bilangan acak rahasia $k \in \{ 0,1,2, \dots, p-2 \}$, didefinisikan

$e_K(m,k) = (\gamma, \delta)$ ……..… (2.13)

dengan

$\gamma = a^k \; mod \; p$ ……..……..... (2.14)

dan

$\delta = \beta^k . m \; mod \; p$ ……..……..……. (2.15)

Untuk $\in Z_p^*$, didefinisikan

$d_K(\gamma, \delta) = \delta . (\gamma^a)^{-1} \; mod \; p$ ……..…… (2.16)

Pembentukan Kunci

Proses pertama adalah pembentukan kunci yang terdiri dari kunci rahasia dan kunci publik. Pada proses ini dibutuhkan sebuah bilangan prima p yang digunakan untuk membentuk grup Z_p^* , elemen primitif □ dan sebarang $a \in \{0,1,..., p-2\}$.

Kunci publik algoritma ElGamal berupa pasangan 3 bilangan, yaitu (p,α ,β) , dengan

$\beta = \alpha^a \; mod \; p$ …….. (2.17)

Sedangkan kunci rahasianya adalah bilangan a tersebut

Agar mempermudah dalam menentukan elemen primitif, digunakan bilangan prima p sedemikian hingga $p=2.q+1$, dengan q adalah bilangan prima. Bilangan prima p seperti ini disebut dengan bilangan *prima aman*. Untuk menentukan apakah suatu bilangan itu prima atau komposit, dapat digunakan tes keprimaan seperti tes keprimaan biasa dan tes Miller-Rabbin. Karena digunakan bilangan bulat yang besar maka perhitungan pemangkatan modulo dilakukan penggunakan metode *fast exponentiation*.

Karena pada algoritma ElGamal menggunakan bilangan bulat dalam proses perhitungannya, maka pesan harus dikonversi ke dalam suatu bilangan bulat. Untuk mengubah pesan menjadi bilangan bulat, digunakan kode ASCII (*American Standard for Information Interchange*). Kode ASCII merupakan representasi numerik dari karakter-karakter yang digunakan pada komputer, serta mempunyai nilai minimal 0 dan maksimal 255. Oleh karena itu, berdasarkan sistem kriptografi ElGamal di atas maka harus digunakan bilangan prima yang lebih besar dari 255. Kode ASCII berkorespondensi 1-1 dengan karakter pesan. (Ramsky, 2009)

Enkripsi

Pada proses ini pesan dienkripsi menggunakan kunci publik (p,α ,β) dan sebarang bilangan acak rahasia $k \in \{0,1,..., \pi - 2\}$ Misalkan m adalah pesan yang akan dikirim. Selanjutnya, m diubah ke dalam blok-blok karakter dan setiap karakter dikonversikan ke dalam kode ASCII, sehingga diperoleh plainteks m_1, m_2, … , m_n dengan $m_i \in \{ 1,2, \dots, p-1\} \; dan \; i = 1, 2, \dots, n$. Untuk nilai ASCII bilangan 0 digunakan untuk menandai akhir dari suatu teks.

Proses enkripsi pada algoritma ElGamal dilakukan dengan menghitung

$\gamma = a^k \; mod \; p$ ……..…… (2.18)

dan

$\delta = \beta^k . m \; mod \; p$ ……. (2.19)

dengan $k \in \{0,1,..., p-2\}$acak. Diperoleh cipherteks (γ ,δ) .

Bilangan acak k ditentukan oleh pihak pengirim dan harus dirahasiakan, jadi hanya pengirim saja yang mengetahuinya, tetapi nilai k hanya digunakan saat melakukan enkripsi saja dan tidak perlu disimpan. (Pratama, 2009)

Dekripsi

Setelah menerima cipherteks (γ ,δ) , proses selanjutnya adalah mendekripsi cipherteks menggunakan kunci publik p dan kunci rahasia a. Dapat ditunjukkan bahwa plainteks m dapat diperoleh dari cipherteks menggunakan kunci rahasia a.

Diberikan (p,α ,β) sebagai kunci publik dan a sebagai kunci rahasia pada algoritma ElGamal. Jika diberikan cipherteks (γ ,δ) , maka

$m = \delta . (\gamma^a)^{-1} \; mod \; p$ ……. (2.20)

dengan m adalah plainteks. (Menezes, Oorschot and Vanstone, 1996)

Entropy

Dalam kriptografi yang efisien, sebuah kunci harus dapat digunakan untuk mengamankan data. Kerahasiaan yang memang sempurna tidak dapat tercapai. Namun yang terbaik yang dapat dilakukan adalah membangun kriptografi yang aman secara komputasi. Pada kerahasiaan yang tidak sempurna terdapat kemungkinan beberapa ciphertext memperlihatkan informasi kunci. Sehingga Shannon memperkenalkan sebuah konsep yang disebut dengan *entropy* untuk menghitung ketidakpastian dari sebuah hasil percobaan.

Entropi $H(x)$ dari x merupakan suatu nilai yang bergantung pada probabilitas $p_1 \dots p_n$ dari hasil x yang mungkin terjadi.

$$H(p_1 \dots p_n) = -\sum_{i=1}^{n} p_i \log_2 p_i \dots\dots\dots\dots\dots\dots (2.21)$$

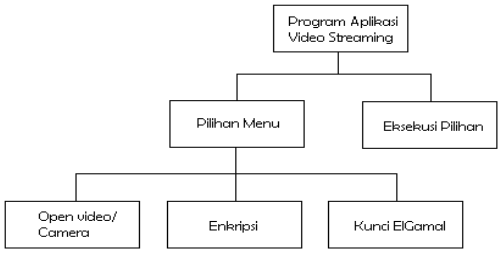
Dengan $H(p_1 \dots p_n)$ merupakan entropi, p_i merupakan probabilitas kemunculan simbol ke (Rinartha, 2010)

PEMBAHASAN

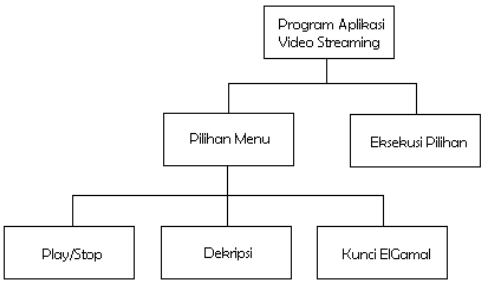
Perancangan

Arsitektur Sistem

Arsitektur sistem merupakan kerangka sistem secara umum yang menampilkan sistem ke dalam sebuah diagram yang nantinya akan digunakan sebagai acuan dalam pembuatan perangkat lunak aplikasi. Arsitektur sistem secara keseluruhan didapat dari arsitektur tiap-tiap komponen di dalam sistem. Data flow diagram yang terdapat dalam program aplikasi ini mempunyai karakteristik tipe *transform flow*. Dalam *transform flow* terdapat tiga komponen, yaitu *incoming flow* (aliran/jalur informasi eksternal yang akan ditransformasikan), *transform center* (pusat transformasi), *outgoing flow* (aliran/jalur informasi internal keluar dari sistem). Perancangan arsitektur program aplikasi video streaming ini terdiri atas arsitektur pada server dan arsitektur pada client. Arsitektur program aplikasi video streaming pada server ditunjukkan dalam Gambar 2: sedangkan pada client ditunjukkan dalam Gambar 3.



Gambar 2: Arsitektur program aplikasi video streaming pada server



Gambar 3: Arsitektur program aplikasi video streaming pada client

Analisis desain model matematis algoritma ElGamal

Analisis desain model matematis algoritma ElGamal memberikan gambaran tentang penerapan algoritma ElGamal dalam proses kriptografi pada video streaming. Pada video streaming ElGamal dikenal tiga proses yaitu; pembuatan kunci publik, enkripsi dan dekripsi. Keseluruhan proses enkripsi dan dekripsi tersebut akan menggunakan bilangan sebagai kunci public maupun kunci private. Proses-proses penerapan algoritma ElGamal ditunjukkan dalam Tabel 1.

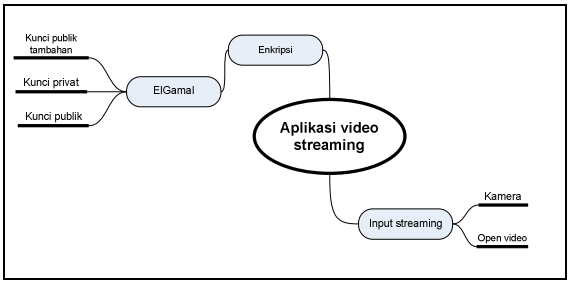
Tabel 1: Proses-proses yang terjadi dalam video streaming ElGamal

Penerima	Pengirim
Pembuatan kunci publik	
Sebelum pihak pengirim mengirimkan pesan, pihak penerima harus membuat kunci publik yang akan digunakan untuk melakukan enkripsi pesan. Pihak penerima memilih kunci pribadi (a), kunci publik tambahan (α) yang akan digunakan untuk membuat kunci publik, kemudian pihak penerima membuat kunci publik (β) dengan bentuk matematis $\beta = \alpha^a \ mod \ p$ kemudian pihak penerima mempublikasikan kunci publik (β) dan kunci publik tambahan (α).	
Enkripsi	
	Pengirim memilih pesan (m) yang akan dikirimkan yang kemudian diolah dengan menggunakan kunci publik (β, a) pengirim dan bilangan acak (k) dengan bentuk matematis $\gamma = a^k \ mod \ p$ $\delta = \beta^k . m \ mod \ p$ kemudian hasil enkripsi γ dan δ dikirimkan kepada pihak penerima.
Dekripsi	
Pihak penerima akan menerima hasil enkripsi γ dan δ dan akan mengolah hasil enkripsi tersebut sehingga pesan dapat terbaca sesuai dengan pesan aslinya, dengan bentuk matematis $m = \delta . (\gamma^a)^{-1} \ mod \ p$	

WBS (*Work Breakdown Structure*)

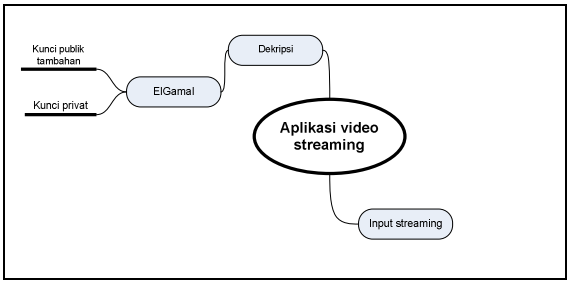
Analisis WBS pada program aplikasi akan menguraikan fungsi-fungsi komponen penyusun

sistem menjadi modular. Struktur komponen fungsional penyusun sistem pada server ditunjukkan dalam Gambar 3.3.



Gambar 4: Struktur komponen fungsional penyusun sistem pada server

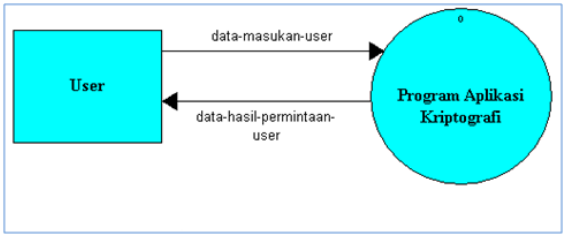
Analisis WBS pada program aplikasi pada client menguraikan fungsi-fungsi komponen penyusun sistem menjadi modular. Struktur komponen fungsional penyusun sistem pada client ditunjukkan dalam Gambar 3.4.



Gambar 5: Struktur komponen fungsional penyusun sistem pada client

Diagram Konteks

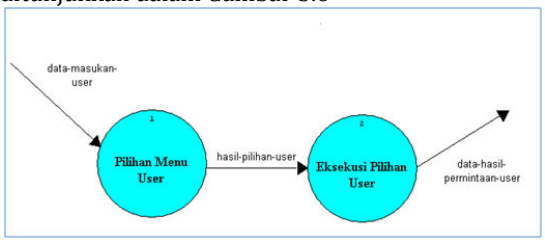
Diagram konteks ditunjukkan dalam Gambar 6.



Gambar 6: Diagram konteks program aplikasi video streaming

Data Flow Diagram

Pada data flow diagram ini dijelaskan tentang proses-proses utama yang dimiliki oleh program aplikasi untuk melakukan fungsinya. Data flow diagram program aplikasi video streaming ditunjukkan dalam Gambar 3.6



Gambar 7: Data flow diagram program aplikasi video streaming

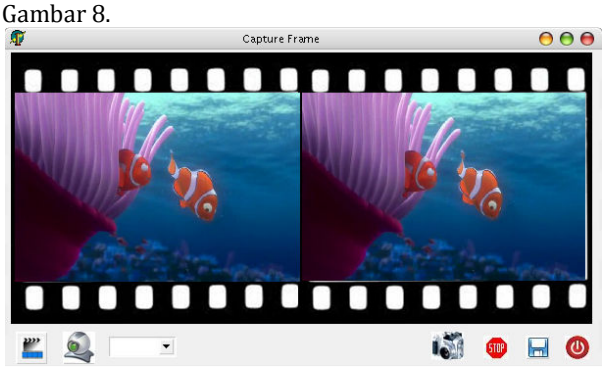
Pengujian

Untuk pengujian perangkat lunak pada sisi server meliputi proses capture frame, pengujian enkripsi dengan algoritma ElGamal, proses streaming. Sedangkan pengujian perangkat lunak pada sisi client meliputi proses pengambilan frame streaming, dan proses dekripsi untuk ditampilkan sebagai output video.

Setelah pengujian tiap tahapan selesai, maka dilakukan pengujian sesuai dengan rumusan masalah yang telah ditetapkan. Pengujian ini meliputi tingkat keakurasian proses enkripsi dekripsi algoritma ElGamal terhadap data video, pengujian time delay yang dibutuhkan dalam proses enkripsi dan dekripsi, dan pengujian nilai entropy algoritma ElGamal dalam penerapannya pada video streaming.

Pengujian *capture frame*

Pada pengujian capture ini bertujuan untuk memperoleh frame dari data input yang diperoleh dari dari file video maupun dari kamera. Proses capture frame ditunjukkan dalam Gambar 8.



Gambar 8: Proses capture frame video

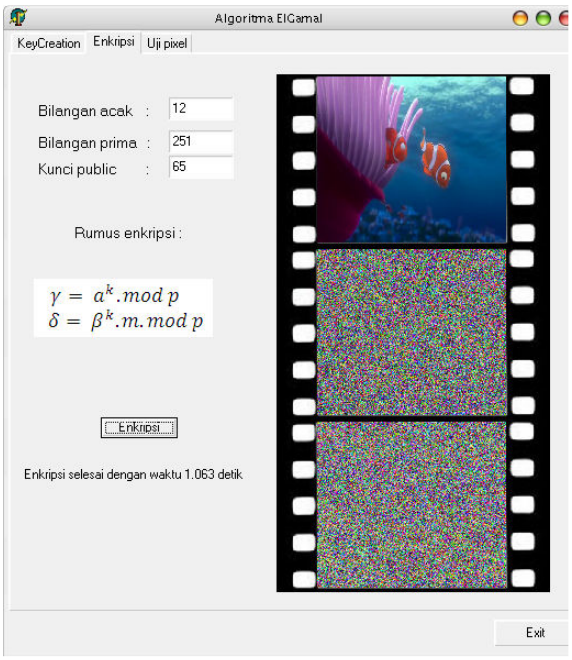
Pengujian enkripsi algoritma ElGamal

Data yang akan dienkripsi adalah frame yang telah dicapture dari tahapan capture file. Dalam proses enkripsi ini, langkah awal adalah pembentukan kunci publik yang diperoleh dari 3 pasang bilangan yaitu parameter kunci publik tambahan (acak), bilangan prima, dan kunci

private. Setelah itu dilakukan proses enkripsi. Untuk pembentukan kunci publik ditunjukkan dalam Gambar 9.

Gambar 9: Proses pembentukan kunci public

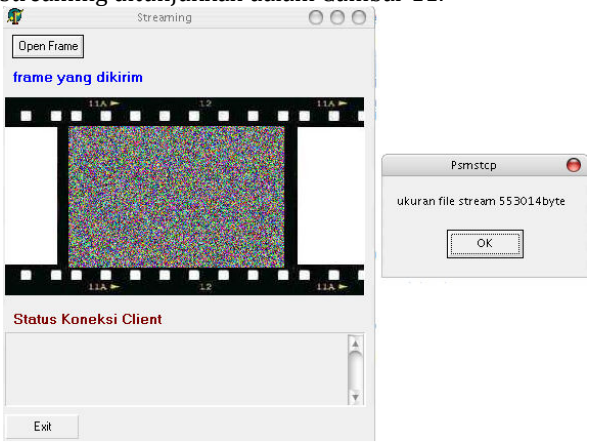
Pengujian proses enkripsi ditunjukkan dalam Gambar 10.



Gambar 10: Proses enkripsi

Pengujian proses streaming

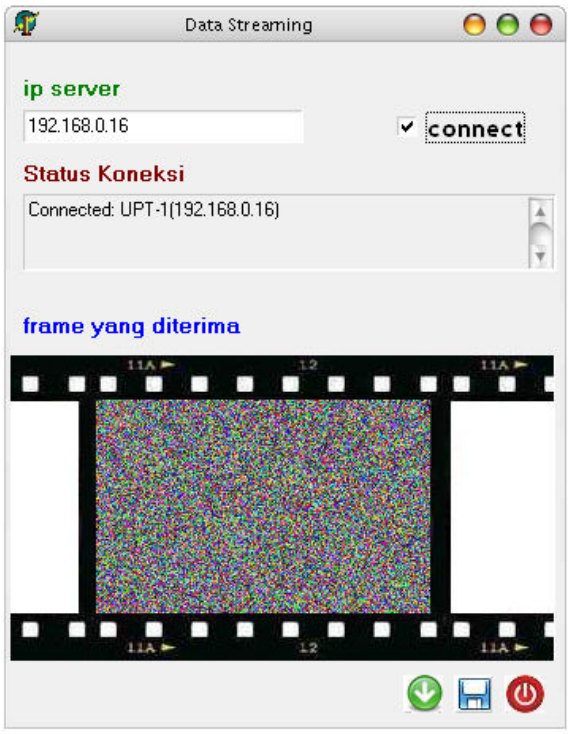
Dalam proses streaming data stream yang dikirimkan adalah chiperteks dari hasil enkripsi. Dalam proses streaming ini dapat diketahui pula nilai data stream yang akan dikirimkan. Proses streaming ditunjukkan dalam Gambar 11.



Gambar 11: Proses streaming dengan ukuran file stream yang dikirim

Pengujian pengambilan data streaming

Pada pengujian data streaming dilakukan pada sisi client. Setelah koneksi terhubung maka dilakukan proses pengambilan data streaming ini. Untuk proses pengambilan data stream ditunjukkan dalam Gambar 4.5.

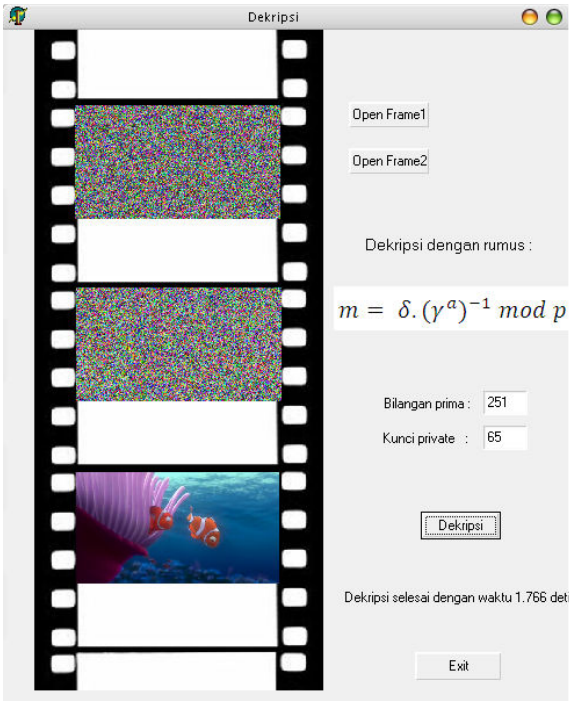


Gambar 12: Proses pengambilan data streaming

Pengujian dekripsi

Proses dekripsi merupakan proses untuk mengembalikan data stream (frame) yang sudah dimanipulasi tersebut ke dalam data (frame) aslinya. Setelah data aslinya diketahui kemudian ditampilkan ke video. Dalam proses dekripsi ini

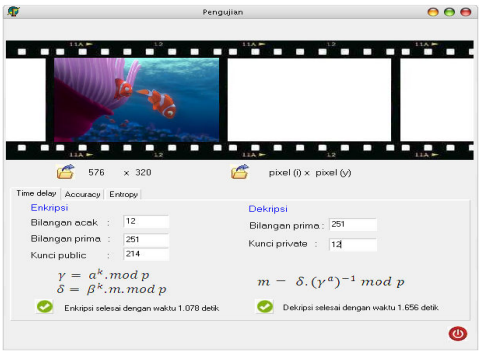
parameter yang digunakan adalah bilangan prima dan kunci private. Pengujian proses dekripsi ditunjukkan dalam Gambar 13.



Gambar 13: Proses dekripsi.

Pengujian time delay enkripsi dekripsi

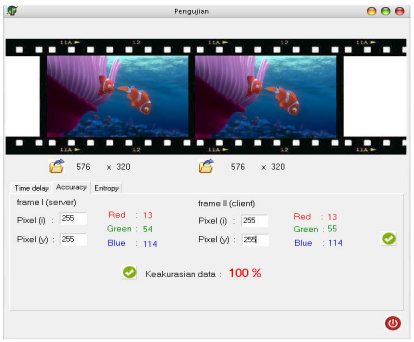
Tujuan dari pengujian time delay ini adalah untuk mengetahui waktu yang dibutuhkan dalam proses enkripsi maupun dekripsi. Pengujian time delay ini ditunjukkan dalam Gambar 14.



Gambar 14: Time delay proses enkripsi dan dekripsi

Pengujian keakurasian data

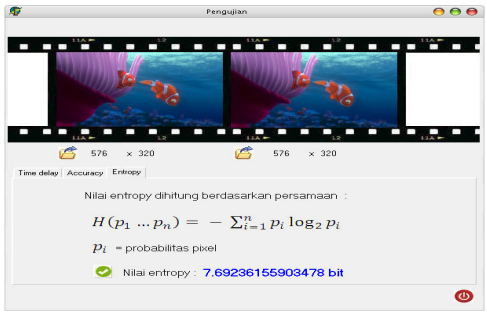
Pada pengujian keakurasian data ini, dibandingkan nilai RGB dari piksel dari frame sebelum data dienkripsi dan dikirim dengan nilai RGB frame yang telah didekripsikan. Pengujian nilai frame ini ditunjukkan dalam Gambar 15.



Gambar 15: Pengujian keakurasian data

Entropy coding

Entropy coding ini juga berguna untuk memperkirakan jumlah bit rata-rata untuk mengkodekan elemen dari pesan. Nilai *entropy coding* ditunjukkan dalam Gambar 16.



Gambar 16: *Entropy coding*

Untuk data hasil pengujian *time delay*, akurasi data dan nilai entropy video standar (MPEG) dan webcam ditunjukkan dalam Tabel 2.

Tabel 2: Data hasil pengujian *time delay*, akurasi data dan nilai entropy video standar (MPEG) dan webcam

Nama file	Reso-lusi *frame*	*Time delay*		Aku-rasi (%)	Entropy (bit)	*Band width* kbps
		Enkripsi	dekripsi			
sfs	480x 272	0,76	1,23	100	7,58	54,7
rosi	450x 360	0,96	1,50	100	7,68	55,6
boy	640x 272	1,03	1,45	100	7,57	68,7
bio	640x 352	1,15	1,53	100	7,68	54,7
car	576x 238	1,00	1,32	100	7,83	46,8
iron	720x 288	1,26	1,57	100	7,65	55,6
nemo	576x 320	0,97	1,29	100	7,74	49,8
webcam	640x 480	1.79	2.86	100	7.59	55,1
Rata-rata		0,77	1,02	100	7,68	55,1

Dari data hasil pengujian pada Tabel 2 dapat diperoleh beberapa analisis sebagai berikut:

1. Rata-rata *time delay* enkripsi untuk format video standar (MPEG) sebesar 0,77 detik dan dekripsi sebesar 1,02 detik.
2. *Time delay* enkripsi *frame* pada webcam standar (640x480) sebesar 1,79 detik dan dekripsi sebesar 2,86 detik.
3. *Time delay* proses enkripsi lebih cepat daripada *time delay* yang dibutuhkan dalam proses dekripsi.
4. Besarnya *time delay* yang dibutuhkan berbanding lurus dengan ukuran *frame* dari video. Semakin besar ukuran *frame* maka semakin besar pula *time delay* yang dibutuhkan.
5. Tingkat keakurasian data antara *frame* asli dengan *frame* setelah didekripsi memiliki tingkat akurasi sebesar 100%.
6. Nilai entropy menunjukkan jumlah rata-rata bit dalam piksel yang terdapat dalam *frame* untuk tiap video. Nilai entropy untuk tiap-tiap video memiliki perbedaan karena hal ini bergantung dari tingkat warna dari piksel pada saat *frame* tersebut ditampilkan.
7. Rata-rata nilai entropy *frame* untuk video standar sebesar 7,68 dan webcam standar sebesar 7,59.
8. Entropy dengan nilai 7,595 menunjukkan bahwa informasi nilai skala warna yang digunakan dalam frame mendekati 8 bit (bit warna dari 0 – 255)
9. Nilai entropy tidak sama dengan keakurasian data. Keakurasian data untuk mengetahui tingkat keakurasian data asli dengan data yang telah diproses sedangkan entropy menunjukkan informasi warna yang digunakan dalam frame video.
10. Rata-rata *bandwidth* yang dibutuhkan untuk satu pengguna sebesar 55,1 kbps.

PENUTUP

Penelitian ini mengembangkan sebuah rancangan algoritma kriptografi baru dalam aplikasi yang berbasis *stream* yang diperoleh dari algoritma yang berbasis *block chipper.* Dari perancangan, implementasi dan pengujian perangkat lunak didapatkan kesimpulan sebagai berikut :

1. Tahapan perancangan penerapan algoritma ElGamal dalam aplikasi video streaming meliputi spesifikasi aplikasi program, analisis dan desain model matematis algoritma ElGamal, analisis dan desain aplikasi agoritma ElGamal, desain aliran data, implementasi program, dan analisis pengujian.
2. Dalam implementasi penerapan algoritma ElGamal digunakan dua program yaitu program aplikasi pada server dan client.
3. Penerapan algoritma ElGamal dalam kriptografi *frame* video memiliki tingkat keakurasian data video sebesar 100%.
4. *Time delay* enkripsi *frame* pada video standar (MPEG) sebesar 0,775 detik dan dekripsi sebesar 1,027 detik.
5. *Time delay* enkripsi *frame* pada webcam standar (640x480) sebesar 1,797detik dan dekripsi sebesar 2,860 detik.
6. Nilai entropy *frame* untuk video standar sebesar 7,680 dan webcam standar sebesar 7,595.
7. Rata-rata *bandwidth* yang dibutuhkan dalam aplikasi video streaming sebesar 55,1 kbps

Dari hasil yang didapatkan dalam penggunaan algoritma ElGamal, menunjukkan adanya peningkatan keamanan dalam hal penggunaan kunci publik dan kunci *private* dalam kriptografi. Akan tetapi penelitian ini masih memerlukan adanya penyempurnaan dan pengembangan, antara lain :

1. Dengan *delay* yang cukup besar dalam proses enkripsi dan dekripsinya sehingga diperlukan suatu metode streaming tertentu untuk memecahkan masalah *delay* sehingga tidak berpengaruh terhadap proses video streaming.
2. Kriptografi algoritma ElGamal, masih memiliki kekurangan pada lamanya waktu proses yang diperlukan serta terjadinya *message expansion* pada *cipherimage, s*ehingga diperlukan metode lain yang dapat digunakan untuk mengurangi waktu proses maupun *message expansion* pada *cipher-image.*

DAFTAR PUSTAKA

1. M, Bojnord. Hashemi, R dan Fatemi, S, O. (2005). *Implementing an Efficient Encryption Block for MPEG Video Streams*. *47th Intenational Symposium ELMAR-2005, 08-10 Juni 2005, Zadar, Croatia.*
2. Menezes, A. J. Oorschot, P.C.v. Vanstone, S. A. (1997). *Handbook of Applied Cryptography*, CRC Press ISBN 0-8493-8523-7.
3. Pratama, A. (2009). *Enkripsi Selektif Video MPEG dengan Algoritma Serpent*. Jurnal Bandung
4. Ramsky, T. (2009). *Perangkat Lunak Enkripsi Video MPEG-1 dengan Modifikasi Video Encryption Algorithm (VEA).* Jurnal Bandung.

5. Rinartha, K. (2010). *Pengamanan Citra Digital Dengan Menggunakan Pengembangan Kriptografi Kunci Public Elgamal*. Prosiding Seminar Nasional Teknologi Informasi dan Aplikasinya Volume 2, Malang : Politeknik Negeri Malang
6. Riyanto, M. Z. (2007). *Pengamanan Pesan Rahasia Menggunakan Algoritma ElGamal atas Group Pergandaan Zp*. Yogyakarta
7. Tekalp, A. Murat. 1995. *Digital Video Processing*, New Jersey: Prentice Hall.