Penerapan Algoritma RSA dan CBC (*Chiper Block Chaining*) untuk Enkripsi-Dekripsi Citra Digital

Muhammad Hilmi Asyrofi and 13515083[1]
Program Studi Teknik Informatika
Sekolah Teknik Elektro dan Informatika
Institut Teknologi Bandung, Jl. Ganesha 10 Bandung 40132, Indonesia
[1]13515083@std.stei.itb.ac.id

***Abstract*—Keamanan menjadi suatu hal penting yang harus dijaga dalam mentransmisikan sebuah informasi dari suatu tempat ke tempat lain. Terdapat berbagai algoritma yang bisa digunakan dalam pengamanan informasi. Dalam penelitian ini penulis akan melakukan kombinasi algoritma RSA dan mode CBC agar dapat diperoleh hasil enkripsi citra digital dengan tingkat kemananan yang baik dan efektif. Metode penelitian yang dilakukan adalah percobaan 4 kali proses enkripsi-dekripsi dengan melakukan perubahan nilai *p* dan *q*. Setiap proses enkripsi-dekripsi dilakukan 2 variasi. Variasi pertama adalah proses enkripsi-dekripsi hanya menggunakan algoritma RSA. Variasi kedua adalah proses enkripsi-dekripsi menggunakan algoritma RSA dan mode CBC. Variabel pembanding yang digunakan adalah kualitas gambar dan waktu *running time*. Berdasarkan percobaan yang telah dilakukan, diperoleh kesimpulan bahwa penggunaan algoritma RSA untuk enkripsi-dekripsi citra digital masih kurang optimal. Dengan mengkombinasikan algoritma RSA dan mode CBC, hasil enkripsi citra digital menjadi lebih optimal tanpa memakan waktu *running time* yang cukup signifikan.**

***Keywords*—enkripsi, dekripsi, citra digital, algoritma RSA, mode CBC.**

I. PENDAHULUAN

Kecanggihan teknologi informasi memberikan perubahan besar dalam kehidupan manusia. Teknologi informasi semakin memudahkan manusia untuk memperoleh informasi dari berbagai belahan dunia. Terdapat berbagai macam pilihan teknologi yang ditawarkan oleh teknologi informasi.

Salah satu teknologi informasi yang banyak digunakan adalah *interconnected network* atau yang biasa disebut internet. Internet telah menjadi kebutuhan yang tidak bisa dilepaskan dari kehidupan masyarakat di Indonesia. Koneksi internet yang cepat, membuat setiap orang mudah dalam mengakses berbagai informasi dan terhubung tanpa lintas batas (Dian, 2014). Kemudahan akses ini menjadikan internet nyaman digunakan sehingga terjadi komunikasi data dalam jumlah yang sangat banyak. Dengan banyaknya komunikasi data, keamanan menjadi suatu hal penting yang harus dijaga dalam mentransmisikan sebuah informasi dari suatu tempat ke tempat lain. Informasi penting yang ditransmisikan melalui internet akan menimbulkan dampak negatif jika tidak diamankan dengan suatu cara. Salah satu cara yang dapat digunakan adalah dengan menggunakan algoritma RSA.

Penelitian tentang enkripsi dan dekripsi citra digital sudah pernah dilakukan oleh beberapa orang, salah satunya oleh Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran. Penelitian ini dilakukan untuk menjelaskan RSA Kriptosistem dan mengetahui efektivitas algoritma RSA dibandingkan dengan algoritma DES dan Blowfish. Dengan membandingkan waktu *running time* program ketika melakukan proses enkripsi dan dekripsi beberapa citra *grayscale*, diperoleh hasil bahwa penggunaan algoritma RSA membutuhkan waktu yang lebih sedikit daripada algoritma DES dan Blowfish. Pemilihan nilai dua bilangan prima (p dan q) untuk menentukan kunci publik akan berbanding lurus dengan waktu yang dibutuhkan untuk dekripsi dan enkripsi citra digital. Nilai p dan q juga berbanding lurus dengan tingkat keamanan citra digital.

Dalam penelitian ini penulis akan melakukan kombinasi algoritma RSA dan CBC agar dapat diperoleh hasil enkripsi citra digital dengan tingkat kemananan yang baik dan efektif.

II. TINJAUAN PUSTAKA

A. Algoritma RSA

RSA merupakan salah satu algoritma kriptografi asimetri yang paling banyak digunakan karena memiliki tingkat keamanan yang tinggi. Kunci yang digunakan untuk mengenkripsi berbeda dengan kunci yang digunakan untuk mendekripsi. Kunci yang digunakan untuk mengenkripsi disebut dengan kunci public. Kunci yang digunakan untuk mendekripsi disebut dengan kunci privat. RSA membutuhkan tiga langkah dalam prosesnya, yaitu pembangkitan kunci, enkripsi, dan dekripsi.

Berikut ini adalah besaran-besaran yang digunakan dalam algoritma RSA:

- p dan q bilangan prima (rahasia)
- $n = p \cdot q$ (tidak rahasia)
- $\phi(n) = (p - 1)(q - 1)$ (rahasia)

  Syarat: PBB(e, $\phi(n)$) = 1
- e (kunci enkripsi) (tidak rahasia)
- d (kunci dekripsi) (rahasia)

d dihitung dari $d \equiv e^{-1} \bmod (\phi(n))$

- m (plainteks) (rahasia)
- c (cipherteks) (tidak rahasia)

Untuk membangkitkan kunci, digunakan algoritma sebagai berikut:

- pilih dua bilangan prima, p dan q
- hitung $n = pq$
- hitung $\phi(n) = (p - 1)(q - 1)$
- pilih sebuah bilangan bulat e untuk kunci publik
- e harus relatif prima terhadap $\phi(n)$
- hitung kunci dekripsi, d, dengan persamaaan

$$ed \equiv 1 \ (\mathbf{mod}\ \phi(n))$$

Untuk menghitung blok cipherteks c_i (mengenkripsi) pada blok plainteks p_i digunakan persamaan:

$$c_i = m_i^e \ \mathbf{mod}\ n$$

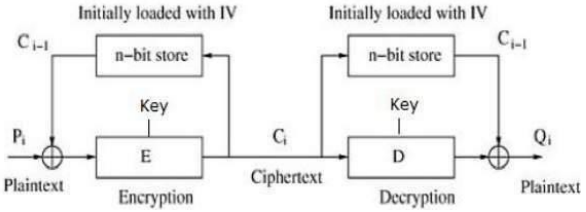
Untuk mendekripsi chiperteks tersebut digunakan persamaan:

$$m_i = c_i^d \ \mathbf{mod}\ n$$

B. CBC

CBC merupakan salah satu jenis *Chiper Block*. *Chiper Block* merupakan cara kriptografi dengan membagi pesan menjadi blok-blok sebesar suatu ukuran. Algoritma ini akan menghasilkan *cipher block* dengan ukuran yang sama dengan plain block sehingga sangat menghemat ukuran terlebih saat dikirimkan melalui suatu jaringan seperti internet (Makalah Kak Boim).

Pada metode CBC, tiap blok memiliki ketergantungan dengan blok yang lain dalam enkripsi dan dekripsinya. Enkripsi dan dekripsi pada metode ini membutuhkan sebuah blok baru yang disebut IV (*Initialization Vector*) yang akan digunakan pada XOR pertama tahap dekripsi maupun enkripsi. Selanjutnya akan dilakukan operasi XOR antara dua blok yang berurutan.



Gambar 1. Cara Kerja CBC
(sumber: Tutorialspoint)

C. Citra Digital

Secara harafiah, citra (*image*) adalah gambar pada bidang dwimatra (dua dimensi). Gambar 2 adalah citra seorang gadis model yang bernama Lena. Ditinjau dari sudut pandang matematis, citra merupakan fungsi menerus (*continue*) dari intensitas cahaya pada bidang dwimatra. Sumber cahaya menerangi objek, objek memantulkan kembali sebagian dari berkas cahaya tersebut. Pantulan cahaya ini ditangkap oleh oleh alat-alat optik, misalnya mata pada manusia, kamera, pemindai (*scanner*), dan sebagainya, sehingga bayangan objek yang disebut citra tersebut terekam (Munir, 2006). Pengolahan citra adalah pemrosesan citra, khususnya dengan menggunakan komputer, menjadi citra yang kualitasnya lebih baik.

III. METODE PENELITIAN

A. Kebutuhan Sistem

Program yang digunakan dalam penelitian ini diimplementasikan menggunakan *library* opencv 3.1.0 dalam bahasa pemrograman C++. Citra digital yang digunakan berukuran *512px* x *512px*. Spesifikasi komputer:

- OS: Ubuntu 16.04 64-bit
- *Processor*: Intel® Core™ i7-6500U @ 2.5 GHz
- RAM: 8 GB

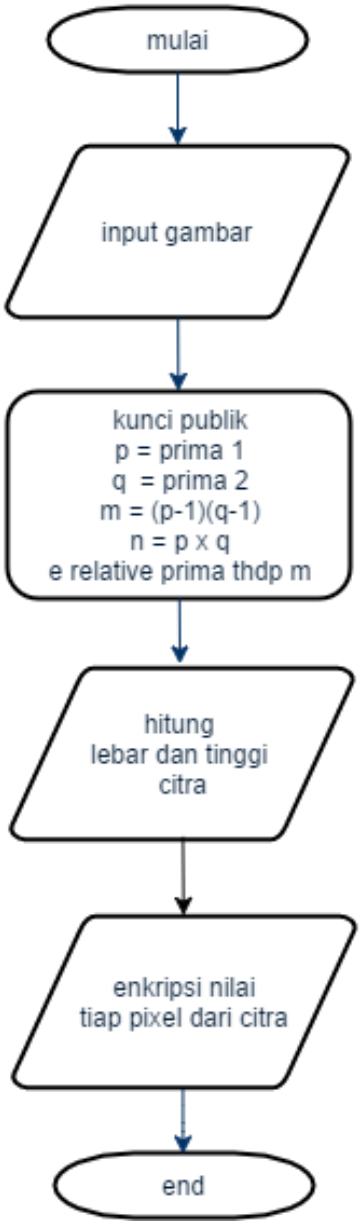
Gambar 2. Citra Uji (Lena)
(sumber:http://informatika.stei.itb.ac.id/~rinaldi.munir)

B. Rancangan Percobaan

Pada makalah ini, peneliti melakukan 4 kali proses enkripsi-dekripsi dengan melakukan perubahan nilai p dan q. Setiap proses enkripsi-dekripsi dilakukan 2 variasi. Variasi pertama adalah proses enkripsi-dekripsi hanya menggunakan RSA. Variasi kedua adalah proses enkripsi-dekripsi menggunakan RSA dan CBC.

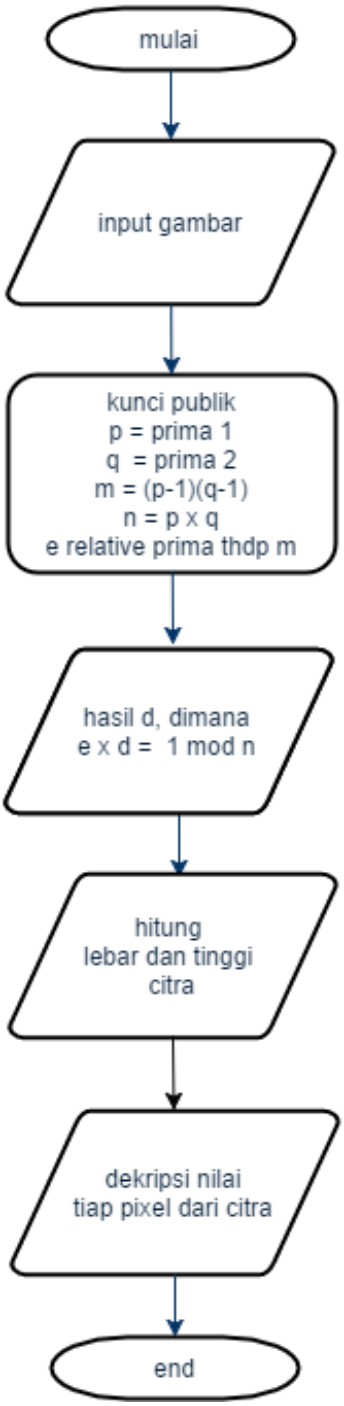
Variabel pembanding yang digunakan adalah kualitas gambar dan waktu *running time*. Perbandingan kualitas gambar digunakan untuk mengetahui kualitas keamanan citra digital. Perbandingan waktu *running time* digunakan untuk mengetahui efektivitas algoritma ketika diimpelmentasikan dalam permasalahan dunia nyata.

B. Proses Enkripsi



Gambar 3. Diagram Alir Proses Enkripsi

C. Proses Dekripsi

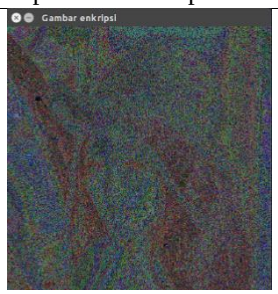
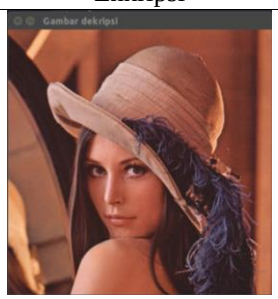


Gambar 4. Diagram Alir Proses Dekripsi

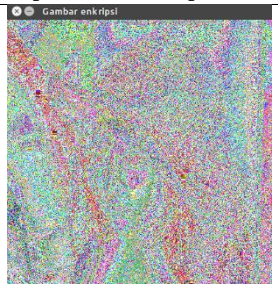
IV. HASIL DAN PEMBAHASAN

A. Hasil Percobaan

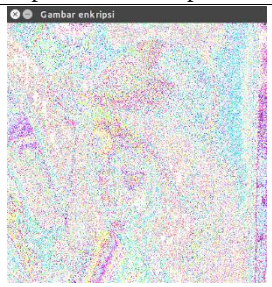
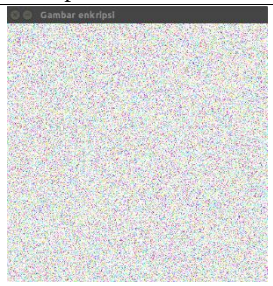
Tabel 1. Perbandingan Citra Uji Percobaan Pertama

Implementasi tanpa CBC	Implementasi CBC
 Enkripsi	 Enkripsi
 Dekripsi	 Dekripsi
Running time : 0,449647 s	*Running time* : 0,478945 s
p = 191 *; q* = 199	

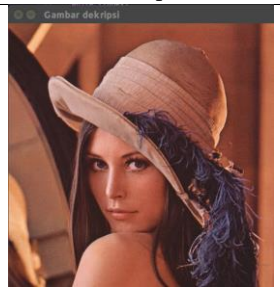
Tabel 2. Perbandingan Citra Uji Percobaan Kedua

Implementasi tanpa CBC	Implementasi CBC
 Enkripsi	 Enkripsi
 Dekripsi	 Dekripsi
Running time : 0,456189 s	*Running time* : 0,448266 s
p = 313 *; q* = 311	

Tabel 3. Perbandingan Citra Uji Percobaan Ketiga

Implementasi tanpa CBC	Implementasi CBC
 Enkripsi	 Enkripsi
Running time : 0,534174 s	*Running time* : 0,543605 s
 Dekripsi	 Dekripsi
p = 523 *; q* = 541	

Tabel 4. Perbandingan Citra Uji Percobaan Keempat

Implementasi tanpa CBC	Implementasi CBC
 Enkripsi	 Enkripsi
 Dekripsi	 Dekripsi
Running time : 0,639287 s	*Running time* : 0,639440 s
p = 1223 *; q* = 1217	

Berdasarkan beberapa tabel di atas, jelas bahwa citra yang dienkripsi hanya dengan algoritma RSA masih memliki tekstur yang kasat mata sehingga pola citra menjadi terlihat. Kemudian pada nilai *p* dan *q* yang sama, citra yang dienkripsi dengan kombinasi RSA dan CBC akan mengalami perubahan citra yang signifikan sehingga secara visual tingkat keamanannya lebih baik dibandingkan citra yang hanya dienkripsi dengan RSA. Dapat kita lihat juga bahwa pada setiap nilai *p* dan *q*,

penggunaan mode CBC tidak mempunyai pengaruh yang signifikan terhadap lama waktu *running time* sehingga kombinasi algoritma ini cukup baik untuk diimplementasikan pada sistem keamanan pada jaringan internet.

B. Proses Enkripsi

	0			1			...			
	R	G	B	R	G	B		R	G	B
0	135	135	083	165	165	263	...	165	165	263
1	100	100	100							
...		...								
	165	165	263					165	165	263

Gambar 5. Asumsi Nilai RGB pada Citra Digital

Nilai tersebut merupakan asumsi nilai RGB dari setiap piksel, misal untuk posisi $f(0,0)$ = (135,135,083) ; $f(1,0)$ = (100,100,100), dengan nilai kunci publik p = 11 dan q = 13.

$n = p \times q = 143$

$\phi(n) = (p-1)\times(q-1) = 120$

Pilih kunci publik e = 17 (yang relatif prima dengan 120 karena pembagi bersama terbesarnya adalah 1)

Nilai e dan n dapat dipublikasikan ke umum

Kunci privat d dihitung dengan kekongruenan:

$$e \times d \equiv 1 \ (\mathbf{mod}\ \phi(n))$$

Dengan melakukan operasi aljabar, diperoleh:

$$d = \frac{1 + (k \times 120)}{17}$$

(k adalah suatu bilangan bulat)

Dengan demikian diperoleh

$$d = 113$$

Blok pesan yang diilustrasikan pada gambar X kemudian dihitung dengan menggunakan rumus $c_i = m_i^e$ **mod** n. Dengan mengambil salah satu koordinat sebagai contoh yaitu koordinat $f(0,0)$ yang memiliki intensitas R = 135, G = 135, dan B = 083 akan dihasilkan

$c_r = m_r^e$ **mod** n.
$c_r = 135^{17}$ **mod** 143
$c_g = 31$

$c_g = m_g^e$ **mod** n.
$c_g = 135^{17}$ **mod** 143
$c_g = 31$

$c_b = m_b^e$ **mod** n.
$c_b = 83^{17}$ **mod** 143
$c_b = 96$

C. Proses Dekripsi

Pada proses deskripsi, koordinat $f(0,0)$ yang telah dienkripsi sebelumnya akan didekripsi menggunakan rumus $m_i = c_i^d$ **mod** n.

$m_r = c_r^d$ **mod** n
$m_r = 31^{113}$ **mod** 143
$m_r = 135$

$m_r = c_r^d$ **mod** n
$m_r = 31^{113}$ **mod** 143
$m_r = 135$

$m_r = c_r^d$ **mod** n
$m_r = 96^{113}$ **mod** 143
$m_r = 83$

Dapat kita lihat bahwa nilai RGB dari citra hasil dekripsi bernilai sama dengan nilai RGB dari citra sebelum enkripsi.

VI. KESIMPULAN

Penggunaan algoritma RSA untuk enkripsi-dekripsi citra digital masih kurang optimal. Dengan mengkombinasikan algoritma RSA dan mode CBC, hasil enkripsi citra digital menjadi lebih optimal tanpa memakan waktu *running time* yang cukup signifikan.

VII. UCAPAN TERIMAKASIH

Penulis mengucapkan terima kasih kepada Tuhan Yang Maha Esa atas selesainya pembuatan tulisan ini. Tidak lupa, penulis berterima kasih kepada dosen mata kuliah IF2120 Matematika Diskrit, yakni Dr. Ir. Rinaldi Munir, MT. dan Dra. Harlili S., M.Sc. yang telah memberikan materi dan bimbingan, baik di dalam maupun di luar kelas, yang bermanfaat dalam pembuatan tulisan ini.

DAFTAR PUSTAKA

[1] Munir, Rinaldi (2005). Matematika Diskrit Revisi Kelima. Bandung: Penerbit ITB, ch. 6

[2] Munir, Rinaldi (2015). Algoritma Kriptografi Modern. Presentasi PowerPoint.

[3] Ali E. Taki El_Deen, El-Sayed A. El-Badawy, Sameh N. Gobran (2014). *Digital Image Encryption Based on RSA Algorithm*. IOSR Journal of Electronics and Communication Engineering (IOSR-JECE) Volume 9

[4] M. Taufiq Tamam, Wakhyu Dwiono, Tri Hartanto (2015). *Penerapan Algoritma Kriptografi ElGamal untuk Pengaman File Citra.*

[5] Feryandi Nurdiantoro, Ibrohim Kholilul Islam, Muhamad Fakhrusy (2015). *Algoritma Cipher Block RG-1*

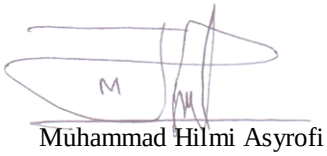
[6] Munir, Rinaldi. Pengolahan Citra Digital. Ebook. Diakses dari http://informatika.stei.itb.ac.id/~rinaldi.munir/Buku/Pengolahan%20Citra%20Digital/Bab-1_Pengantar%20Pengolahan%20Citra.pdf pada 9 Desember 2016.

[7] Annisa Dian. 2014. *Kebutuhan Masyarakat Indonesia akan Internet*. Diakses dari http://www.kompasiana.com/annisadiand/kebutuhan-masyarakat-indonesia-akan-internet_54f400dd7455139f2b6c852c pada 9 Desember 2016.

PERNYATAAN

Dengan ini saya menyatakan bahwa makalah yang saya tulis ini adalah tulisan saya sendiri, bukan saduran, atau terjemahan dari makalah orang lain, dan bukan plagiasi.

Bandung, 9 Desember 2016



Muhammad Hilmi Asyrofi

LAMPIRAN

A. Source Code

https://gitlab.com/mhilmiasyrofi/enkripsi-dekripsi-citra