ALGORITMA: Jurnal Ilmu Komputer dan Informatika
Volume: 01, Number : 01, November 2017 ISSN 2598-6341 (online)

RANCANG BANGUN APLIKASI PENGAMAN ISI FILE DOKUMEN DENGAN ALGORITMA RSA

Rakhmat Kurniawan

Program Studi Ilmu Komputer
Fakultas Sains dan Teknologi
Universitas Islam Negeri Sumatera Utara Medan
Email: rakhmat.kr@uinsu.ac.id

Abstrak

Keamanan dokumen merupakan salah satu hal yang sangat penting dalam penukaran data, khusunya pertukaran data didunia maya yang didalamnya terdapat banyak ancaman pada saat proses itu dilakukan. Keamanan data, khususnya untuk dokumen teks bagi suatu organisasi yang mengasumsikan bahwa dokumen tersebut bernilai rahasia (*private and confidential)*. Salah satu aspek keamanan dalam dokumen teks adalah keaslian, bentuk dan isinya harus sesuai dengan yang dimaksud oleh pembuat. Hingga saat ini sistem kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu data yaitu dengan menyandikan isi atau *content file* dokumen tersebut menjadi isi yang sulit bahkan tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli dilakukan, proses dekripsi disertai dengan menggunakan kunci yang benar. Salah satu metode yang sangat popular didalam kriptografi adalah RSA, dimana sampai saat ini metode ini sangat sulit untuk dipecahkan dan akan membutuhkan waktu yang sangat lama. Metode ini menggunakan 2 (dua) kunci, yaitu *public key* dan *private key.* Dimana panjang kunci dapat ditentukan dan disesuaikan dengan tingkat kemanan yang diinginkan.
Kata kunci: *keamanan data, RSA, kriptografi*

Abstract

Document security is one of the most important things in the exchange of data, especially the exchange of data in the virtual world in which there are many threats when the process is done. Data security, especially for text documents for an organization that assumes that the document is confidential (private and confidential). One aspect of security in a text document is its authenticity, form and contents must be in accordance with the intended by the author. Until now the cryptographic system is one solution to ensure the security of a data that is by encode the contents or content file the document becomes difficult content not even understood through the process of encryption and to recover the original information is done, the decryption process is accompanied by using the key correct. One of the most popular methods in cryptography is RSA, which to this day is very difficult to solve and will take a very long time. This method uses 2 (two) keys, namely public key and private key. Where the key length can be determined and adjusted to the desired level of security.
Keywords: *data security, RSA, cryptography*

1. PENDAHULUAN

Saat ini sistem komputer yang terpasang makin mudah diakses. Sistem *time sharing* dan akses jarak jauh menyebabkan masalah keamanan menjadi salah satu kelemahan komuniksi data seperti internet. Disamping itu kecendrungan lain saat ini adalah memberikan tanggung jawab sepenuhnya kepada komputer untuk mengelola aktifitas pribadi dan bisnis seperti sistem transfer dana elekronis yang melewatkan uang sebagai aliran bit dan lain sebagainya. Untuk itu diperlukan sistem komputer yang memiliki tingkat keamanan yang dapat terjamin, demikian pula dengan keamanan data.

Keamanan dokumen merupakan salah satu hal yang sangat penting dalam penukaran data, khusunya pertukaran data didunia maya yang didalamnya terdapat banyak ancaman pada saat proses itu dilakukan. Keamanan data, khususnya untuk dokumen teks bagi suatu organisasi yang mengasumsikan bahwa dokumen tersebut bernilai rahasia (*private and confidential)*. Salah satu aspek keamanan dalam dokumen teks adalah keaslian, bentuk dan isinya harus sesuai dengan yang dimaksud oleh pembuat.

Hingga saat ini sistem kriptografi merupakan salah satu solusi untuk menjamin keamanan dari suatu data yaitu dengan menyandikan isi atau *content file* dokumen tersebut menjadi isi yang sulit bahkan tidak dipahami melalui proses enkripsi dan untuk memperoleh kembali informasi yang asli dilakukan, proses dekripsi disertai dengan menggunakan kunci yang benar.

Salah satu metode yang sangat popular didalam kriptografi adalah RSA, dimana sampai saat ini metode ini sangat sulit untuk dipecahkan dan akan membutuhkan waktu yang sangat lama. Metode ini menggunakan 2 (dua) kunci, yaitu *public key* dan *private key.* Dimana panjang kunci

dapat ditentukan dan disesuaikan dengan tingkat kemanan yang diinginkan.

2. LANDASAN TEORI

2.1. Kriptografi

Salah satu sarana komunikasi manusia adalah tulisan. Sebuah tulisan berfungsi untuk menyampaikan pesan kepada pembacanya. Pesan itu sendiri merupakan suatu informasi yang dapat dibaca dan dimengerti maknanya. Sebelum ditemukan media untuk mendokumentasikan suatu informasi, pengiriman informasi dari satu tempat ke tempat yang lain sudah terjadi. Dengan berkembangnya cara pengiriman pesan, berkembang pula cara menyembunyikan pesan dan bagaimana agar orang lain tidak mengetahui isi pesan walau pesan tersebut ditemukan. Disinilah lahir suatu ilmu baru disebut dengan kriptografi (Al Azad 2012).

2.1.1. Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani yaitu *crypto* dan *graphia*. Crypto berarti *secret* atau rahasia dan graphia berarti *writing* atau tulisan. Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain (Al Azad 2012). Definisi lain kriprografi adalah ilmu dan seni untuk menjaga kerahasian pesan dengan cara menyandikan ke dalam bentuk yang tidak dapat dimengerti lagi maknanya (Munir 2006).

Definisi terminologi algoritma adalah urutan langkah-langkah logis untuk menyelesaikan masalah yang disusun secara sistematis. Algoritma kriptografi merupakan langkah-langkah logis bagaimana menyembunyikan pesan dari orang-orang yang tidak berhak atas pesan tersebut (Al Azad 2012).

2.1.2. Masalah dan Ancaman Keamanan

Masalah keamanan merupakan salah satu aspek terpenting dari sebuah sistem informasi. Masalah keamanan sering kurang mendapatkan perhatian dari para perancang dan pengelola sistem informasi. Hampir setiap aspek masyarakat menggunakan sistem informasi yang berbasis komputer ditambah dengan kemudahan yang didapat melalui jaringan komputer seperti *Local Area Network* (LAN) dan internet yang telah menyediakan informasi cepat dan akurat.

Terjadinya banyak pertukaran informasi setiap detiknya di internet serta tindakan atau ancaman kejahatan atas informasi tertentu oleh pihak-pihak yang tidak bertanggung jawab. Ancaman keamanan yang terjadi terhadap informasi adalah:

1. *Interruption*
   Interupsi merupakan ancaman terhadap *availability* informasi, data yang ada dalam sistem komputer dirusak atau dihapus sehingga jika data atau informasi tersebut dibutuhkan maka pemiliknya akan mengalami kesulitan untuk mengaksesnya, bahkan mungkin informasi itu hilang.
2. *Interception*
   Intersepsi merupakan ancaman terhadap kerahasiaan. Informasi disadap sehingga orang yang tidak berhak dapat mengakses computer di mana informasi tersebut disimpan.
3. *Modification*
   Modifikasi merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil menyadap lalu lintas informasi yang sedang dikirim dan kemudian mengubahnya sesuai keinginan orang tersebut.
4. *Fabrication*
   Pemalsuan merupakan ancaman terhadap integritas. Orang yang tidak berhak berhasil meniru atau memalsukan informasi sehingga orang yang menerima informasi tersebut menyangka bahwa informasi tersebut berasal dari orang yang dikehendaki oleh penerima informasi.

2.1.3. Tujuan Kriptografi

Salah satu peran utama kriptografi adalah mengamankan data atau dokumen dengan menggunakan teknik enkripsi terhadap data atau dokumen itu sehingga tidak bisa dibaca. Keamanan komputer meliputi beberapa aspek antara lain:

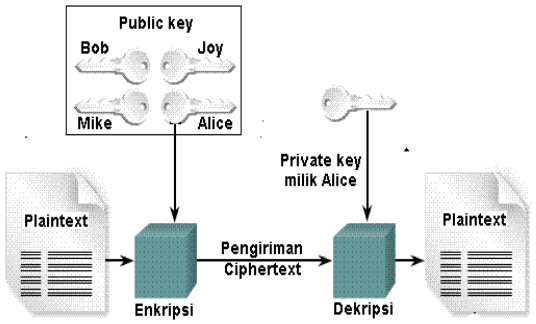
1. *Authentication*
   Penerima informasi dapat memastikan keaslian pengirim informasi. Dengan kata lain, informasi itu benar-benar dating dari orang yang dikehendaki.
2. *Integrity*
   Keaslian pesan yang dikirimkan melalui jaringan dan dapat dipastikan bahwa informasi yang dikirim tidak dimodifikasi oleh orang yang tidak berhak.
3. *Nonrepudiation*
   Hal yang berhubungan dengan pengirim. Pengirim tidak dapat mengelak bahwa telah mengirim informasi tersebut.
4. *Authority*
   Informasi yang berada pada sistem jaringan tidak dapat dimodifikasi oleh pihak yang tidak berhak untuk mengaksesnya.
5. *Confidentiality*
   Suatu usaha untuk menjaga informasi dari orang yang tidak berhak mengakses. Kerahasiaan ini biasanya berhubungan dengan informasi yang diberikan ke pihak lain.
6. *Privacy*
   Informasi yang lebih menuju ke arah data yang bersifat pribadi tidak dapat hak mengakses.
7. *Availability*
   Aspek availabilitas berhubungan dengan ketersediaan informasi ketika dibutuhkan. Sistem informasi yang diserang dapat menghambat atau meniadakan akses ke informasi.

8. *Access Control*

Aspek ini berhubungan dengan cara pengaturan akses ke informasi. Hal ini biasanya berhubungan dengan masalah otentikasi dan privasi. Kontrol akses sering dilakukan dengan menggunakan kombinasi *user id* dan *password* ataupun dengan mekanisme lain.

2.2. Algoritma RSA

Algoritma RSA dibuat oleh 3 (tiga) orang peneliti dari MIT (Massachusset Institute of Technology) pada tahun 1976 yaitu Ron Riverst, Adi Shamir, dan Leonard Adleman. Algoritma RSA juga merupakan kriptografi kunci umum yang paling popular dikarenakan algoritma ini melakukan pemfaktoran bilangan yang sangat besar sehingga dianggap paling aman (Al Azad 2012).



Sumber: (Beny 2012)

Gambar 2.1 Proses Enkripsi dan Dekripsi RSA

Untuk melakukan enkripsi dan dekripsi menggunakan algoritma RSA harus memenuhi langkah-langkah berikut yaitu:

1. p dan q merupakan bilangan prima. Hasil n = p.q
2. Hitung nilai $\Phi(n) = (p-1)(q-1)$,
3. Nilai e merupakan kunci umum untuk enkripsi. Nilai e harus relatif prima terhadap $\Phi(n)$,
4. Nilai d merupakan kunci rahasia untuk dekripsi. Nilai d didapatkan dengan persamaan invers e mod n atau $e.d = 1 + k.\Phi(n)$.

Algoritma RSA didasarkan pada teorema Euler yang menyatakan bahwa nilai $a^{\Phi(n)} \equiv 1 \pmod n$ yang dalam hal ini:

1. a harus relatif prima terhadap r atau gcd(a,n) = 1.
2. $\Phi(n) = n(1-1/p1)(1-1/p2) \ldots (1-1/pn)$, yang dalam hal ini p1, p2, …, pn adalah factor prima dari n. $\Phi(n)$ adalah fungsi yang menentukan berapa banyak bilangan 1, 2, 3, …, n yang relatif prima terhadap n.

Berdasarkan persamaan $(Xe)d \equiv X \pmod r$ maka enkripsi dan dekripsi dirumuskan sebagai berikut:

1. $Ee(X) = Y \equiv Xe \pmod n$ untuk enkripsi,
2. $Dd(Y) = X \equiv Yd \pmod n$ untuk dekripsi.

Misalkan Childva mengirim pesan "HELLO WORLD" kepada Chitra dengan nilai numerik pesan adalah 07 04 11 11 14 26 22 14 17 11 03. Kemudian Childva memilih kunci umum e = 17 dan pasangan kunci rahasia d = 53. Childva melakukan enkripsi dengan kunci umum untuk menghasilkan *ciphertext*. Kemudian Chitra melakukan dekripsi dengan kunci rahasia untuk menghasilkan *plaintext*. Sebagai ilustrasi dapat dilihat pada Tabel 2.1.

Tabel 2.1 Ilustrasi dari Algoritma RSA

Enkripsi				Dekripsi			
Teks Asli (X)	Desimal (X)	Y=Xe (Mod n)	Teks Kode (Y)	Teks Kode (Y)	Y=Xe (Mod n)	Desimal (X)	Teks Kode (X)
H	7	$7^{17} \bmod 77$	28	28	$28^{17} \bmod 77$	7	H
E	4	$4^{17} \bmod 77$	16	16	$16^{17} \bmod 77$	4	E
L	11	$11^{17} \bmod 77$	14	14	$14^{17} \bmod 77$	11	L
L	11	$11^{17} \bmod 77$	14	14	$14^{17} \bmod 77$	11	L
O	14	$14^{17} \bmod 77$	42	42	$42^{17} \bmod 77$	14	O
	26	$26^{17} \bmod 77$	38	38	$38^{17} \bmod 77$	26	
W	22	$22^{17} \bmod 77$	22	22	$22^{17} \bmod 77$	22	W
O	14	$14^{17} \bmod 77$	42	42	$42^{17} \bmod 77$	14	O
R	17	$17^{17} \bmod 77$	19	19	$19^{17} \bmod 77$	17	R
L	11	$11^{17} \bmod 77$	44	44	$44^{17} \bmod 77$	11	L
D	13	$13^{17} \bmod 77$	75	75	$75^{17} \bmod 77$	13	D

2.3. Dokumen Digital

Dokumen merupakan suatu sarana transformasi informasi dari satu orang ke orang lain atau dari suatu kelompok ke kelompok lain. Dokumen meliputi berbagai kegiatan yang diawali dengan bagaimana suatu dokumen dibuat, dikendalikan, diproduksi, disimpan, didistribusikan, dan digandakan. Dokumen sangat penting, baik dalam kehidupan sehari-hari, organisasi, maupun bisnis.

Dokumen digital merupakan setiap informasi elektronik yang dibuat, diteruskan, dikirimkan, diterima, atau disimpan dalam bentuk analog, digital, elektromagnetik, optikal, atau sejenisnya, yang dapat dilihat, ditampilkan dan/atau didengar melalui komputer atau sistem elektronik, termasuk tetapi tidak terbatas pada tulisan, suara atau gambar, peta, rancangan, foto atau sejenisnya, huruf, tanda, angka, kode akses, simbol atau perforasi yang memiliki makna atau arti atau dapat dipahami oleh orang yang mampu memahaminya.

Dokumen digital dapat dihasilkan dengan menggunakan aplikasi pengolah kata (*word processor*) seperti *Microsoft Word*, *Notepad* atau *OpenOffice* untuk menghasilkan sebuah berkas komputer dengan ekstension yang berbeda-beda

sesuai dengan aplikasi pengolah kata yang digunakan. (Harahap 2010).

2.3.1. Pengolahan Dokumen Digital

Untuk mengolah suatu dokumen digital, dibutuhkan perangkat lunak (*software*) khusus yang sering disebut dengan perangkat lunak pengolah kata (*Word Processor*). Perangkat lunak pengolah kata adalah suatu aplikasi komputer yang digunakan untuk menyusun, menyunting, memformat dan mencetak segala jenis bahan yang dapat dicetak. Adapun contoh dari perangkat lunak pengolah kata yang sering digunakan adalah *Microsoft Word*, *OpenOffice.org Writer*, *Adobe Acrobat* dan *Foxit PDF Creator*.

1. *Microsoft Word*

Microsoft Word atau sering disebut dengan *Microsoft Office Word* adalah perangkat lunak pengolah kata (*word processor*) yang diproduksi oleh Microsoft. Perangkat lunak ini pertama diterbitkan pada tahun 1983 dengan nama *Multi-Tool Word* untuk *Xenix*. Seiring dengan perkembangan zaman, versi-versi lain kemudian dikembangkan untuk berbagai sistem operasi, misalnya DOS (1983), Apple *Macintosh* (1984), SCO UNIX, OS/2, dan *Microsoft Windows* (1989). Perangkat lunak ini kemudian berubah nama menjadi *Microsoft Office Word* setelah menjadi bagian dari *Microsoft Office* System 2003 dan 2007.

Konsep yang digunakan oleh *Microsoft Office Word* adalah WYSIWYG (*What You See Is What You Get*). WYSIWYG merupakan sebuah konsep sistem dimana konten yang sedang disunting akan terlihat sama persis dengan hasil keluaran akhir, yang mungkin berupa dokumen yang dicetak, halaman web, *slide* presentasi, atau bahkan sebuah animasi bergerak.

Microsoft Office Word merupakan perangkat lunak pengolah kata pertama yang mampu menampilkan tulisan cetak miring atau cetak tebal pada IBM PC sementara perangkat lunak pengolah kata lain hanya menampilkan teks dengan kode *markup* dan warna untuk menandai pemformatan cetak tebal atau miring.

2. *OpenOffice.org Writer*

OpenOffice.org Writer adalah salah satu komponen dalam OpenOffice.org yang berfungsi untuk mengedit dokumen adapun dokumen format yang bisa digunakan adalah .doc .odt .rtf dan dapat dikonversi dalam bentuk .pdf dengan sekali klik.

OpenOffice.org Writer memiliki fitur pengolah kata modern seperti *AutoCorrect*, *AutoComplete*, *AutoFormat*, *Styles and Formatting*, *Text Frames*, *Linking*, *Tables of Contents*, *Indexing*, *Bibliographical References*, *Illustrations* dan *Tables*.

Perangkat lunak ini sangat mudah digunakan untuk membuat memo cepat, sangat stabil dan mampu untuk membuat dokumen dengan banyak halaman serta banyak gambar dan judul heading. Selain itu, kelebihannya adalah pengaturan formating untuk *bullet* and *number* yang sangat mudah (diatur terintegrasi melalui satu *toolbar*).

3. *Foxit PDF Creator*

Foxit PDF Creator merupakan sebuah perangkat lunak pengolah kata yang cepat dan mudah dalam membuat dokumen digital dengan format PDF dan mampu mengubah dokumen digital dengan format DOC, XLS, PPT, TXT, E-MAIL atau HTML ke format PDF.

Foxit PDF Creator menyediakan cara cepat dan dapat diandalkan untuk membuat dokumen PDF sehingga membantu penggunanya untuk menghasilkan *file* PDF yang akurat dalam waktu yang singkat dengan tetap mempertahankan tata letak asli dokumen digital yang dikonversi.

Dengan kemampuan pencarian yang kuat dan kinerjanya yang tinggi, *Foxit PDF Creator* mampu menampilkan dan mengolah PDF dalam ukuran yang kecil, dalam waktu yang cepat dan tingkat akurasi yang tinggi menjadi format yang diinginkan pengguna.

4. *Adobe Acrobat*

Adobe Acrobat merupakan sebuah perangkat lunak pengolah kata yang dapat mengkonversi suatu dokumen digital menjadi sebuah *file* dalam format PDF. Dokumen digital yang dihasilkan oleh *adobe acrobat* dapat ditampilkan pada sebuah *web browser* dengan tampilan dan isi yang sama dengan dokumen aslinya. *Adobe Acrobat* menyediakan *tools* keamanan untuk membatasi akses terhadap *file* hasil konversi, misalnya mencegah orang lain untuk melakukan pencetakan atau pengubahan terhadap dokumen digital. *Adobe Acrobat* berbeda dengan *Acrobat Reader*, dimana *adobe reader* hanya dapat membaca *file* PDF tanpa dapat mengkoversi suatu *file* ke format PDF.

3. ANALISA DAN PERANCANGAN

3.1 Analisis Permasalahan

Pembahasan masalah yang terdapat pada bab ini adalah penelusuran secara manual penggunaan algoritma RSA pada enkripsi *file content*. Untuk dapat menerapkan algoritma RSA, terlebih dahulu dilakukan pembangkitan kunci. Kunci yang dibangkitkan adalah pasangan kunci *private* dan kunci *public*. Kunci *public* digunakan untuk melakukan enkripsi, sedangkan kunci *private* digunakan untuk dekripsi.

3.2 Analisis Algoritma

Untuk menganalisis algoritma yang digunakan, akan dilakukan dengan membuat suatu skenario sebagai berikut:

Edi akan mengirimkan sebuah *file* dokumen rahasia terenkripsi dengan algoritma RSA kepada Ani. Untuk menyelesaikan skenario ini berikut adalah tahapannya.

1. Pembangkitan kunci

   Untuk membangkitkan kunci, Edi sebagai pengirim akan membangkitakn bilangan acak

integerp dan *q*. Kemudian Edi juga memilih satu bilangan acak prima sebagai *public key e*. Dalam skenario ini Edi memilih bilangan *p = 13*, *q = 23*. Setelah memilih bilangan prima acak, Edi akan melakukan perhitungan terhadap bilangan-bilangan tersebut.

$p = 13, q = 23$

$n = p \times q$

$n = 13 \times 23$

$n = 299$

$\Phi(n) = (p-1)(q-1)$

$\Phi(n) = p \cdot q - p - q + 1$

$\Phi(n) = 13 \cdot 23 - 13 - 23 + 1$

$\Phi(n) = 299 - 13 - 23 + 1$

$\Phi(n) = 264$

Memilih nilai prima acak *e* sebagai *public key*, dimana *e* relatif prima terhadap $\Phi(n)$, dimana *e* tidak bisa membagi rata nilai $\Phi(n)$. Nilai *e* dapat dipilih secara acak dengan syarat $1 < e < \Phi(n)$.

$e = 5$

Selanjutnya Edi menghitung nilai *d* dengan menggunakan *Euclidian* yang diperluas.

$(d \times e) \, mod \, \Phi(n) = 1$

$(d \times 5) \, mod \, 264 = 1$

$d = 53$

Dari perhitungan diatas diperoleh *public key* dan *private key*.

$Public\ Key = \{e, n\} = \{5, 299\}$

$Private\ Key = \{d, n\} = \{53, 299\}$

2. Enkripsi

Setelah mendapatkan pasangan kunci, Edi dapat melakukan enkripsi terhadap blok*file content* yang akan dikirim. Blok *file content* yang akan dienkripsi akan asumsikan seperti ilustrasi dibawah ini.

```
50 4B 03 04 14 0006 00
08 00 00 00 21 00 DF A4
```

Blok *file content* yang akan dienkrip berupa sekumpulan *byte* data, dimana tiap *byte* data tersebut akan dienkripsi sehingga dapat menyembunyikan isi aslinya. Untuk melakukan enkripsi terhadap *file content*akan dilakukan perhitungan secara berikut:

a. Konversi nilai *byte* kedalam bentuk decimal

Byte I:

$50_{(hex)} = 80_{(dec)}$

50	5	5×16^1	80
	0	0×16^0	0
			80

Byte II:

$50_{(hex)} = 80_{(dec)}$

4B	4	4×16^1	64
	B	11×16^0	11
			75

Hasil konversi keseluruhan disajikan pada Tabel 3.1 dibawah ini.

Tabel 3.1 Hasil Konversi *Byte* Kedalam Bentuk Desimal

Hexa	Desimal
50	80
4B	75
03	3
04	4
14	20
00	0
06	6
00	0
08	8
00	0
00	0
00	0
21	33
00	0
DF	223
A4	164

b. Perhitungan nilai desimal menjadi *ciphertext*

Perhitungan untuk mendapat *ciphertext* dapat dilakukan dengan menggunakan persamaan berikut:

$C = m^e \, Mod \, n$

Iterasi I:

$m = 80$

$C = 80^5 \, Mod \, 299$

$C = 97$

Iterasi II:

$m = 75$

$C = 75^5 \, Mod \, 299$

$C = 186$

Hasil perhitungan selengkapnya disajikan pada Tabel 3.2 dibawah ini.

Tabel 3.2 Perhitungan Enkripsi

Plaintext	Enkripsi	Ciphertext
80	$C = 80^5 \, Mod \, 299$	97
75	$C = 75^5 \, Mod \, 299$	186
3	$C = 3^5 \, Mod \, 299$	243
4	$C = 4^5 \, Mod \, 299$	127
20	$C = 20^5 \, Mod \, 299$	102
0	$C = 0^5 \, Mod \, 299$	0
6	$C = 6^5 \, Mod \, 299$	2

0	$C = 0^5 \ Mod \ 299$	0
8	$C = 8^5 \ Mod \ 299$	177
0	$C = 0^5 \ Mod \ 299$	0
0	$C = 0^5 \ Mod \ 299$	0
0	$C = 0^5 \ Mod \ 299$	0
33	$C = 33^5 \ Mod \ 299$	180
0	$C = 0^5 \ Mod \ 299$	0
223	$C = 223^5 \ Mod \ 299$	6
164	$C = 164^5 \ Mod \ 299$	151

3. Dekripsi
   Setelah Ani menerima *file* terenkrip dari Edi, selanjutnya Ani akan melakukan dekripsi terhadap *file* tersebut. Dekripsi dilakukan dengan cara sebagai berikut:

$$Private\ Key = \{d, n\} = \{53, 299\}$$

Iterasi I:

$$C = 97$$
$$M = C^d \ Mod \ N$$
$$M = 97^{53} \ Mod \ 299$$
$$M = 80$$

Iterasi II:

$$C = 186$$
$$M = C^d \ Mod \ N$$
$$M = 186^{53} \ Mod \ 299$$
$$M = 75$$

Hasil perhitungan dekripsi selengkapnya disajikan pada Tabel 3.3 dibawah ini.

Tabel 3.3 Hasil Perhitungan Dekripsi

Ciphertext	Enkripsi	Plaintext
97	$M = 97^{53} \ Mod \ 299$	80
186	$M = 186^{53} \ Mod \ 299$	75
243	$M = 243^{53} \ Mod \ 299$	3
127	$M = 127^{53} \ Mod \ 299$	4
102	$M = 102^{53} \ Mod \ 299$	20
0	$M = 0^{53} \ Mod \ 299$	0
2	$M = 2^{53} \ Mod \ 299$	6
0	$M = 2^{53} \ Mod \ 299$	0
177	$M = 177^{53} \ Mod \ 299$	8
0	$M = 0^{53} \ Mod \ 299$	0
0	$M = 0^{53} \ Mod \ 299$	0
0	$M = 0^{53} \ Mod \ 299$	0
180	$M = 180^{53} \ Mod \ 299$	33
0	$M = 07^{53} \ Mod \ 299$	0
6	$M = 6^{53} \ Mod \ 299$	223
151	$M = 151^{53} \ Mod \ 299$	164

Setelah mendapatkan plaintext dalam bentuk desimal, tahap berikutnya adalah melakukan konversi nilai desimal kedalam bentuk *byte*.

Iterasi I:

$$80_{(dec)} = 50_{(hex)}$$
$$80 \ Mod \ 16 = 0$$
$$80 \backslash 16 = 5$$

Iterasi II:

$$186_{(dec)} = 75_{(hex)}$$
$$80 \ Mod \ 16 = 5$$
$$186 \backslash 16 = 7$$

Hasil konversi selengkapnya disajikan pada Tabel 3.4 dibawah ini.

Tabel 3.4 Konversi *Plaintext* Desimal Ke *Byte*

Desimal	Byte
80	50
75	4B
3	03
4	04
20	14
0	00
6	06
0	00
8	08
0	00
0	00
0	00
33	21
0	00
223	DF
164	A4

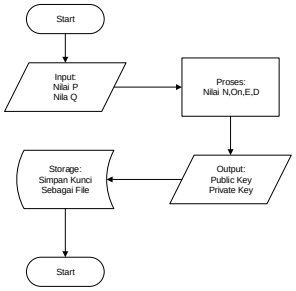
3.3 *Flowchart Program*

Untuk menggambarkan aliran data pada algoritma yang akan diterapkan pada aplikasi yang akan dibangun, digunakan sebuah diagram yang disebut dengan *flowchart*. Diagram ini akan memberikan gambaran aliran data dari setiap *input*, proses, maupun *output*. Dalam pembahasan ini, ada 3 (tiga) *flowchart* yang akan disajikan, yaitu:

1. *Flowchart* pembangkitan kunci
2. *Flowchart* enkripsi
3. *Flowchart* dekripsi

3.3.1 *Flowchart* Pembangkitan Kunci

Pada *flowchart* ini akan menggambarkan proses pembentukan *public key* dan *private key*. Gambar 3.1 merupakan *flowchart* pembangkitan kunci.



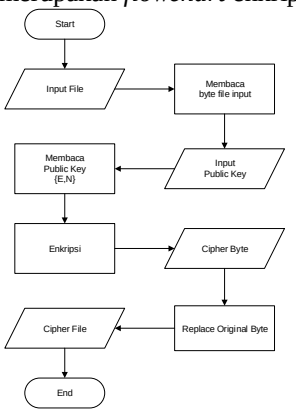
Gambar 3.1 *Flowchart* Pembangkitan Kunci

Keterangan:

Untuk membangkitkan kunci, diperlukan 2 (dua) bilangan prima acak yang bernilai besar *P* dan *Q*. Kedua bilangan ini selanjutnya diproses sehingga menghasilkan *public key* dan *private key*. Hasil pembangkitan kunci ini akan disimpan dalam bentuk *file*. Dimana pada proses enkripsi dan dekripsi, akan memerlukan input berupa *file* kunci yang telah dibuat.

3.3.2 *Flowchart* Enkripsi

Pada *flowchart* ini akan menggambarkan proses pembentukan enkripsi dari *plaintext*. Gambar 3.2 merupakan *flowchart* enkripsi.



Gambar 3.2 *Flowchart* Enkripsi

DAFTAR PUSTAKA

Al Azad, Aqib. 2012. "Efficient VLSI Implementation of DES and Triple DES Algorithm with Cipher Block Chaining concept using Verilog and FPGA." *International Journal of Computer Applications (0975-8887)* 1-10.

Ariyus, Donny. 2009. *Keamanan Multimedia.* Yogyakarta: Andi Offset.

Beny. 2012. *Analisis Dan Perancangan Sistem Kriptografi Simetris Triple DES Dan Kriptografi Asimetris RSA.* Medan: Univesitas Sumatra Utara.

Cox, Ingemar, Matthew Miller, Jeffrey Bloom, Jessica Fidrich, and Ton Kalker. 2008. *Digital Watermarking and Steganography, 2nd Ed. (The Morgan Kaufmann Series in Multimedia Information and Systems).* Burlington: Morgan Kaufman.

Harahap, Putri Hartati. 2010. *Teknik Pendeteksian Kerusakan File Dokumen Dengan Metode Cyclic Redundancy Check 32 (CRC32).* Medan: Universitas Sumatra Utara.

Kekre, H B, Archana Athawale, and Pallavi N Halarnkar. 2008. "Increased Capacity of Information Hiding in LSB's Method for Text and Image." *International Journal of Electrical, Computer & Systems Engineering* 246-249.

Kipper, Gregory. 2004. *Investigator's Guide To Steganography.* Auerbach: CRL Press LLC.

Lestriandoko, Nova Hadi. 2006. "Pengacakan Pola Steganografi Untuk Meningkatkan Keamanan Penyembunyian Data Digita." *Seminar Nasional Aplikasi Teknologi Informasi 2006.*

Munir, Rinaldi. 2006. *Kriptografi.* Bandung: Informatika.

Suharja, Marchel Yan. 2009. *Perancangan Program Aplikasi Audio Steganografi Dengan Menggunakan Metode Kriptografi Rijndael Advanced Encryption Standard.* Jakarta: Universitas Bina Nusantara.

Tanenbaum, Andrew S, and Todd Austin. 2012. *Structured Computer Organization 6th Edition.* New Jersey: Prentice Hall.

Wibowo, Rudini. 2012. *Perancangan Program Penyembunyian Pesan Audio Dengan Metode Steganografi Least Significant Bit Berbasis Android.* Jakarta: Universitas Bina Nusantara.