



**"PEMBUATAN APLIKASI KRIPTOGRAFI VIDEO (MP4)
MENGUNAKAN ALGORITMA RC4"**

Disusun dan Diajukan Untuk Memenuhi Persyaratan Ujian Akhir Memperoleh

Gelar Sarjana Komputer Pada Fakultas Sains Dan Teknologi

Universitas Pembangunan Panca Budi

Medan

SKRIPSI

OLEH

NAMA : VERAWATY BR SIMAMORA

NPM : 1514370269

PROGRAM STUDI : SISTEM KOMPUTER

**FAKULTAS SAINS DAN TEKNOLOGI
UNIVERSITAS PEMBANGUNAN PANCA BUDI**

MEDAN

2019

ABSTRAK

VERAWATY BR SIMAMORA

PEMBUATAN APLIKASI KRIPTOGRAFI VIDEO (*MP4*) MENGGUNAKAN ALGORITMA *RC4*.

Perkembangan teknologi merupakan satu kemajuan yang sudah melekat ke kehidupan manusia. Dengan berkembangnya teknologi, banyaknya orang yang menyalahgunakan data seperti video salah satu contohnya dengan memanfaatkan teknologi tanpa bertanggungjawab. Algoritma *RC4* adalah algoritma kriptografi yang mengamankan sebuah data dengan cara membangkitkan aliran kunci (*keystream*) yang kemudian di-*XOR*-kan dengan *plainteks* pada waktu *enkripsi* (atau di-*XOR*-kan dengan bit-bit *cipherteks* pada waktu dekripsi). Algoritma *RC4* ini juga memakai kunci simetris dimana kunci *enkripsi* dan kunci *dekripsi* adalah kunci yang sama, sehingga pada saat proses *enkripsi* dan *dekripsinya* mudah. Pada pembuatan aplikasi kriptografi video ini menggunakan format *MP4*, dikarenakan format *MP4* lebih memiliki kualitas yang bagus dari segi gambar maupun audionya. Dengan adanya aplikasi kriptografi algoritma *RC4* ini video berformat (*MP4*) dapat diamankan dari orang yang tidak bertanggungjawab.

Kata Kunci : Aplikasi, Video, Kriptografi, *Algoritma RC4*.

DAFTAR ISI

	Halaman
COVER	
LEMBAR PENGESAHAN	
ABSTRAK	
KATA PENGANTAR	i
DAFTAR ISI	iii
DAFTAR GAMBAR	v
DAFTAR TABEL	ix
BAB I PENDAHULUAN	1
1.1 Latar Belakang	1
1.2 Perumusan Masalah	3
1.3 Batasan Masalah	3
1.4 Tujuan Penelitian.....	3
1.5 Manfaat Penelitian.....	4
BAB II LANDASAN TEORI	5
2.1 Pengertian Aplikasi.....	5
2.2 Kriptografi	5
2.3 Video.....	7
2.4 Multimedia	8
2.5 <i>MP4</i>	9
2.6 Algoritma Kriptografi	10

2.7	Algoritma <i>RC4</i>	11
2.8	Algoritma <i>Simetris</i>	13
2.9	Bahasa Pemrograman	14
2.10	<i>Visual Basic</i>	16
2.11	<i>Microsoft Visual Studio</i>	18
2.12	<i>UML (Unified Modeling Language)</i>	19
2.13	<i>Use Case Diagram</i>	20
2.14	<i>Activity Diagram</i>	23
BAB III	METODE PENELITIAN	26
3.1	Tahapan Penelitian	26
3.2	Metode Pengumpulan Data	27
3.3	Analisis Permasalahan yang Berjalan.....	27
3.4	Analisa Kelemahan yang Berjalan	28
3.5	Solusi Pemecahan Masalah	29
3.6	Analisa Kebutuhan Sistem.....	30
	1. <i>Hardware</i>	30
	2. <i>Software</i>	31
3.7	Analisa Proses Sistem Yang Berjalan	31
3.8	Perancangan Berorientasi Objek	37
	1. <i>Use Case Diagram</i>	38
	2. <i>Activity Diagram</i>	39
	3. <i>Squence Diagram</i>	40

3.9	Perancangan Antar Muka	41
1.	Rancangan Halaman <i>Enkripsi</i>	41
2.	Rancangan Halaman <i>deskripsi</i>	41
3.	Rancangan Halaman Pengaturan	42
BAB IV	IMPLEMENTASI DAN PENGUJIAN SISTEM	44
4.1	Pengujian Sistem	44
4.1	Spesifikasi Sistem	44
1.	<i>Hardware</i>	45
2.	<i>Software</i>	45
4.3.	Tampilan Awal/Home	46
1.	Tampilan halaman program.....	46
2.	Tampilan halaman <i>enkripsi</i> video	46
3.	Tampilan halaman <i>deskripsi</i> video	47
4.	Tampilan halaman proses <i>enkripsi</i>	48
3.	Tampilan halaman proses <i>dsenkripsi</i>	48
4.4.	Kelebihan dan Kekurangan Sistem	49
BAB V	PENUTUP	50
1.	Kesimpulan	50
2.	Saran	50

DAFTAR PUSTAKA

LAMPIRAN

DAFTAR GAMBAR

No	Judul	Hal
<hr/>		
2.1	Proses Algoritma Simetris	15
3.1	Tahapan Penelitian	26
3.2	Analisis permasalahan yang berjalan.....	28
3.3	<i>Use Case Diagram</i>	38
3.4	<i>Activity Diagram</i>	39
3.5	<i>Squence Diagram</i>	40
3.6	Rancangan Halaman enkripsi	41
3.7	Rancangan Halaman deskripsi.....	42
3.8	Rancangan Halaman pengaturan.....	43
4.1	Tampilan aturan pengaturan aplikasi.....	46
4.2	Tampilan Halaman enkripsi video	47
4.3	Tampilan halaman deskripsi video.....	47
4.4	Tampilan Halaman Proses enkripsi.....	48
4.5	Tampilan Halaman Proses deskripsi.....	49
4.6	Tampilan Halaman Proses Enkripsi.....	50
4.7	Tampilan Halaman Proses Deskripsi.....	51

DAFTAR TABEL

No	Judul	Hal
2.1	Simbol <i>Use Case Diagram</i>	38
2.2	Simbol <i>Activity Diagram</i>	39
2.3	Simbol <i>Simbol Sequence Diagram</i>	40
2.5	Simbol <i>Activity Diagram</i>	22
3.1	<i>Tabel Perancangan</i>	29

KATA PENGANTAR

Puji Syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat-Nya kepada peneliti, sehingga Skripsi ini dapat diselesaikan oleh peneliti tepat pada waktunya dengan judul **Pembuatan Aplikasi Kriptografi Video (MP4) Menggunakan Algoritma RC4**.

Skripsi ini dilakukan guna memenuhi salah satu syarat pemenuhan kurikulum dalam menyelesaikan pendidikan pada Program Studi S1 Sistem Komputer Fakultas Teknik Universitas Pembangunan Panca Budi Medan. Pada kesempatan ini, penulis menyampaikan rasa terima kasih dan penghargaan yang sebesar-besarnya kepada :

1. Bapak Dr. H. Muhammad Isa Indrawan, SE, MM, selaku Rektor Universitas Pembangunan Panca Budi Medan.
2. Ibu Sri Shindi Indira, S.T., M.S.C, selaku Dekan Fakultas Sains dan Teknologi Universitas Pembangunan Panca Budi Medan.
3. Bapak Andisyah Putera Siahaan S.Kom, M.Kom, Selaku Pembimbing 1 yang juga telah memberikan pengarahan dan petunjuk Skripsi Ini.
4. Bapak Supiyandi S.Kom, M.Kom, selaku Dosen Pembimbing II yang juga telah memberikan pengarahan dan petunjuk dalam Skripsi ini.
5. Bapak/Ibu Dosen beserta seluruh staf Universitas Pembangunan Panca Budi Medan.

6. Teristimewa kepada Kedua Orang Tua dan Keluarga saya, yang telah banyak memberikan bimbingan dan bantuan baik moril maupun material selama penulis mengikuti pendidikan hingga selesainya Skripsi ini.
7. Kepada seluruh rekan-rekan di program Studi Teknik Komputer Universitas Pembangunan Panca Budi Medan yang telah memberikan dukungan moril kepada penulis.

Penulis menyadari bahwa Skripsi ini masih kurang sempurna. Oleh karena itu, penulis sangat mengharapkan dan menghargai saran maupun kritikan dari pembaca dan semua pihak yang mengarah kepada perbaikan Tuga Akhir ini.

Medan, April 2019
Penulis,

VERAWATY BR SIMAMORA
1514370269

BAB I

PENDAHULUAN

1.1 Latar Belakang

Saat ini data dan informasi menjadi hal yang penting. Berbagai sebuah perusahaan, organisasi, instansi, dan lainnya telah memanfaatkan teknologi yang menggabungkan berbagai dari sumber media (teks, grafik, dan suara) untuk menyampaikan sesuatu dalam bentuk komunikasi. Pada saat ini multimedia sering kali digunakan dalam bentuk dunia seperti penggunaan video digital yang cukup populer di kalangan sosial media. Keamanan terhadap video yang di *upload* pada sosial media menjadi hal yang sangat dibutuhkan. Namun keamanan pada video dengan pembatasan hak akses sudah tidak lagi dapat menjamin keamanan video karena kebocoran data dapat disebabkan oleh pihak-pihak yang langsung berhubungan dengan video itu sendiri.

MP4 merupakan salah satu bentuk format berkas pengodean suara, gambar, dan video digital. *MP4* format video ini memiliki kualitas gambar yang jauh lebih bagus dan berukuran file yang lebih kecil. Multimedia yang sering di kenal dengan sebutan *MPEG-4*, pada umumnya format *MP4* ini digunakan untuk merekam video serta audio, tetapi kemampuan lain dari format *MP4* ini dapat menangani data lain seperti subtitle. Adapun kelebihan yang bias dilakukan dari format *MP4* yaitu streaming melalui internet.

Menurut Galuh Adjeng Sekarsari (2015:251) Kriptografi merupakan salah satu bagian dari ilmu matematika yang disebut *Cryptology* yang bertujuan untuk menjaga kerahasiaan informasi yang terdapat pada data maupun citra sehingga informasi tidak dapat diketahui oleh pihak yang tidak berwenang. Dalam kriptografi, terdapat 2 proses utama, *enkripsi* dan *dekripsi*. *Enkripsi* adalah proses penyandian pesan asli atau *plainteks* menjadi *cipherteks* (teks tersandi). Sedangkan *dekripsi* adalah proses penyandian kembali *cipherteks* menjadi *plainteks*.

Pada penelitian yang dilakukan oleh penulis (2018) yang berjudul “Pembuatan Aplikasi Kriptografi Video (MP4) Menggunakan Algoritma RC4” dijelaskan bahwa hasil penelitian tersebut menunjukkan bahwa video dapat terenkripsi dengan menggunakan algoritma RC4 yang bersifat *stream cipher* yakni didekripsikan secara *byte per byte* dan proses *enkripsi* dan *dekripsi* jauh lebih cepat karena menggunakan kunci yang sama serta memiliki tingkat keamanan yang tinggi sesuai panjang kunci.

Berdasarkan pada informasi yang dipaparkan, peneliti membuat sebuah penerapan *enkripsi* dan *dekripsi* dengan menggunakan metode RC4 dengan mengenkripsi dan mendekripsi isi video. Kemudian cara kerja dari proses *enkripsi* dan *dekripsi* akan dibuat menjadi lebih mudah dari penelitian sebelumnya yaitu dengan mengenkripsi dan mendekripsi isi video secara keseluruhan sehingga tidak perlu harus memilih video yang akan dienkripsi dan dekripsi. Implementasi ini menerapkan metode sistem enkripsi dan dekripsi dengan metode RC4 simetris dalam pengamanan data mahasiswa Jurusan Ilmu Komputer dengan judul

“Pembuatan Aplikasi Kriptografi Video (MP4) Menggunakan Algoritma RC4”.

1.2 Rumusan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka rumusan masalah dalam penelitian ini adalah :

- a. Bagaimana mengamankan video menggunakan kriptografi?
- b. Bagaimana pembuatan aplikasi kriptografi ini akan sama efektifnya dengan aplikasi lain?
- c. Bagaimana mengamankan video yang relevan menggunakan kriptografi?

1.3 Batasan Masalah

Berdasarkan latar belakang masalah yang telah diuraikan di atas, maka batasan masalah dalam penulisan ini adalah :

- a. *Enkripsi* dan *dekripsi* sebuah video menggunakan metode algoritma *RC4* yang bersifat *stream cipher* dan memiliki kunci *simetris*.
- b. Pembuatan aplikasi kriptografi ini dibuat hanya menggunakan algoritma *RC4* dalam mengamankan video berformat *MP4*.
- c. Pembuatan aplikasi kriptografi yang digunakan hanya berkapasitas maksimal *1024 Kb* dan menggunakan bahasa pemrograman *Visual Basic.Net*.

1.4 Tujuan Penelitian

Tujuan dari penulisan ini adalah :

- a. Mengamankan video dari orang yang tidak bertanggung jawab menggunakan kriptografi.
- b. Membuat aplikasi kriptografi yang efisien dan relevan.
- c. Membuat aplikasi kriptografi video berbasis *MP4* menggunakan algoritma *RC4*.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini di antaranya yaitu :

- a. Mengamankan video dari orang yang tidak bertanggung jawab.
- b. Dengan adanya aplikasi kriptografi ini dapat menjamin kerahasiaan isi video.
- c. Menambah pengetahuan tentang algoritma *RC4*.

BAB II

LANDASAN TEORI

2.1 Pengertian Aplikasi

Menurut Widianti (2015), aplikasi adalah suatu program yang siap untuk digunakan yang dibuat untuk melaksanakan suatu fungsi bagi pengguna jasa aplikasi serta penggunaan aplikasi lain yang dapat digunakan oleh suatu sasaran yang akan dituju. Secara istilah, aplikasi komputer adalah suatu subkelas perangkat lunak komputer yang menggunakan kemampuan komputer langsung untuk melakukan suatu tugas yang diinginkan pemakai. Contoh utama perangkat lunak aplikasi adalah program pengolah kata, lembar kerja, dan pemutar media.

Pengertian aplikasi secara umum merupakan alat terapan yang dapat difungsikan secara khusus dan terpadu sesuai dengan kemampuan yang dimiliki aplikasi dengan adanya suatu perangkat komputer yang siap pakai bagi *user*.

2.2 Kriptografi

Menurut Galuh Adjeng Sekarsar, et al (2015), Kriptografi merupakan salah satu bagian dari ilmu matematika yang disebut *Cryptology* yang bertujuan untuk menjaga kerahasiaan informasi yang terdapat pada data maupun citra sehingga informasi tidak dapat diketahui oleh pihak yang tidak berwenang

Secara umum kriptografi dapat disimpulkan bahwa kriptografi merupakan ilmu sekaligus seni untuk menjaga kerahasiaan data atau informasi agar

tidak dapat di lihat, dibaca, dimengerti oleh pihak ketiga yang tidak memiliki wewenang terhadap data atau informasi tersebut. Kriptografi memiliki 4 komponen utama yaitu :

1. *Plaintext*, yaitu pesan yang dapat dibaca.
2. *Ciphertext*, yaitu pesan sandi/pesan acak yang tidak bisa dibaca.
3. *Key*, yaitu kunci untuk melakukan teknik kriptografi.
4. *Algoritma*, yaitu metode untuk melakukan *enkripsi* dan *dekripsi*.

a. Pesan, *plainteks* dan *cipherteks*

Pesan merupakan informasi yang dapat dibaca maknanya, nama lain dari pesan yaitu *plainteks*. Agar pesan tersebut tidak dimengerti pihak orang lain maka perlu disandikan kebentuk yang tidak dimengerti orang lain yang di sebut *cipherteks*.

b. Pengirim dan penerima

Pengirim adalah entitas pengirim pesan kepada entitas lainnya. Sedangkan penerima adalah entitas yang menerima pesan tersebut.

c. *Enkripsi* dan *dekripsi*

Enkripsi yaitu proses menyandikan *plainteks* menjadi *cipherteks*, sedangkan *dekripsi* mengembalikan *cipherteks* menjadi *plainteks*.

d. *Cipher*

Cipher merupakan aturan untuk mengenkripsi dan dekripsi. *Cipher* memiliki konsep matematika untuk memetakan elemen-elemen *plainteks* dan himpunan yang berisi *cipherteks*.

e. Sistem kriptografi

Sistem kriptografi ini sendiri merupakan sekumpulan yang terdiri dari algoritma kriptografi, semua *plainteks* dan *cipherteks* yang akan dikunci.

f. Penyadap

Penyadap merupakan orang yang berusaha untuk menangkap pesan yang ditransmisikan dengan tujuan untuk mendapatkan informasi.

g. Kriptanalisis dan kriptologi

Kriptanalisis (*cryptanalysis*) adalah suatu seni dan ilmu untuk memecahkan *cipherteks* menjadi *plainteks* tanpa mengetahui kunci yang digunakan, sedangkan kriptologi yaitu studi yang mengenai kriptografi dan kriptanalisis.

2.3 Video

Menurut Aria Pramudito (2015), Video merupakan teknologi pemrosesan sinyal elektronik mewakilkan gambar bergerak. Jadi video adalah teknologi yang mewakili pemrosesan pesan (pita suara atau piringan suara) dalam bentuk *auditif* dan gerak gambar.

Video secara umum merupakan media salah satu jenis media audio-visual dan dapat menggambarkan suatu objek yang bergerak bersama-sama dengan suara alamiah atau suara yang sesuai.

2.4 Multimedia

Menurut Munir (2013), Multimedia adalah integrasi elemen beberapa media seperti audio, video, grafik, teks dan animasi yang saling sinergis guna memberi manfaat bagi pengguna daripada hanya satu media. Sedangkan pengertian multimedia dalam konteks komputer adalah penggunaan komputer untuk menyajikan dan menggabungkan teks, suara, video, gambar dan animasi.

Manusia dapat memanfaatkan multimedia untuk mengkombinasi text, menampilkan *graphics*, audio, video dan animasi dengan menggunakan *links* dan *tools* yang memungkinkan pemakai untuk melakukan navigasi, berinteraksi, membuat, dan berkomunikasi.

Secara umum multimedia memiliki beberapa jenis, yaitu:

- a. Multimedia *interaktif*: Multimedia *interaktif* merupakan gabungan media-media yang terdiri dari teks, desain grafis, audio, dan rancangan lain.
- b. Multimedia *linier*: Multimedia *linier* dapat berjalan secara lurus yang artinya berjalan tanpa kontrol dari pengguna dan merupakan jenis yang paling umum di masyarakat.

- c. Multimedia *Hiperaktif* : Multimedia *hiperaktif* ini mempunyai struktur dengan unsur yang terkait nantinya diarahkan oleh pengguna melalui link dengan unsur multimedia yang ada.
- d. Multimedia *kits* : Multimedia *kits* ini digunakan sebagai pembelajaran yang melibatkan lebih dari satu jenis media dan diorganisir oleh topik tunggal.

Manfaat multimedia di dalam kalangan masyarakat yaitu :

- a. Manfaat multimedia untuk pendidikan

Dalam dunia pendidikan, multimedia dapat digunakan sebagai media pembelajaran modern seiring dengan perkembangan jaman dimana koneksi semakin luas dan sumber yang diperoleh tidak hanya didapat dari benda berwujud dengan pembelajaran monoton. Melalui multimedia ini sistem belajar mengajar pun dapat dilakukan secara otodidak serta dapat membuka wawasan lebih luas.

- b. Manfaat multimedia untuk bisnis

Di dalam dunia bisnis pun, multimedia menjadi sesuatu yang sangat untuk mempromosikan, mengelola termasuk dijadikan multimedia digunakan sebagai profil perusahaan, promosi produk, hingga media informasi serta bermanfaat untuk sistem e-learning. Sehingga penggunaan multimedia dapat meningkatkan kinerja perusahaan lebih baik dan cepat.

2.5 *MP4*

Menurut Hengki Tamando Sihotang (2018), mengatakan bahwa *MP4* adalah Satu-satunya ekstensi nama file resmi untuk file *MP4*. *MP4* adalah salah satu format multimedia, bisa juga disebut dengan *MPEG-4*. Pada umumnya format ini digunakan untuk merekam video serta audio, tetapi kemampuan lainnya adalah dapat menangani data lain seperti *subtitle*. Kelebihan lainnya adalah bisa dilakukannya streaming melalui internet. *MP4* adalah nama *extension* atau ekstensi untuk format *MPEG-4*.

2.6 **Algoritma Kriptografi**

Menurut Muhammad Fauzan Edy Purnomo, et al (2015) Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut dengan melakukan pembangkitan kunci, *enkripsi* dan *dekripsi*. Algoritma Kriptografi terdiri dari tiga fungsi dasar yaitu :

1. Kunci yang di pakai untuk melakukan enkripsi dan dekripsi, kunci terbagi dua bagian yaitu kunci publik (*public key*) dan kunci privat (*private key*).
2. *Enkripsi* merupakan proses transformasi terhadap teks asli sehingga menghasilkan teks sandi. Sedangkan dekripsi merupakan proses pemulihan kembali teks sandi menjadi teks asli bila kunci rahasia yang dipakai dekripsi sama dengan kunci rahasia yang dipakai untuk enkripsi .

3. *Dekripsi* merupakan kebalikan dari enkripsi, pesan telah dienkripsi dikembalikan ke bentuk asalnya (*plaintext*) disebut dengan dekripsi pesan.

Enkripsi dan dekripsi merupakan fungsi yang memetakan elemen-elemen antara kedua himpunan tersebut. Misalkan P menyatakan plaintext dan C menyatakan ciphertext, maka fungsi enkripsi E memetakan P ke C :

$$E(P) = C \dots\dots\dots (1)$$

Dan fungsi dekripsi D memetakan C ke P ,

$$D(C) = P \dots\dots\dots (2)$$

Karena proses enkripsi kemudian dekripsi mengembalikan pesan ke pesan asal,

maka kesamaan berikut harus benar,

$$D(E(P)) = P \dots\dots\dots (3)$$

2.7 Algoritma RC4

Menurut Kirman (2018:82) Mengatakan Algoritma *RC4* secara luas pada sistem keamanan seperti protokol SSL (*Secure Socket Layer*). Algoritma kriptografi ini sederhana dan mudah diimplementasikan. *RC4* dibuat oleh *Ron Rivest* dari laboratorium *RSA* (*RC* adalah singkatan dari *Ron's Code*). *RC4* membangkitkan aliran kunci (*keystream*) yang kemudian di-*XOR*-kan dengan *plaintext* pada waktu *enkripsi* (atau di-*XOR*-kan dengan bit-bit *ciphertext* pada waktu dekripsi). Tidak seperti *chipper* aliran yang memproses data dalam

bit, *RC4* memproses data dalam ukuran byte (1 byte = 8 bit). Untuk membangkitkan aliran kunci, *chipper* menggunakan status internal yang terdiri dari 2 bagian:

1. Permutasi angka 0 sampai 255 di dalam larik S_0, S_1 sampai dengan S_{255} .
Permutasi merupakan kunci U dengan panjang variable.
2. Dua buah pencacah indeks, i dan j . Sistem sandi *RC4* menggunakan state, yaitu larik *byte* berukuran 256 yang terpermutasi, dan tercampur oleh kunci. Kunci enkripsi juga dan tercampur oleh kunci. Kunci enkripsi juga merupakan larik *byte* berukuran 256. Sebelum melakukan enkripsi, dan dekripsi, sistem sandi *RC4* melakukan inisialisasi terhadap *state* dengan algoritma, Algoritma ini disebut dengan penjadwalan kunci (*key scheduling*).

Terdapat dua tahapan untuk membangkitkan aliran kunci algoritma *RC4* yaitu Key Scheduling Algorithm (KSA) dan Pseudo-Random Generator Algorithm (PRGA). Key Scheduling Algorithm (KSA) merupakan tahapan pemberian nilai awal berdasarkan kunci enkripsi. State dari nilai awal tersebut berupa array dengan representasi permutasi 256 byte (dengan indeks 0 sampai dengan 255) dinamakan array S . Menggunakan rentang tersebut karena *RC4* mengenkripsi pada mode byte ($255 = 2^8$ dan 8 bit = 1 byte). Artinya maksimal panjang kunci yang dapat tersimpan pada array U adalah 256 karakter. Permutasi terhadap nilai array S dilakukan dengan pseudo-code berikut :

$j = 0$

for $i = 0$ to 255

```

S[i] = i
for i = 0 to 255
    j = ( j + S[i] + U[i] ) mod 256 swap ( S[i], S[j] ) (*pertukaran
    nilai S[i] dan S[j] *)

```

Tahap selanjutnya hasil dari array S yang telah melalui KSA akan diproses kembali pada *PRGA* (*Pseudo-Random Generator Algorithm*). Pada tahap *PRGA* terjadi modifikasi state dan output sebuah byte dari aliran kunci, dimana *array S* beroperasi dengan *array U* yang selanjutnya akan menghasilkan kestream. Nilai $S[i]$ dan $S[j]$ diambil dan dijumlahkan dengan modulo 256 untuk membangkitkan aliran kunci. Hasil dari perhitungan tersebut akan menjadi indeks $S[\text{indeks}]$ yang menjadi aliran kunci K yang kemudian digunakan untuk mengenkripsi plainteks ke-aliran kunci K yang kemudian digunakan untuk mengenkripsi plainteks ke-idx. Setiap putaran bagian *kestream* sebesar 1 *byte* (dengan nilai antara 0 sampai dengan 255) di outputkan oleh *PRGA* berdasarkan state S . Berikut adalah *PRGA* dalam bentuk pseudo-code:

```

i = 0
j = 0
for idx = 0 to Panjang Plainteks 1 do
    i = ( i + 1 ) mod 256
    j = ( j + S[i] ) mod 256
    swap ( S[i], S[j] ) (* penukaran nilai S[i] dan S[j] *)

```

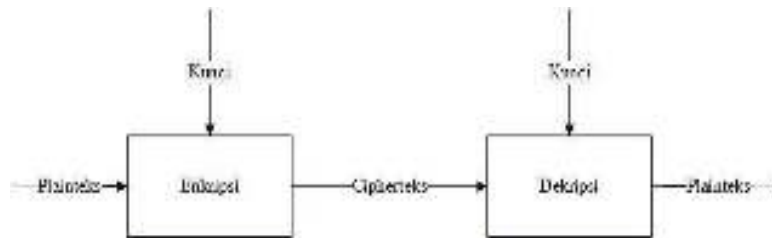
$$K = (S[i] + S[j]) \bmod 256$$

Setelah *keystream* terbentuk, kemudian *keystream* tersebut dimasukkan dalam operasi *XOR* dengan plaintext.

2.8 Algoritma *Simetris*

Algoritma *simetris* merupakan algoritma kriptografi yang menggunakan kunci *enkripsi* yang sama dengan kunci *dekripsi*. Istilah lain untuk kriptografi kunci-simetri adalah kriptografi kunci *privat* (*private-key cryptography*), kriptografi kunci rahasia (*secret-key cryptography*), atau kriptografi konvensional (*conventional cryptography*). Mengasumsikan pengirim dan penerima pesan sudah berbagi kunci yang sama sebelum bertukar pesan. Keamanan sistem kriptografi simetris terletak pada kerahasiaan kuncinya. Kriptografi simetris merupakan satu-satunya jenis kriptografi yang dikenal dalam catatan sejarah hingga tahun 1976. Semua algoritma kriptografi klasik termasuk ke dalam sistem kriptografi simetris. Kelebihan algoritma simetris ini adalah proses enkripsi dan deskripsinya yang jauh lebih cepat dibandingkan dengan algoritma *asimetris*. Sedangkan kelemahan algoritma ini adalah permasalahan distribusi kunci (*key distribution*). Seperti yang telah dibahas, proses *enkripsi* dan *deskripsi* menggunakan kunci yang sama. Sehingga muncul persoalan

menjaga kerahasiaan kunci, yaitu pada saat pengiriman kunci pada media yang tidak aman seperti internet. Tentunya jika kunci ini sampai hilang atau sudah dapat ditebak oleh orang lain. Berikut gambar proses enkripsi dan dekripsi algoritma simetris:



Gambar 2.1. Proses algoritma simetris

Sumber: Frenky Fernando (2016)

2.9 Bahasa pemrograman

Bahasa pemrograman adalah perintah-perintah atau instruksi yang dimengerti oleh komputer untuk melakukan tugas tertentu. Bahasa pemrograman merupakan sebuah instruksi untuk memerintah komputer agar bisa menjalankan fungsi tertentu, namun hanya instruksi standar saja. Bahasa pemrograman juga memiliki perhimpunan dari aturan sintaks dan semantik yang tugasnya untuk mendefinisikan program komputer. Bahasa pemrograman komputer yang kita kenal antara lain adalah *Java*, *Visual Basic*, *C++*, *C*, *PHP*, dan bahasa pemrograman lainnya. Namun tentu saja kebutuhan bahasa ini harus disesuaikan dengan fungsi dan perangkat yang menggunakannya.

Menurut generasi bahasa pemrograman digolongkan menjadi 4 generasi, yaitu:

- a. Generasi ke-1: *machine language*

- b. Generasi ke-2: *assembly language: Assembler*
- c. Generasi ke-3: *high level programming language*, contoh: C dan *Pascal*
- d. Generasi ke-4: *4 GL (fourth-generation language)*, contoh: *SQL*
- e. Generasi ke-5: *Programming Language Based Object Oriented & Web*

Secara umum bahasa pemrograman dibagi menjadi 4 kelompok, yaitu :

1. *Object Oriented Language* : Seperti bahasa *Visual C, Delphi, Visual dBase, Visual FoxPro*.
2. *Low Level Language* : Bahasa *Assembly*.
3. *Middle Level Language* : Bahasa *C*.
4. *High Level Language* : Bahasa *Basic* dan *Pascal*.

Menurut tingkat kedekatannya dengan mesin komputer, bahasa pemrograman terdiri dari:

- a. Bahasa Mesin, yaitu memberikan perintah kepada komputer dengan memakai kode bahasa biner, contohnya 01100101100110.
- b. Bahasa Tingkat Rendah, atau dikenal dengan istilah bahasa rakitan (bah.Ingggris *Assembly*), yaitu memberikan perintah kepada komputer dengan memakai kode-kode singkat (kode *mnemonic*), contohnya *MOV, SUB, CMP, JMP, JGE, JL, LOOP*, dsb.

- c. Bahasa Tingkat Menengah, yaitu bahasa komputer yang memakai campuran instruksi dalam kata-kata bahasa manusia (lihat contoh Bahasa Tingkat Tinggi di bawah) dan instruksi yang bersifat simbolik, contohnya {, }, ?, <<, >>, &&.
- d. Bahasa Tingkat Tinggi, yaitu bahasa komputer yang memakai instruksi berasal dari unsur kata-kata bahasa manusia, contohnya *begin, end, if, for, while, and, or, dsb.* Komputer dapat mengerti bahasa manusia itu diperlukan program *compiler* atau *interpreter*.

Fungsi dari bahasa pemrograman adalah untuk memerintahkan sebuah komputer agar dapat mengolah data yang sesuai dengan di inginkan. *Output* dari bahasa pemrograman ini dapat berupa aplikasi ataupun program khusus. Contoh sederhananya seperti lampu lalu lintas di jalan raya.

2.10 Visual Basic.Net

Platform Microsoft.Net merupakan model untuk *development* dimana *platform* dan aplikasi bisa dibuat dan dijalankan tanpa bergantung pada alat (*device*) yang dipakai. Teknologi ini memungkinkan beberapa aplikasi bekerja sama. *Visual Basic.Net* merupakan *core* dari pembuatan aplikasi berbasis .Net, yang merupakan lingkungan pemrograman yang mempermudah tahapan *design, development, debugging, dan development* dari aplikasi berbasis .Net dan *XML web service*, serta meningkatkan efisiensi *developer* dengan menyediakan lingkungan pemrograman yang sudah biasa digunakan.

Bahasa *Visual Basic* pada dasarnya adalah bahasa yang mudah dimengerti sehingga pemrograman di dalam bahasa *Basic* dapat dengan mudah dilakukan meskipun oleh orang yang baru belajar membuat program. *Visual Basic* mempunyai teknik pemrograman *visual* yang memungkinkan penggunanya untuk berkreasi lebih baik dalam menghasilkan suatu program aplikasi. Ini terlihat dari dasar pembuatan dalam *visual basic* adalah *FORM*, dimana pengguna dapat mengatur tampilan form kemudian dijalankan dalam script yang sangat mudah. Pemakaian *Visual Basic* ditandai dengan kemampuan *Visual Basic* untuk dapat berinteraksi dengan aplikasi lain di dalam sistem operasi *Windows* dengan komponen *ActiveX Control*. Dalam *Microsoft Visual Basic.Net* terdapat dua komponen utama adalah:

1. *Net Framework Class Library*.

Komponen ini digunakan untuk menjalankan sebuah aplikasi melalui objek yang telah didefinisikan, antara lain : label, form, textbox, button, listbox, datetimestamp, dan lain-lain.

2. *Common Language Runtime (CLR)*

Komponen ini digunakan untuk mengeksekusi program yang ditulis dalam bahasa pemrograman yang ada dalam lingkungan *Microsoft Visual Studio.Net*, seperti: *C.Net*, *C++*, *Net*, dan juga *Visual basic.Net*.

1. Kelebihan *Visual Basic*

- a. *VB.Net* mempunyai fasilitas *Real Time Background Compiler* yaitu sebagai penanganan dalam error atau bug.
- b. Lebih cepat dalam pembuatan aplikasi berbasis desktop
- c. Menyediakan untuk *developer* pemrograman data akses *ActiveX Data Object (ADO)*.

2. Kelemahan Visual Basic

- a. Untuk versi *VB.Net 2010* dan seterusnya tidak mempunyai Komponen *Crystal Report* karena sudah terpisah.
- b. Harus *ada Net framework* agar aplikasi bisa berjalan
- c. Tidak mempunyai database sendiri.
- d. Memerlukan kapasitas yang besar untuk instalasi *VB.Net*.

2.11 Microsoft Visual Studio

Microsoft Visual Studio merupakan sebuah perangkat lunak lengkap (*suite*) yang dapat digunakan untuk melakukan pengembangan aplikasi, baik aplikasi bisnis, aplikasi personal, ataupun komponen aplikasi lainnya.

Visual Studio mencakup *compiler*, *SDK*, *Integrated Development Environment (IDE)*, dan dokumentasi. *Visual Studio* dapat digunakan untuk mengembangkan aplikasi dalam *native code* (dalam bentuk bahasa mesin yang berjalan di atas *windows*) ataupun *managed code* (dalam bentuk *Microsoft Intermediate Language* diatas *.NET Framework*).

Pengguna dapat memanfaatkan *Visual Studio* untuk membuat beberapa hal seperti web dan menulis beberapa kode pemrograman seperti *Python*, *Ruby*, *Visual Basic*, *C*, *C++* dan *Java*.

2.12 UML (*Unified Modeling Language*)

UML (Unified Modeling Language) awalnya termotivasi oleh keinginan untuk membakukan sistem notasi yang berbeda dan pendekatan untuk desain perangkat lunak yang dikembangkan oleh Grady Booch , Ivar Jacobson dan James Rumbaugh Rational Software ditahun 1994-1995, dengan pengembangan lebih lanjut yang dipimpin oleh mereka melalui tahun 1996. Pada tahun 1997 *UML* diadopsi sebagai standar oleh *Object Management Group (OMG)*, dan telah dikelola oleh organisasi ini sejak. Pada tahun 2005 *UML* juga diterbitkan oleh *International Organization for Standardization (ISO)* sebagai *standart ISO* disetujui. Sejak itu telah periodik direvisi untuk menutupi revisi terbaru dari *UML*.

UML (Unified Modeling Language) adalah Metodologi kolaborasi antara metode-metode Booch, *OMT (Object Modeling Technique)*, serta *OOSE (Object Oriented Software Engineering)* dan beberapa metoda lainnya, merupakan metodologi yang paling sering digunakan saat ini untuk analisa dan perancangan sistem dengan metodologi berorientasi objek mengadaptasi maraknya penggunaan bahasa “*pemrograman berorientasi objek*” (*OOP*).

Berikut beberapa tujuan atau fungsi dari penggunaan *UML*, yang diantaranya:

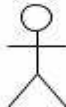




- a. Dapat memberikan bahasa permodelan *visual* kepada pengguna dari berbagai macam pemrograman maupun proses rekayasa.
- b. Dapat menyatukan praktek-praktek terbaik yang ada dalam permodelan.
- c. Dapat memberikan model yang siap untuk digunakan, merupakan bahasa permodelan *visual* yang ekspresif untuk mengembangkan sistem dan untuk saling menukar model secara mudah.
- d. Dapat berguna sebagai *blue print*, sebab sangat lengkap dan detail dalam perancangannya yang nantinya akan diketahui informasi yang detail mengenai koding suatu program.
- e. Dapat memodelkan sistem yang berkonsep berorientasi objek, jadi tidak hanya digunakan untuk memodelkan perangkat lunak (*software*) saja.
- f. Dapat menciptakan suatu bahasa permodelan yang nantinya dapat dipergunakan oleh manusia maupun oleh mesin.




2.13 Use Case Diagram

Use case Diagram yang menggambarkan actor, use case dan relasinya sebagai suatu urutan tindakan yang memberikan nilai terukur untuk aktor. Sebuah use case digambarkan sebagai elips horizontal dalam suatu diagram *UML use case*. *Use Case* memiliki dua istilah yaitu :

1. *System use case*: interaksi dengan sistem.
2. *Business use case*: interaksi bisnis dengan konsumen atau kejadian nyata.

Tabel 2.1. Simbol *Use Case Diagram*.

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i> .
2		<i>Dependency</i>	Hubungan dimana perubahan yang terjadi pada suatu elemen mandiri (<i>independent</i>) akan mempengaruhi elemen yang bergantung padanya .
3		<i>Generalization</i>	Hubungan dimana objek anak (<i>descendent</i>) berbagi perilaku dan struktur data dari objek yang ada di atasnya objek induk (<i>ancestor</i>).
4		<i>Include</i>	Menspesifikasikan bahwa <i>use case</i> sumber secara <i>eksplisit</i> .
5		<i>Extend</i>	Menspesifikasikan bahwa <i>use case</i> target memperluas perilaku dari <i>use case</i> sumber pada suatu titik yang diberikan.


NO	GAMBAR	NAMA	KETERANGAN
6		<i>Association</i>	Apa yang menghubungkan antara objek satu dengan objek lainnya.
7		<i>System</i>	Menspesifikasikan paket yang menampilkan sistem secara terbatas.
8		<i>Use Case</i>	Deskripsi dari urutan aksi-aksi yang ditampilkan sistem yang menghasilkan suatu hasil yang terukur bagi suatu aktor.





Sumber: Yosua P.W Simaremare, 2013

2.14 Activity Diagram

Activity Diagram Menggambarkan aktifitas-aktifitas, objek, state, transisi state dan event. Dengan kata lain kegiatan diagram alur kerja menggambarkan perilaku sistem untuk aktivitas.

Tabel 2.2 Simbol Activity Diagram

NO	GAMBAR	NAMA	KETERANGAN
1		<i>Actifity</i>	Memperlihatkan bagaimana masing-masing kelas antarmuka saling berinteraksi satu sama lain.





NO	GAMBAR	NAMA	KETERANGAN
2		<i>Action</i>	<i>State</i> dari sistem yang mencerminkan eksekusi dari suatu aksi.
3		<i>Initial Node</i>	Bagaimana objek dibentuk atau diawali.
4		<i>Activity Final Node</i>	Bagaimana objek dibentuk dan dihancurkan.
5		<i>Fork Node</i>	Satu aliran yang pada tahap tertentu berubah menjadi beberapa aliran.

Sumber: Yosua P.W Simaremare (2013)

2.15 Sequence Diagram

Sequence diagram adalah suatu diagram yang menggambarkan interaksi antar obyek dan mengindikasikan komunikasi diantara objek-objek tersebut. Diagram ini juga menunjukkan serangkaian pesan yang dipertukarkan oleh objek-objek yang melakukan suatu tugas atau aksi tertentu. Objek-objek tersebut kemudian diurutkan dari kiri ke kanan, aktor yang menginisiasi interaksi biasanya ditaruh di paling kiri dari diagram. Pada diagram ini, dimensi vertikal merepresentasikan waktu.

Tabel 2.3. Simbol Sequence Diagram

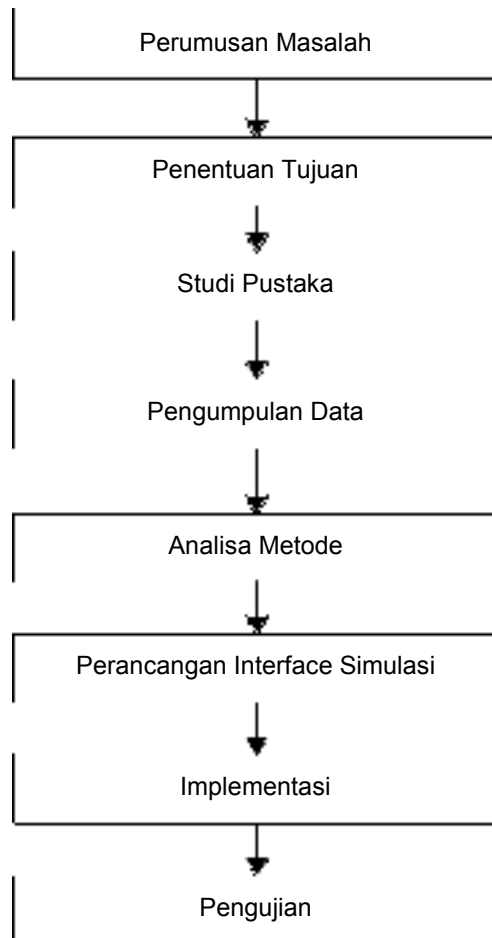
NO	GAMBAR	NAMA	KETERANGAN
1		<i>Actor</i>	Menspesifikasikan himpunan peran yang pengguna mainkan ketika berinteraksi dengan <i>use case</i> .
2		<i>LifeLine</i>	Objek <i>entity</i> , antarmuka yang saling berinteraksi.
3		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi
4		<i>Message</i>	Spesifikasi dari komunikasi antar objek yang memuat informasi-informasi tentang aktifitas yang terjadi

Sumber: Yosua P.W Simaremare (2013)

BAB III METODE PENELITIAN

3.1 Tahapan Penelitian

Adapun tahapan penelitian yang dilakukan oleh penulis ini dengan judul Pembuatan Aplikasi Kriptografi Video (*Mp4*) Menggunakan Algoritma *RC4* adalah sebagai berikut:



Gambar 3.1 *Tahapan Penelitian*

3.2 Metode Pengumpulan Data

Pengumpulan data adalah pencarian terhadap sesuatu karena ada perhatian dan keinginan terhadap hasil suatu aktivitas. Metode pengumpulan data dalam penulisan ini dibagi menjadi 2, yaitu :

1. Pengamatan (*Observation*)

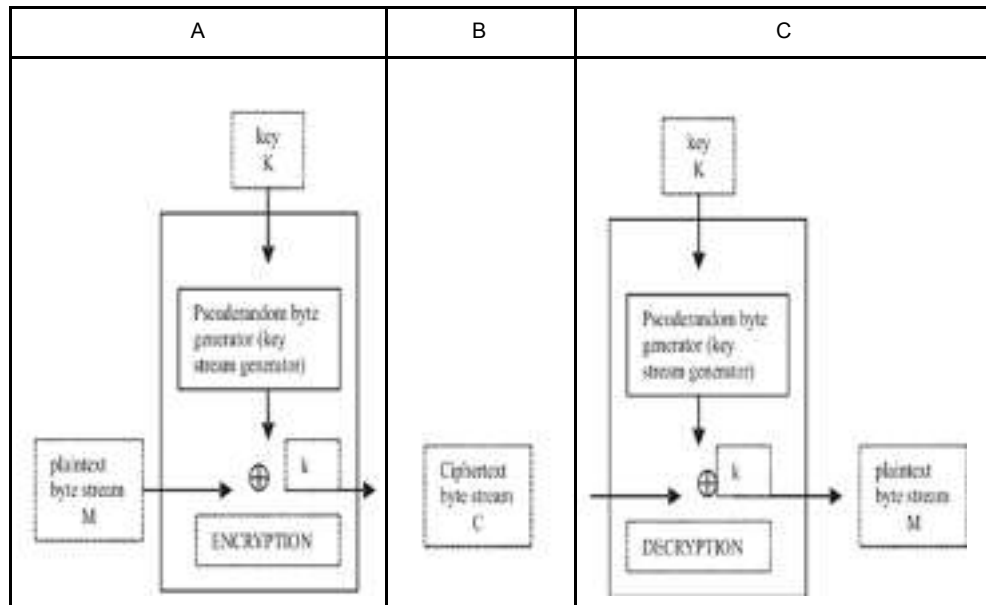
Penulis melakukan pengamatan langsung pada setiap jenis-jenis proses pengamanan video untuk menentukan keamanan video.

2. Penelitian Kepustakaan (*Library Research*)

Merupakan cara untuk mencari referensi dengan mengumpulkan bahan-bahan pustaka yang dilakukan di perpustakaan kampus, maupun perpustakaan umum, juga melakukan pencarian lewat internet, dengan mengunjungi situs-situs seperti *google Book online* yang dapat membantu pembahasan materi.

3.3 Analisis Permasalahan yang Berjalan

Pertukaran data dalam hal ini pesan rahasia berbentuk video dengan menggunakan metode tradisional yaitu dengan cara bertukar kata kunci tunggal. Diagram dibawah adalah penggambaran bagaimana pertukaran pesan rahasia menggunakan kunci tunggal terjadi.



Gambar 3.2 Analisis Permasalahan yang Berjalan

Pemberitahuan kata kunci dari pengirim ke penerima menggunakan media yang umum digunakan oleh banyak orang.

Keterangan:

- A = Proses *Enkripsi* video
- B = Proses Penambahan byte kunci pada Proses *Enkripsi*
- C = Proses Deskripsi video yang sudah di *enkripsi*.

3.4 Analisa Kelemahan yang Berjalan

1. Penggunaan kata kunci tunggal berpotensi terjadinya salah pemahaman. Dalam hal ini kemungkinan penerima salah mengartikan kunci yang diberikan oleh pengirim adalah hal yang dapat terjadi.

2. Pemberitahuan atau pertukaran kata kunci yang dikirimkan oleh pengirim ke penerima memiliki potensi dapat diketahui oleh orang lain sehingga pesan rahasia dapat terbongkar.

3.5 Solusi Pemecahan Masalah

Pemecahan masalah yang penulis lakukan adalah dengan melakukan penerapan metode ini yang didalamnya terdapat Algoritma *RC4*. Penggunaan metode ini dapat digunakan sebagai solusi agar pengirim dan penerima tidak lagi harus bertukar kunci tunggal untuk membuka pesan melainkan dapat memiliki kata kunci masing-masing.

Tabel 3.1 *Tabel Perencanaan Rancangan*

No	Sistem yang Berjalan	Sistem yang Diusulkan	Hasil yang Ingin Dicapai
1.	Penggunaan kunci tunggal yang harus diketahui oleh pengirim dan penerima untuk membuka pesan.	Pengirim dan penerima memiliki kunci masing-masing untuk membuka pesan	Tidak ada lagi kesalahan pemahaman atau salah tafsir kunci tunggal karena pengirim dan penerima memiliki kunci yang ditetapkan masing pihak.

2	Pertukaran kunci tunggal menggunakan media komunikasi yang rentan untuk dapat diketahui orang lain.	Pengirim dan penerima dapat menentukan sendiri kunci yang ingin digunakan untuk membuka pesan.	Kemungkinan bocornya kunci saat proses pertukaran informasi kunci tunggal dapat dihindari.
---	-----------------------------------------------------------------------------------------------------	------------------------------------------------------------------------------------------------	--------------------------------------------------------------------------------------------

3.6 Analisa Kebutuhan Sistem

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen-komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukan sehingga menghasilkan suatu keluaran yang diinginkan.

1. Analisis Perangkat Keras (*Hardware*)

Perangkat keras minimum yang digunakan untuk membangun Sistem Informasi Penjualan ini adalah

- a. *Processor* berkecepatan 2.0 Ghz
- b. *RAM* 2 Gb

- c. Harddisk minimal 10 Gb untuk menyimpan data
- d. LAN Card
- e. Keyboard dan Mouse
- f. Monitor 14.

2. Analisis Perangkat Lunak (*Software*)

Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (*software*) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

- a. *Microsoft Windows* 10 sebagai sistem operasi
- b. *Visual Basic* Sebagai bahasa pemrograman.
- c. *Visual Studio*

3.7 Analisa Proses Sistem Yang Berjalan

Visual basic 2010 akan menjadi sarana untuk menciptakan perangkat lunak ini. Pada analisa proses ini penggunaan digunakan sebagai metode yang didalamnya terdapat kombinasi dari algoritma *RC4*. Algoritma *RC4* digunakan oleh pengirim untuk mengenkripsi pesan yang akan dikirimkan..

Implementasi algoritma *RC4* dengan mode 4 *byte* (untuk lebih menyederhanakan dalam perhitungan manual) serta untuk kebutuhan sistem yang sangat terbatas. S-Box dengan panjang 4 *byte*, dengan $S[0]=0$, $S[1]=1$, $S[2]=2$ dan $S[3]=3$ sehingga array S menjadi:

0123

Inisialisasi 4 *byte* kunci *array*, K. Misalkan kunci Ulang kunci sampai memenuhi seluruh adalah 2 5 7 3, sehingga array K berisi 2 5 7 3 dan mencoba untuk mengenkripsikan kata HALO.

Inisialisasi *i* dan *j* dengan 0 kemudian dilakukan KSA agar tercipta *state-array* yang acak.

Penjelasan iterasi lebih lanjut dapat dijelaskan sebagai berikut:

Iterasi 1

$i = 0$

$j = (0 + S[0] + K [0 \bmod 4]) \bmod 4$

$= (0 + 0 + 2) \bmod 4 = 2$

Swap ($S[0], S[2]$)

Hasil *Array* S

2103 Iterasi 2

$i = 1$

$j = (2 + S[1] + K [1 \bmod 4]) \bmod 4$

$$= (2 + 1 + 5) \bmod 4 = 0$$

Swap (S[1],S[0]) Hasil

Array S

1203

Iterasi 3

$$i = 2$$

$$j = (0 + S[2] + K [2 \bmod 4]) \bmod 4$$

$$= (0 + 0 + 7) \bmod 4 = 3$$

1230

Iterasi 4

$$i = 3$$

$$j = (3 + S[3] + K [3 \bmod 4]) \bmod 4$$

$$= (3 + 0 + 3) \bmod 4 = 2$$

Swap (S[3],S[2])

Hasil Array S

1203

Setelah melakukan KSA, akan dilakukan PRGA. PRGA akan dilakukan sebanyak 4 kali dikarenakan plainteks yang akan dienkrpsi berjumlah 4 karakter. Hal ini disebabkan karena

dibutuhkan 1 kunci dan 1 kali pengoperasian XOR untuk tiap tiap karakter pada plainteks.

Berikut adalah tahapan penghasilan kunci enkripsi dengan PRGA.

Array S

1203

Inisialisasi

$i = 0$

$j = 0$

Iterasi 1

$i = (0 + 1) \bmod 4 = 1$

$j = (0 + S[1]) \bmod 4 = (0 + 2) \bmod$

$4 = 2$

swap (S[1],S[2])

1023

$K1 = S[(S[1]+S[2]) \bmod 4] = S[2]$

$\bmod 4] = 2$

$K1 = 00000010$

Iterasi 2

$i = (1 + 1) \bmod 4 = 2$

$j = (2 + S[2]) \bmod 4 = (2 + 2) \bmod$

$4 = 0$

swap (S[2],S[0])

2013

$K2 = S[(S[2]+S[0]) \bmod 4] = S[3]$

$\bmod 4] = 3$

$K2 = 00000011$

Iterasi 3

$i = (2 + 1) \bmod 4 = 3$

$j = (0 + S[3]) \bmod 4 = (0 + 3) \bmod$

$4 = 3$

swap (S[3],S[3])

1023

$K3 = S[(S[3]+S[3]) \bmod 4] = S[6]$

$\bmod 4] = 2$

$K3 = 00000010$

Iterasi 4

$i = (3 + 1) \bmod 4 = 0$

$j = (3 + S[0]) \bmod 4 = (3 + 1) \bmod$

$4 = 0$

swap (S[0],S[0])

1023

$$K1 = S[(S[0]+S[0]) \bmod 4] = S[2]$$

$$\bmod 4] = 2$$

$$K4 = 00000010$$

Setelah menemukan kunci untuk tiap karakter, makadilakukan operasi XOR antara karakter pada plaintext dengan kunci yang dihasilkan. Berikut adalah tabel ASCII untuk tiap-tiap karakter pada plaintks yang digunakan.

Huruf Kode ASCII (Binary 8 bit)

Karakter	Decimal	Binary
H	72	01001000
A	65	01000001
L	76	01001100
O	79	01001111

Berikut adalah proses pengXORan dari plainteks dengan key yang telah didapat:

HALO : 01001000 01000001 01001100 01001111

Key : 01100101 01101001 01101100 01100101

Cipherteks : 01001010 01000010 01001110 01001101

Proses dekripsi ciphertext menggunakan algoritma RC4 ini sama untuk proses key-schedule-nya. Untuk mendapatkan plaintext, ciphertext yang diperoleh di XORkan dengan

pseudo random byte yang didapat sebelumnya. Maka hasilnya adalah plainteks atau teks asli.

Pesan dikirim dalam bentuk cipherteks sehingga setelah sampai di penerima pesan dapat kembali diubah menjadi plainteks dengan meng-XOR-kan dengan kunci yang sama.

Pemrosesan pesan setelah sampai pada penerima dapat dilihat pada dibawah ini.

Proses XOR pseudo random byte dengan cipherteks pada dekripsi yaitu:

Cipherteks : 01001010 01000010 01001110 01001101

pseudo random byte : 01100101 01101001 01101100 01100101

Plainteks : 01001000 01000001 01001100 01001111

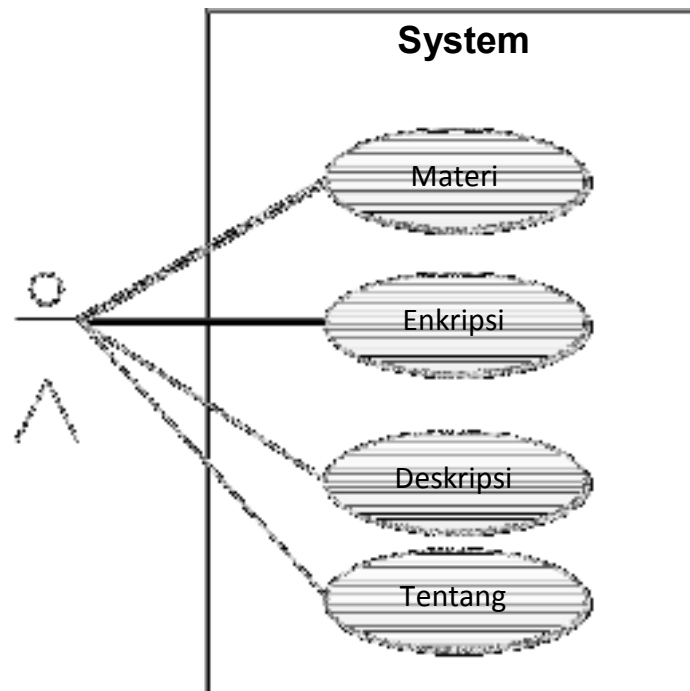
H A L O

3.8 Perancangan Berorientasi Obejek

Perancangan atau Pemodelan Berorientasi Ojek merupakan proses mendapatkan informasi dari model dan menampilkannya secara grafik dengan menggunakan sebuah standar elemen grafik. Tujuan dari perancangan berorientasi ojbek ini memungkinkan adanya komunikasi yang lebih berkualitas antara pengguna, pengembang penganalisis, tetster, manajer dan siapapun yang terlibat dalam proyek pengembangan sistem informasi.

1. Use case Diagram

Berikut adalah *use case* diagram yang menggambarkan kegiatan.

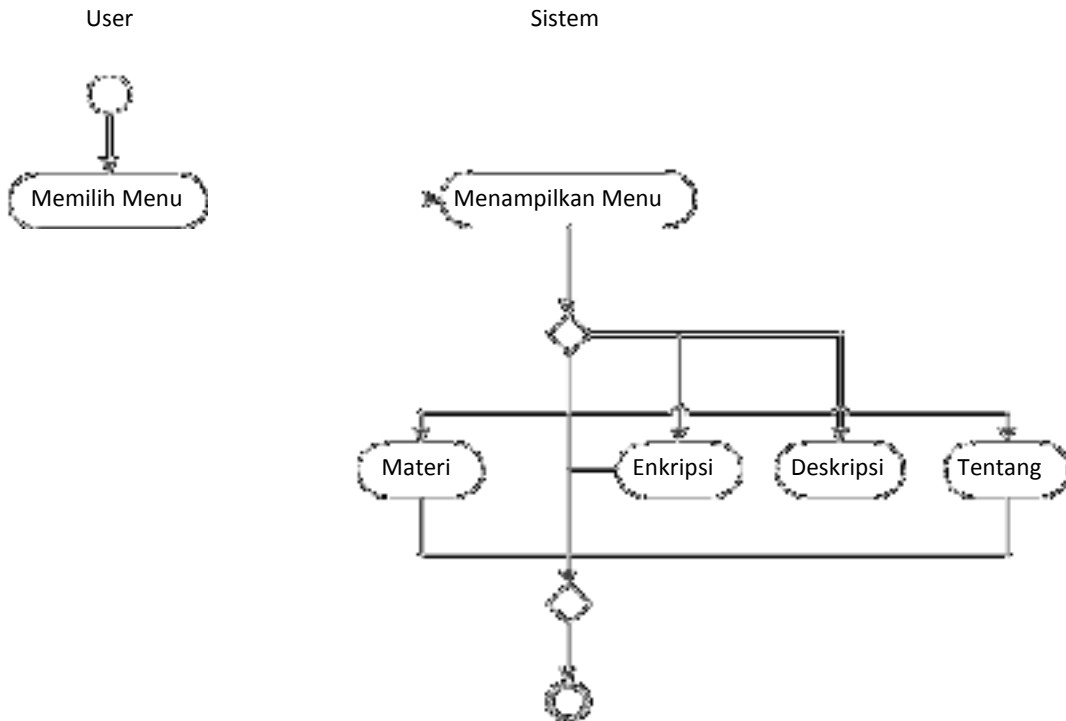


Gambar 3.3. *Use Case Diagram*

Dalam use case diagram di atas, user/pengguna sebagai actor yang mempunyai use case Materi, Enkripsi dan Tentang.

2. *Activity Diagram*

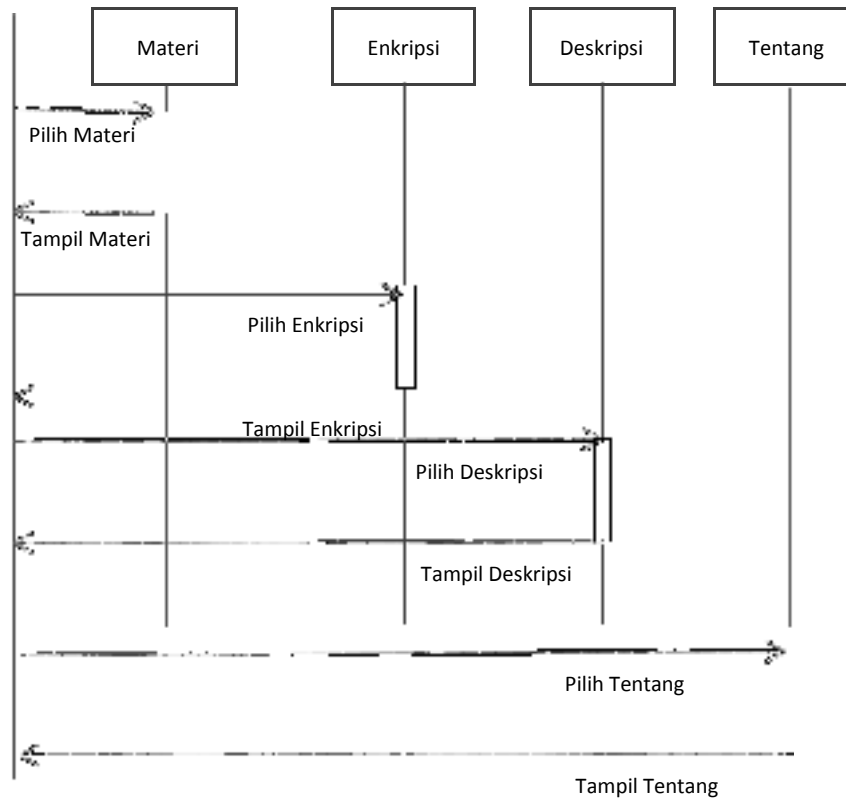
Berikut *Activity diagram* yang menggambarkan aktifitas aplikasi.



Gambar 3.4 *Activity Diagram*

Activity diagram menggambarkan aktifitas-aktifitas yang terjadi dalam aplikasi dari aktivitas dimulai sampai aktivitas berhenti.

3. Sequence Diagram



Gambar 3.5. *Sequence Diagram*

Keterangan Gambar :

1. Dalam diagram di atas menjelaskan bahwa user memilih materi kemudian Sistem menampilkan materi yang berkaitan dengan materi
2. *User merequest Enkripsi* kemudian Sistem menampilkan menu *Enkripsi*
3. *User merequest Deskripsi* kemudian Sistem menampilkan menu *Deskripsi*
4. *User merequest Menu Tentang* kemudian Sistem menampilkan *Form Tentang*.

3.9 Perancangan Antarmuka

1. Rancangan Halaman *Enkripsi*

Halaman *enkripsi* merupakan halaman yang pertama muncul pada saat program dijalankan.

Pengaturan About			
LOKASI FILE			:
Informasi File :			
Ukuran File :			
PASSWORD			
Enkripsi			

Gambar 3.6 *Rancangan Halaman Enkripsi*

Pada rancangan di atas akan menampilkan lokasi video, ukuran video, *password*, dan *enkripsi*.

2. Rancangan Halaman *Deskripsi*

Halaman *deskripsi* merupakan halaman yang muncul setelah melakukan proses *enkripsi* pada video (*MP4*).

Pengaturan About			
LOKASI FILE			:
Informasi File :			
Ukuran File :			
PASSWORD			

Deskripsi

Gambar 3.7 *Rancangan Halaman Deskripsi*

Pada rancangan di atas akan menampilkan lokasi video, ukuran video, *password*, dan *deskripsi*.

3. Rancangan Halaman Pengaturan

Form ini digunakan untuk menjelaskan cara kerja dari program, dimulai dari pemilihan file hingga proses enkripsi dan deskripsi.

Pengaturan
Keterangan: Menggunakan opsi ini akan membutuhkan Anda mempunyai sebuah USB Flashdisk yang terkoneksi ketika proses enkripsi dan dekripsi file. Peringatan : Jika opsi ini digunakan dan Anda kehilangan USB Flashdisk tersebut, maka akan tidak mungkin untuk men-dekripsi file Anda walaupun mengetahui password yang benar.

Cancel

OK

Gambar 3.8 *Rancangan Halaman Pengaturan*

BAB IV

HASIL DAN PEMBAHASAN

4.1 Pengujian Sistem

Pengujian dilakukan dengan memasukkan karakter atau huruf dari video berformat *MP4* selanjutnya diproses oleh aplikasi apakah aplikasi tersebut dapat memberikan hasil yang sesuai. Proses yang akan dilakukan pengujian dalam aplikasi ini adalah simulasi pengiriman pesan dengan menggunakan metode algoritma *RC4* antara pengirim kepada penerima dengan kunci yang dimiliki masing-masing pihak tanpa perlu bertukar kunci tunggal hingga pada akhirnya pesan asli yang dikirimkan oleh pengirim dapat dibaca oleh penerima .

4.2 Spesifikasi Sistem

Analisis kebutuhan sistem merupakan analisis yang dibutuhkan untuk menentukan spesifikasi kebutuhan sistem. Spesifikasi ini juga meliputi elemen atau komponen-komponen apa saja yang dibutuhkan untuk sistem yang akan dibangun sampai dengan sistem tersebut diimplementasikan. Analisis kebutuhan ini juga menentukan spesifikasi masukan yang diperlukan sistem, keluaran yang akan dihasilkan sistem dan proses yang dibutuhkan untuk mengolah masukan sehingga menghasilkan suatu keluaran yang diinginkan.

1. Analisis Perangkat Keras (*Hardware*)

Perangkat keras minimum yang digunakan untuk membangun Sistem Informasi

Penjualan ini adalah

- a. Processor Berkecepatan 3.0 Ghz
- b. RAM 4 Gb
- c. Hardisk minimal 10 Gb untuk menyimpan data
- d. LAN Card
- e. Keyboard dan Mouse
- f. Monitor 20 inch.

2. Analisis Perangkat Lunak (*Software*)

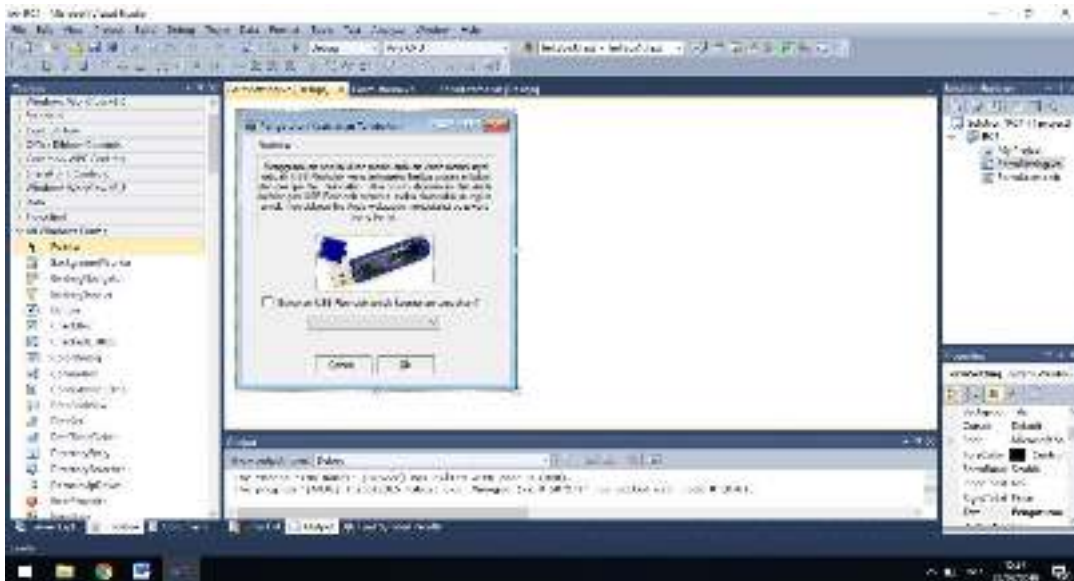
Untuk mendukung dalam penyimpanan informasi, dibutuhkan suatu fasilitas yang memadai. Yaitu berupa perangkat lunak (*software*) yang dirancang untuk memudahkan dalam pembangunan dan menjalankan sisten nantinya. Adapun perangkat lunak yang digunakan adalah sebagai berikut :

- a. Microsoft Windows 10 , Windows 10 sebagai sistem operasi
- b. Visual Studio 2010, Sebagai Perancangan Program Aplikasi.

4.3 Tampilan Aturan Penggunaan Aplikasi

1. Tampilan pengaturan program

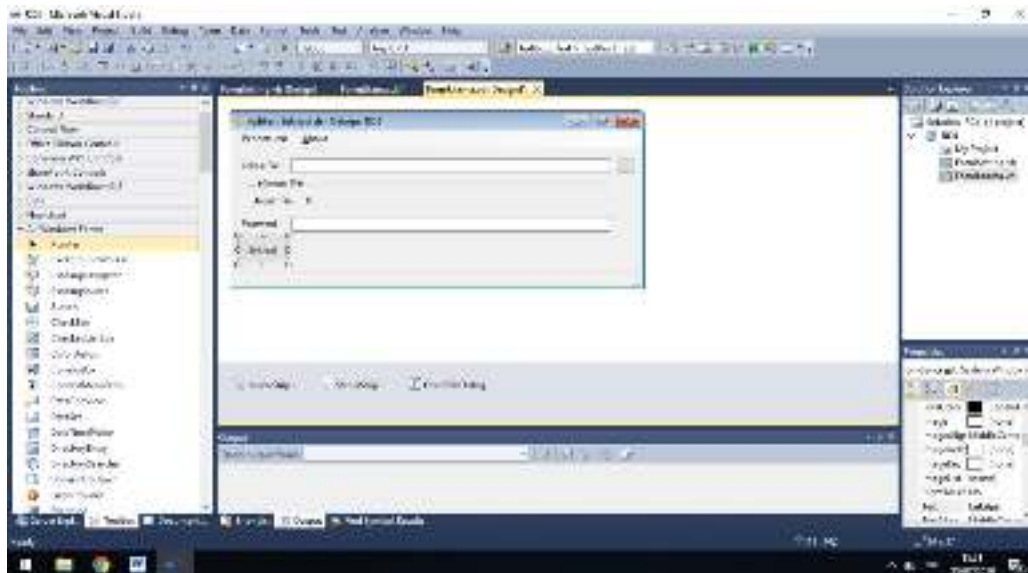
Tampilan aturan penggunaan aplikasi merupakan tampilan halaman atau form yang berisi tentang tata cara penggunaan aplikasi yang dijalankan. Pada halaman tersebut dijelaskan apa-apa saja yang menjadi kewajiban bagi pengirim dan penerima saat menjalankan simulasi algoritma *RC4*.



Gambar 4.1 Tampilan Aturan Penggunaan Aplikasi

2. Tampilan Halaman *Enkripsi* video

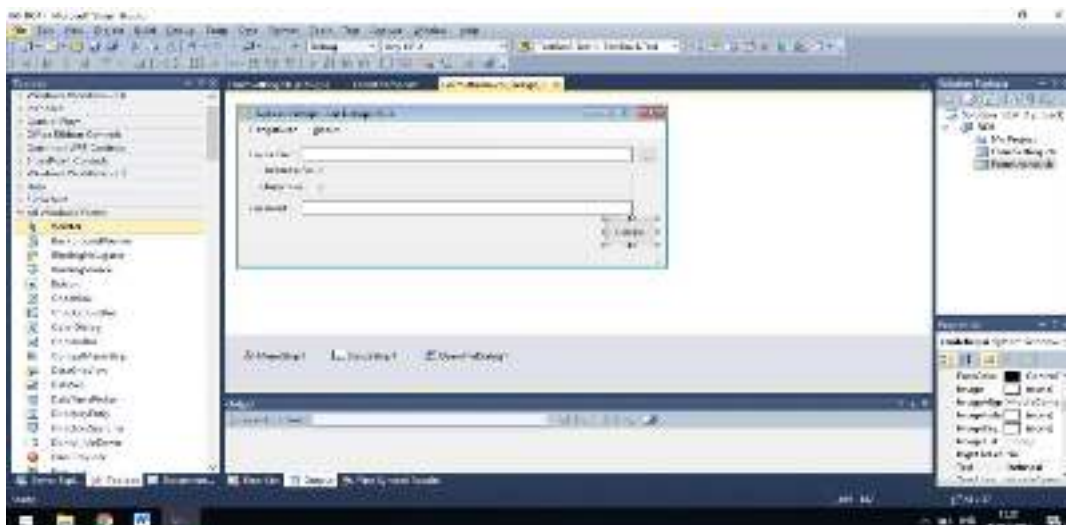
Tampilan berikut merupakan tampilan *enkripsi* pada aplikasi ini. algoritma *RC4* merupakan yang menjamin tidak adanya pertukaran kunci antara pihak-pihak yang melakukan *enkripsi* dan *dekripsi*.



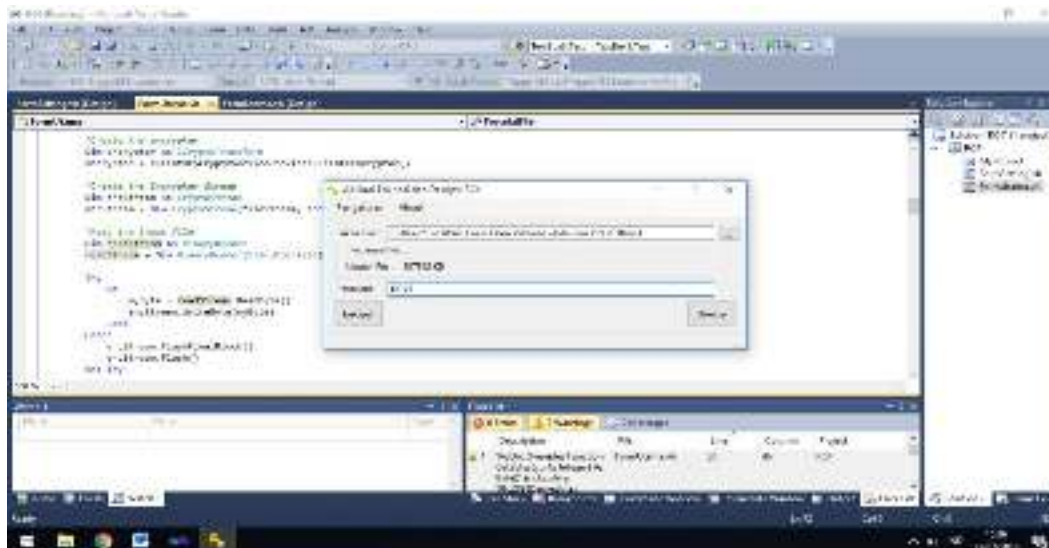
Gambar 4.2 *Tampilan Halaman Enkripsi video*

3 **Tampilan Halaman Deskripsi video**

Tampilan berikut merupakan tampilan penerima video pada aplikasi ini.



Gambar 4.3 *Tampilan Halaman Deskripsi video*



Gambar 4.5 *Tampilan Halaman Proses Deskripsi*

4.4 Kelebihan dan Kekurangan Sistem

Adapun kelebihan dan kekurangan dari media pembelajaran ini adalah sebagai berikut:

1. Kelebihan Sistem
 - a. Keamanan Pesan lebih terjamin.
 - b. Proses kemanan pesan lebih mudah dan cepat.
 - c. Proses membaca pesan lebih mudah dan cepat.
2. Kekurangan Sistem
 - a. Masih bersifat jaringan local.
 - b. Sebaiknya dapat digunakan pada Android.

BAB V

PENUTUP

5.1 Kesimpulan

Berdasarkan pembahasan dalam perancangan Pembuatan Aplikasi Kriptografi Video (*MP4*) Menggunakan Algoritma *RC4*, maka dapat diambil kesimpulan sebagai berikut :

1. Perangkat lunak ini dirancang untuk menampilkan simulasi pengiriman video berekstensi *MP4* antara pengirim dan penerima.
2. Pengirim mengirimkan video menggunakan kunci yang ditentukan sendiri oleh pengirim.
3. Penerima pesan menggunakan kunci yang diberikan oleh pengirim video, agar bisa membuka video asli yang dikirimkan oleh pengirim.

5.2 Saran

Adapun saran-saran yang dapat dilakukan penelitian atau pengembangan selanjutnya adalah sebagai berikut:

1. Diharapkan adanya kombinasi algoritma keamanan data lainnya.

2. Proses pengamanan data yang dilakukan oleh penulis masih menggunakan *Visual Studio*, diharapkan ada yang menggunakan di Android agar bisa digunakan pada mobile.

DAFTAR PUSTAKA

- Aryza, S., Irwanto, M., Lubis, Z., Siahaan, A. P. U., Rahim, R., & Furqan, M. (2018). A Novelty Design Of Minimization Of Electrical Losses In A Vector Controlled Induction Machine Drive. In IOP Conference Series: Materials Science and Engineering (Vol. 300, No. 1, p. 012067). IOP Publishing.
- Bahri, S. (2018). Metodologi Penelitian Bisnis Lengkap Dengan Teknik Pengolahan Data SPSS. Penerbit Andi (Anggota Ikapi). Percetakan Andi Offset. Yogyakarta.
- Hakim, Elka Lukman; Khairil; Utami, Ferry Hari. 2015. *APLIKASI ENKRIPSI DAN DESKRIPSI DATA MENGGUNAKAN ALGORITMA RC4 DENGAN MENGGUNAKAN BAHASA PEMROGRAMAN PHP*. Jurnal Media Infotama. Vol. 10 No.1
- Sekarsari, Galuh Adjeng; Nurhadiyono, Bowio; Dan Rahayu, Yuniarsi. 2015. *ANALISIS ALGORITMA .KRIPTOGRAFI RC PADA ENKRIPSI CITRA DIGITAL*. Techno.COM. Vol. 14, No. 4. 250-251. Diakses dari dinus.ac.id
- Fachri, B. (2018, September). APLIKASI PERBAIKAN CITRA EFEK NOISE SALT & PAPPER MENGGUNAKAN METODE CONTRAHARMONIC MEAN FILTER. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 87-92).
- Fachri, B. (2018). Perancangan Sistem Informasi Iklan Produk Halal Mui Berbasis Mobile Web Menggunakan Multimedia Interaktif. Jurasik (Jurnal Riset Sistem Informasi dan Teknik Informatika), 3, 98-102.
- Fernando, Frenky; Siswanto; Dan Suryana, Eko. 2016. *APLIKASI KRIPTOGRAFI UNTUK MENGAMANKAN FILE AUDIO VIDEO MENGGUNAKAN VISUAL BASIC .NET*. Jurnal Media Infotama, Vol. 10 No.1, 27-34. Tanggal akses 1 Februari 2016.
- Fitriani, W., Rahim, R., Oktaviana, B., & Siahaan, A. P. U. (2017). Vernam Encrypted Text in End of File Hiding Steganography Technique. Int. J. Recent Trends Eng. Res, 3(7), 214-219.
- Ginting, G., Fadlina, M., Siahaan, A. P. U., & Rahim, R. (2017). Technical approach of TOPSIS in decision making. Int. J. Recent Trends Eng. Res, 3(8), 58-64.
- Kurniawan, H. (2018). Pengenalan Struktur Baru untuk Web Mining dan Personalisasi Halaman Web. Jurnal Teknik dan Informatika, 5(2), 13-19.

- Rahim, R. (2018, October). A Novelty Once Methode Power System Policies Based On SCS (Solar Cell System). In International Conference of ASEAN Prespective and Policy (ICAP) (Vol. 1, No. 1, pp. 195-198).
- Ramadhan, Z., Zarlis, M., Efendi, S., & Siahaan, A. P. U. (2018). Perbandingan Algoritma Prim dengan Algoritma Floyd-Warshall dalam Menentukan Rute Terpendek (Shortest Path Problem). JURIKOM (Jurnal Riset Komputer), 5(2), 135-139.
- Sihotang, Hengki Tamando. 2018. *PERANCANGAN DAN IMPLEMENTASI ALGORITMA ARITHMETIC CODING UNTUK APLIKASI KOMPRESI DATA VIDEO DAN AUDIO*. Jurnal Teknik Informatika. Volume 2, No. 1, 58-64, diakses Juni 2018
- Suherman, S., & Khairul, K. (2018). Seleksi Pegawai Kontrak Menjadi Pegawai Tetap Dengan Metode Profile Matching. IT Journal Research and Development, 2(2), 68-77.
- Kirman. 2018. *IMPLEMENTASI ALGORITMA RC4 UNTUK PROTEKSI FILE MP3*. Jurnal Pseudocode, Volume V Nomor 1, 80-86. Diakses Februari 2018
- Mayasari, Nova. "Comparison of Support Vector Machine and Decision Tree in Predicting On-Time Graduation (Case Study: Universitas Pembangunan Panca Budi)." Int. J. Recent Trends Eng. Res 2.12 (2016): 140-151.
- Pemrograman. Wikipedia. Web. 12 Februari 2018. <https://id.wikipedia.org/wiki/Pemrograman>
- Tarigan, A. D., & Pulungan, R. (2018). Pengaruh Pemakaian Beban Tidak Seimbang Terhadap Umur Peralatan Listrik. RELE (Rekayasa Elektrikal dan Energi): Jurnal Teknik Elektro, 1(1), 10-15.
- Tarigan, A. D. (2018, October). A Novelty Method Subjectif of Electrical Power Cable Retirement Policy. In International Conference of ASEAN Prespective and Policy (ICAP) (Vol. 1, No. 1, pp. 183-186).
- Wahyuni, S., Lubis, A., Batubara, S., & Siregar, I. K. (2018, September). IMPLEMENTASI ALGORITMA CRC 32 DALAM MENGIDENTIFIKASI KEASLIAN FILE. In Seminar Nasional Royal (SENAR) (Vol. 1, No. 1, pp. 1-6).
- Wibowo, P., Lubis, S. A., & Hamdani, Z. T. (2017). Smart Home Security System Design Sensor Based on Pir and Microcontroller. International Journal of Global Sustainability, 1(1), 67-73.