PENGAMANAN DATA CITRA DENGAN GABUNGAN ALGORITMA RSA DAN OTP

SKRIPSI

Oleh

Prastowo Sandy Asmoro
NIM. 071810101092

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER

2015

PENGAMANAN DATA CITRA DENGAN GABUNGAN ALGORITMA RSA DAN OTP

SKRIPSI

diajukan guna melengkapi tugas akhir dan memenuhi salah satu syarat
untuk menyelesaikan Program Studi Matematika (S1)
dan mencapai gelar Sarjana Sains

Oleh

Prastowo Sandy Asmoro
NIM. 071810101092

JURUSAN MATEMATIKA
FAKULTAS MATEMATIKA DAN ILMU PENGETAHUAN ALAM
UNIVERSITAS JEMBER

2015

PERSEMBAHAN

Syukur alhamdulillah penulis ucapkan atas segala limpahan rahmat dari Allah SWT yang telah memudahkan segala urusan penulis hingga skripsi ini dapat terselesaikan. Semoga skripsi ini menjadi awal yang baik bagi langkah penulis di masa depan. Segala ketulusan dan rasa terimakasih yang tak terhingga, skripsi ini penulis persembahkan untuk:

1. kedua orang tuaku tercinta, Ayahanda Sunaryo H.S. (Alm) dan Ibunda Nursamsi, terimakasih banyak atas doa, kasih sayang tanpa batas, perhatian, dan segala kebaikan yang telah diberikan, semoga Allah SWT selalu mendekap erat dengan kasih sayang-Nya;
2. guru-guru sejak taman kanak-kanak hingga perguruan tinggi, yang telah memberikan ilmu serta bimbingan dengan penuh kesabaran;
3. almamater Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember; SMA Negeri Ambulu; SMP Negeri 1 Ambulu; SDN Andongsari 7.

MOTTO

Yakinlah atas segala usaha yang yang telah kamu lakukan, serahkan hasilnya kepada Allah S.W.T dan jika niatmu baik, maka Allah S.W.T pasti akan memberi lebih atas semua yang kamu harapkan
(QS. Al Kahfi: 45)

PERNYATAAN

Saya yang bertanda tangan di bawah ini:

Nama : Prastowo Sandy Asmoro

NIM : 071810101092

menyatakan dengan sesungguhnya bahwa skripsi yang berjudul ”Pengamanan Data Citra dengan Gabungan Algoritma RSA Dan OTP” adalah benar-benar hasil karya sendiri, kecuali jika dalam pengutipan substansi disebutkan sumbernya dan belum pernah diajukan pada institusi manapun, serta bukan karya jiplakan. Saya bertanggung jawab atas keabsahan dan kebenaran isinya sesuai dengan sikap ilmiah yang harus dijunjung tinggi.

Demikian pernyataan ini saya buat dengan sebenar-benarnya, tanpa adanya tekanan dan paksaan dari pihak manapun serta bersedia mendapat sanksi akademik jika ternyata dikemudian hari pernyataan ini tidak benar.

Jember, Januari 2015

Yang menyatakan,

Prastowo Sandy Asmoro

NIM 071810101092

SKRIPSI

PENGAMANAN DATA CITRA DENGAN GABUNGAN ALGORITMA RSA DAN OTP

Oleh
Prastowo Sandy Asmoro
NIM 071810101074

Pembimbing

Dosen Pembimbing Utama : Kiswara Agung Santoso, S.Si., M.Kom.
Dosen Pembimbing Anggota : Ahmad Kamsyakawuni, S.Si, M.Kom.

PENGESAHAN

Skripsi yang berjudul ”Pengamanan Data Citra Dengan Gabungan Algoritma RSA dan OTP” telah diuji dan disahkan pada:

hari, tanggal :

tempat : Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember

Tim Penguji :

Dosen Pembimbing Utama,	Dosen Pembimbing Anggota,
Kiswara Agung Santoso, S.Si., M.Kom.	Ahmad Kamsyakawuni, S.Si., M.Kom.
NIP. 19720907 199803 1 003	NIP. 19721129 199802 1 001
Penguji I,	Penguji II,
Kusbudiono, S.Si., M.Si.	Ika Hesti Agustin, S.Si., M.Si.
NIP. 19770430 200501 1 001	NIP. 19840801 200801 2 006

Mengesahkan
Dekan,

Prof. Drs. Kusno, DEA, Ph.D.
NIP. 19610108 198602 1 001

RINGKASAN

Pengamanan Data Citra Dengan Gabungan Algoritma RSA dan OTP. Prastowo Sandy Asmoro, 071810101092; 2015: 38 halaman; Jurusan Matematika Fakultas MIPA Universitas Jember.

Kriptografi adalah seni dan ilmu untuk menyembunyikan informasi dari penerima yang tidak berhak. Pada penelitian ini digunakan dua algoritma yaitu algoritma *Rivest Shamir Adleman* (RSA) dan *One Time Pad* (OTP) dengan dua proses utama, yaitu proses enkripsi dan dekripsi. Enkripsi merupakan proses mengubah citra asli (*plain image*) menjadi citra tersandi (*cipher image*) sedangkan dekripsi merupakan proses mengubah citra tersandi (*cipher image*) menjadi citra asli (*plain image*).

Pada penelitian ini proses enkripsi dibagi menjadi beberapa tahapan. Tahap pertama adalah menentukan kunci publik untuk algoritma RSA. Selanjutnya menentukan kunci algoritma OTP yang dimensinya sama dengan dimensi *plain image.* Setelah kunci publik RSA dan kunci OTP terbentuk, dilakukan enkripsi dengan algoritma RSA yang dilanjutkan dengan enkripsi dengan algoritma OTP hingga menghasilkan *cipher image.*

Proses dekripsi pada penelitian ini dibagi menjadi dua tahap. Tahap pertama adalah mendekripsi *cipher image* dengan algoritma OTP. Tahap selanjutnya adalah mendekripsi dengan algoritma RSA menggunakan kunci privat dan menghasilkan *plain image* kembali.

Langkah selanjutnya dalam penelitian ini adalah pembuatan program enkripsi dan dekripsi. Pada tahap pembuatan program ini akan dibuat program dengan bahasa pemrograman PHP. Setelah pembuatan program selesai, selanjutnya dilakukan simulasi program tersebut. Program yang telah selesai diuji dengan menggunakan citra digital berekstensi *.bmp* dengan berbagai ukuran.

Tahap terakhir dalam pembuatan skripsi ini adalah menganalisis hasil simulasi. Pada tahap ini, akan dilakukan analisis hasil yang diperoleh dari simulasi

program. Analisis dilakukan dengan membandingkan ukuran, nilai PSNR dan ketampakan visual citra digital sebelum dan sesudah proses enkripsi.

Berdasarkan hasil implementasi dan pengujian yang telah dilakukan, dapat diambil kesimpulan bahwa pada proses pengujian program dengan melakukan enkripsi, terjadi perubahan ukuran file *cipher image* sebesar 2 byte dibandingkan dengan ukuran file *plain image*. Berdasarkan perhitungan nilai MSE dan PSNR didapatkan nilai MSE yang sangat besar dan menghasilkan nilai PSNR yang bernilai kecil sehingga *cipher image* sangat berbeda dengan *plain image.* Sedangkan untuk perbandingan *image* sebelum dienkripsi dan *image* setelah didekripsi diperoleh nilai $MSE = 0$ dan nilai $PSNR$ yang tidak dapat didefinsikan yang berarti tidak ada perbendaan sama sekali antara kedua *image* tersebut. Pada proses pengamatan visual secara langsung, terlihat perbedaan yang siginifikan antara *plain image* dan *cipher image*. Hal ini karena komponen RGB pada tiap-tiap piksel yang membentuk *cipher image* berbeda dengan yang membentuk *plain image*.

PRAKATA

Puji syukur kami atas kehadirat Allah SWT atas segala limpahan rahmat, taufik, serta hidayah-Nya, sehingga penulis dapat menyelesaikan skripsi yang berjudul **"Pengamanan Data Citra Dengan Gabungan Algoritma RSA dan OTP".** Skripsi ini disusun untuk memenuhi salah satu syarat menyelesaikan pendidikan strata satu (S1) pada Jurusan Matematika Fakultas Matematika dan Ilmu Pengetahuan Alam Universitas Jember.

Penulis banyak mendapat bantuan dalam penyusunan skripsi. Oleh karena itu, penulis menyampaikan terima kasih yang sebesar-besarnya kepada:

1. Prof. Drs. Kusno, DEA., Ph.D., selaku Dekan FMIPA Universitas Jember
2. Bapak Kiswara Agung Santoso, S.Si., M.Kom., selaku Dosen Pembimbing Utama dan Bapak Ahmad Kamsyakawuni, S.Si., M.Kom., selaku Dosen Pembimbing Anggota yang telah meluangkan waktu dan pikiran serta perhatiannya guna memberikan bimbingan dan pengarahan demi terselesaikannya penulisan skripsi ini;
3. Bapak Kusbudiono, S.Si., M.Si., sebagai Dosen Penguji I dan Dosen Pembimbing Akademik serta Ibu Ika Hesti Agustin, S.Si., M.Si., selaku Dosen Penguji yang telah memberikan saran dan kritik demi terselesainya penulisan skripsi ini;
4. Ibunda Nursamsi yang telah memberikan doa, dorongan semangat, serta nasihat demi terselesaikannya skripsi ini;
5. Yogi dan Ferry yang telah berbagi saran, pemikiran dan tenaga dalam penulisan skripsi ini.
6. teman-teman "Akatsuki 07" yang telah menemani dan membantu dalam menyelesaikan skripsi ini;
7. serta semua pihak yang tidak dapat disebutkan satu per satu.

Penulis menerima kritik dan saran dari semua pihak demi kesempurnaan skripsi ini. Semoga skripsi ini dapat diterima dan bermanfaat bagi pembaca.

Jember, 15 Januari 2014 Penulis

DAFTAR ISI

DAFTAR TABEL

Halaman

DAFTAR GAMBAR

Halaman

DAFTAR LAMPIRAN

BAB 1. PENDAHULUAN

1.1 Latar Belakang

Teknologi yang makin berkembang semakin memudahkan manusia untuk memenuhi kebutuhannya dalam hal komunikasi. Dahulu kala manusia harus melakukan perjalanan untuk berkomunikasi dengan orang lain di tempat yang berbeda. Namun pada masa kini manusia bisa dengan mudah berkomunikasi dengan orang lain melalui internet. Dengan hadirnya internet, informasi dapat dengan mudahnya menyebar ke seluruh penjuru dunia hanya dalam hitungan detik. Internet sebagai jalan raya informasi *(the information highway)* telah banyak dirasakan membawa perubahan pada banyak aspek dalam kehidupan manusia.

Namun internet juga merupakan salah satu jaringan publik yang tidak aman. Kegiatan-kegiatan transaksi informasi tersebut tentu saja akan menimbulkan resiko apabila informasi yang sensitif dan berharga tersebut diakses oleh orang-orang yang tidak berhak *(unauthorized persons),* misalnya pesan berupa data teks atau gambar yang besifat pribadi dan rahasia. Setiap orang yang mengirimkan pesan tentu berkeinginan pesan yang dikirimkan akan aman. Aman dalam artian aman dari ancaman orang yang tidak berhak. Berbagai ancaman yang mungkin terjadi antara lain tidak sampainya pesan, tersadapnya pesan, pesan yang dimanipulasi, hingga penyamaran dan penyangkalan karena ada pihak yang mengirimkan pesan dengan identitas orang lain. Tanpa fasilitas keamanan yang baik, sang penerima akan menerima dokumen tersebut tanpa mencurigai adanya perubahan yang dapat merugikan baik bagi pengirim maupun penerima. Untuk itu diperlukan sistem pengamanan yang dapat melindungi data yang ditransmisikan melalui suatu jaringan komunikasi. Salah satu cara yang dapat dilakukan untuk pengamanan data melalui suatu saluran data adalah kriptografi.

Kriptografi merupakan bagian dari suatu cabang ilmu matematika yang disebut *Cryptology*. Kriptografi bertujuan menjaga kerahasiaan informasi yang terkandung dalam data sehingga informasi tersebut tidak dapat diketahui oleh pihak yang tidak sah. Oleh karena itu, Kriprografi atau penyandian dikatakan sebagai metode yang cukup tangguh karena dalam kriptografi data yang

dikirimkan melalui jaringan akan disamarkan sedemikian rupa menggunakan algoritma sandi. Data tersebut akan tetap aman kendati setiap orang dapat mengaksesnya secara bebas, sehingga kalaupun data tersebut dapat dibaca tetapi tidak dapat dipahami oleh pihak yang tidak berhak (Schneier, 1996). Oleh karena itu pengembangan metode kriptografi perlu diperluas penggunaannya yang tidak hanya terbatas untuk penyandian berupa teks, tetapi juga berupa gambar, audio maupun video (Siang, 2002).

Kriptografi semakin berkembang seiring perkembangan teknologi komputer. Beragam algoritma kriptografi dibuat untuk mengamankan suatu data. Dalam beberapa penelitian sebelumnya telah dibahas mengenai kriptografi, antara lain: Aplikasi Kriptosistem RSA pada Proses Autentikasi User dengan urutan Abjad terbalik (Mustaqim, 2011), Implementasi Algoritma *One Time Pad* pada Data Teks dan *Knapsack* pada Kunci (Prameswara, 2012)

Algoritma RSA merupakan algoritma kriptografi kunci publik yang terkenal aman karena sulitnya memecahkan fungsi matematis yang dipakai sebagai dasar pembuatan algoritmanya (Ariyus, 2008). Sedangkan algoritma OTP merupakan suatu metode yang sangat kuat karena panjang kunci sama dengan panjang pesan yang dikirim dan kunci yang digunakan adalah *session key*, dimana kunci hanya berlaku untuk satu kali proses enkripsi. Metode ini sangat baik untuk mengirim pesan yang panjang karena akan semakin sulit untuk mengetahui kunci yang digunakan (Sujono, 2007).

Berdasarkan kelebihan dari algoritma RSA dan OTP diatas maka peneliti akan mengkaji pengamanan data citra menggunakan gabungan metode RSA dan OTP. Metode ini diharapkan dapat membantu upaya dalam peningkatan pengamanan terhadap pengiriman suatu pesan terutama yang berupa *image*.

1.2 Rumusan Masalah

Berdasarkan penjelasan pada bagian latar belakang, maka permasalahan yang menjadi titik utama pembahasan adalah “Bagaimana mengimplementasikan proses enkripsi dan dekripsi *image* menggunakan gabungan algoritma RSA dan OTP”

1.3 Batasan Masalah

Agar tidak terjadi kesalahan persepsi dan meluasnya pokok bahasan maka dibuat batasan bahwa *file image* yang akan digunakan sebagai input penelitian adalah *image* berformat bitmap 24 bit.

1.4 Tujuan

Tujuan yang ingin dicapai dalam tugas akhir ini adalah:

a. Menerapkan suatu sistem keamanan dengan menggunakan gabungan algoritma RSA dan OTP pada data *image*,
b. Merancang dan membangun suatu program yang dapat digunakan untuk mengenkripsi dan mendekripsi *file image*.

1.5 Manfaat

Dari hasil penelitian ini diharapkan dapat diperoleh beberapa manfaat yaitu: Meningkatkan keamanan dalam penyampaian pesan yang berupa *image* dan memberikan tambahan referensi bagi perancang keamanan sistem aplikasi berbasis *web*.

BAB 2. TINJAUAN PUSTAKA

2.1 Landasan Matematika

Perkembangan kriptografi akan dipengaruhi oleh perkembangan matematika, terutama dalam hal algoritma (Kromodimoeljo, 2009). Beberapa teori dalam matematika yang berkaitan dengan kriptografi adalah:

2.1.1 *Greatest Common Divisor* (GCD)

Greatest Common Divisor (GCD) atau biasa disebut dengan Faktor Persekutuan Terbesar (FPB) adalah pembagi terbesar dari dua buah bilangan.

Definisi 2.1 Jika $d|a$ dan $d|b$ maka d adalah pembagi persekutuan (common divisor) dari a dan b. Untuk setiap pasangan bilangan bulat a dan b kecuali jika $a = b = 0$,
pembagi persekutuan terbesar dari a dan b adalah bilangan bulat unik d dimana:

a. d merupakan pembagi persekutuan dari a dan b,
b. jika c merupakan pembagi persekutuan dari a dan b, maka $c \leq d$.

Definisi 2.2 Dua bilangan bulat a dan b, dimana salah satu dari keduanya tidak sama dengan 0, dikatakan relatif prima jika $\gcd(a, b) = 1$ (Kromodimoeljo, 2009).

2.1.2 Aritmatika Modulo

Aritmatika modulo (*modular arithmethic*) memainkan peran yang penting dalam komputasi integer, khususnya pada aplikasi kriptografi. Operator yang digunakan pada aritmatika modulo adalah mod. Operator mod, jika digunakan pada pembagian bilangan bulat memberikan sisa pembagian sebagai kembaliannya.

Misalkan a adalah bilangan bulat dan m adalah bilangan bulat yang lebih besar dari 0. Operasi $a \bmod m$ (dibaca "a modulo m") memberikan sisa jika a

dibagi dengan m. Notasi a mod $m = r$ sedemikian sehingga $a = mq + r$, dengan $0 \leq r < m$. Bilangan m disebut modulus atau modulo (Munir, 2004).

Aritmetika modulo cocok digunakan untuk kriptografi karena dua alasan:

a. Oleh karena nilai-nilai aritmetika modulo berada dalam himpunan berhingga (0 sampai modulus $m - 1$), maka kita tidak perlu khawatir hasil perhitungan berada di luar himpunan.
b. Karena kita bekerja dengan bilangan bulat, maka kita tidak khawatir kehilangan informasi akibat pembulatan (*round off*) sebagaimana pada operasi bilangan riil.

Teorema 2.1 (*Chinese Reminder Theorem*) Jika terdapat beberapa persamaan dengan modulus berbeda sebagai berikut:

$$x \equiv a_1 (\text{mod } m_1)$$
$$x \equiv a_2 (\text{mod } m_2)$$
$$\vdots$$
$$x \equiv a_i (\text{mod } m_j)$$

dimana setiap pasangan modulus adalah relatif prima ($\gcd(m_i, m_j) = 1$ untuk $i \neq j$), maka terdapat solusi untuk x. jika x_1 dan x_2 merupakan solusi untuk x, maka $x \equiv x_1 (\text{mod } M)$ dimana $M = m_1 m_2 \ldots m_r$

Bukti:

Pembuktian bahwa sistem persamaan seperti diatas mempunyai solusi untuk x bersifat konstruktif, jadi menghasilkan algoritma untuk mencari solusi. Didefnisikan $M_i = M = m_i$, jadi M_i merupakan produk dari semua modulus kecuali m_i. Karena $\gcd(m_i, M_i) = 1$, maka terdapat bilangan bulat $N_i$dimana $M_i N_i \equiv 1 \ (\text{mod } m_i)$.

Maka suatu solusi untuk x adalah

$$x = \sum_{j=1}^{r} a_j M_j N_j$$

Untuk setiap i, karena semua suku kecuali suku i dapat dibagi dengan m_i, maka hanya suku i yang tidak $\equiv 0 \ (\text{mod } m_i)$, jadi

$$x \equiv a_i M_i N_i \equiv a_i \ (\text{mod } m_i)$$

seperti yang dikehendaki. Untuk menunjukkan bahwa solusi x unik modulo M, kita tunjukkan bahwa jika x_1 dan x_2 adalah solusi untuk x, maka $x_1 \equiv x_2 (\mathrm{mod}\, M)$. Untuk setiap i, $x_1 \equiv x_2 \equiv a_i \,(\mathrm{mod}\, m_1)$, atau $x_1 - x_2 \equiv 0 \,(\mathrm{mod}\, m_i)$. Jadi $x_1 - x_2 \equiv 0 \,(\mathrm{mod}\, M)$. yang berarti $x_1 \equiv x_2 \,(\mathrm{mod}\, M)$ ■ (Irawan, 2013).

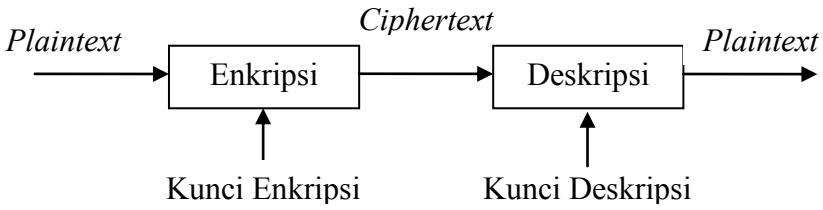
Teorema 2.2: (Teorema Fermat Kecil). Jika p adalah bilangan prima dan a adalah bilangan bulat positif, maka

$$a^{p-1} = 1 \,(\mathrm{mod}\, p)$$

2.2 Kriptografi

Kriptografi adalah suatu ilmu yang mempelajari bagaimana cara menjaga agar data atau pesan tetap aman saat dikirimkan, dari pengirim ke penerima tanpa mengalami gangguan dari pihak ketiga. Menurut Bruce Scheiner (1996) dalam bukunya *"Applied Cryptography"*, kriptografi adalah ilmu pengetahuan dan seni menjaga *message-message* agar tetap aman *(secure).* Ada beberapa definisi kriptografi yang digunakan sebelum tahun 1980 yang menyatakan bahwa kriptografi adalah ilmu untuk menjaga kerahasiaan pesan dengan cara menyandikan ke bentuk yang tidak dimengerti.

Kriptografi itu sendiri terdiri dari dua proses utama yakni proses enkripsi dan proses dekripsi. Seperti yang telah dijelaskan di atas, proses enkripsi mengubah *plaintext* menjadi *ciphertext* (dengan menggunakan kunci tertentu) sehingga isi informasi pada pesan tersebut sukar dimengerti. Urutan proses enkripsi dan deskripsi dalam kriptografi secara umum dapat dilihat pada Gambar 2.1.



Gambar 2.1 Diagram proses enkripsi dan deskripsi

2.2.1 Komponen Kriptografi

Dalam kriptografi terdapat beberapa istilah penting antara lain:

a. Pesan, Plainteks, dan Cipherteks

Pesan merupakan data atau informasi yang dapat dibaca dan dimengerti maknanya. Nama lain untuk pesan adalah plainteks (*plaintext*). Pesan dapat berupa data atau informasi yang dikirim atau yang disimpan dalam media penyimpanan. Pesan yang tersimpan bisa berbentuk teks, citra (*image*), suara/bunyi (*audio*) dan video. Agar pesan tidak dapat dimengerti maknanya oleh pihak lain maka, pesan dapat disandikan ke bentuk lain yang tidak dapat dipahami. Bentuk pesan yang tersandi disebut cipherteks (*ciphertext*).

b. Pengirim dan Penerima

Komunikasi data melibatkan pertukaran pesan antara dua entitas. Pengirim (*sender*) adalah entitas yang mengirim pesan kepada entitasnya yang lain. Penerima (*receiver*) adalah entitas yang menerima pesan. Entitas di sini dapat berupa orang, mesin (komputer), kartu k*red*it, dan sebagainya. Proses menyandikan plainteks menjadi cipherteks disebut enkripsi (*encryption*) sedangkan proses untuk mengembalikan pesan tersandi (cipherteks) menjadi plainteks semula dinamakan dekripsi (*decryption*).

c. *Cipher* dan Kunci

Algoritma kriptografi disebut juga *cipher* yaitu aturan untuk *enchipering* dan dechipering, atau fungsi matematika yang digunakan untuk enkripsi dan dekripsi. Keamanan algoritma kriptografi sering diukur dari banyaknya kerja (*work*) yang dibutuhkan untuk memecahkan cipherteks menjadi plainteks tanpa mengetahui kunci yang digunakan. Kunci (*key*) merupakan parameter yang digunakan untuk transformasi *enciphering* dan *deciphering*. Kunci biasanya berupa *string* atau deretan bilangan.

d. Sistem kriptografi

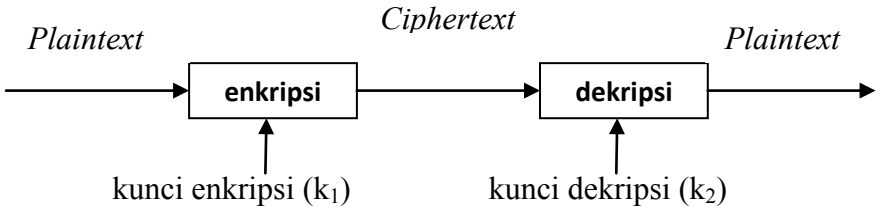
Kriptografi membentuk sebuah sistem yang dinamakan sistem kriptografi. Sistem kriptografi (*cryptosystem*) terdiri dari algoritma kriptografi, semua plainteks dan cipherteks yang mungkin dan kunci.

2.2.2 Teknik Kriptografi

Berdasarkan kuncinya, terdapat 2 (dua) teknik yang digunakan dalam kriptografi modern yaitu:

a. Algoritma Kunci Asimetris

Algoritma asimetris (*asymmetric algorithm*) adalah suatu algoritma di mana kunci enkripsi yang digunakan tidak sama dengan kunci dekripsi. Pada algoritma ini menggunakan 2 (dua) kunci yaitu kunci umum (*public key*) dan kunci pribadi (*privacy key*). Kunci publik disebarkan secara umum sedangkan kunci pribadi disimpan secara rahasia oleh si pengguna. Walau kunci publik telah diketahui namun akan sangat sukar mengetahui kunci pribadi yang digunakan. Pada umumnya kunci publik (*public key*) digunakan sebagai kunci enkripsi sementara kunci pribadi (*privacy key*) digunakan sebagai kunci dekripsi.

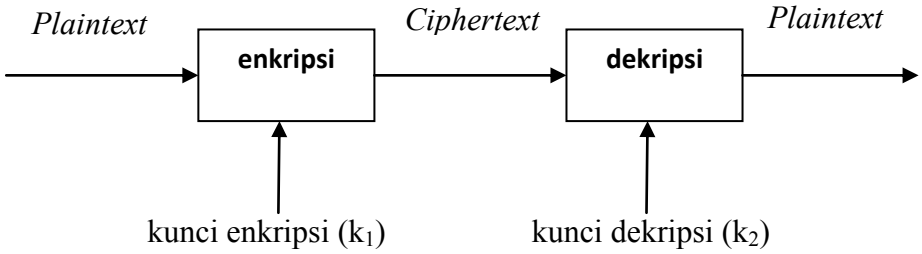


Gambar 2.2 Algoritma Asimetris

Contoh algoritma kunci asimetri: DSA (*Digital Signature Algorithm*), RSA (*Rivest Shamir Adleman*), DH (*Diffie Hellman*), ElGamal, ECC (*Elliptic Curve Cryptography*) dan lain sebagainya.

b. Algoritma Kunci Simetris

Algoritma simetris (*symmetric algorithm*) adalah algoritma dimana kunci enkripsi yang digunakan sama dengan kunci dekripsi sehingga algoritma ini disebut juga sebagai *single-key algorithm*. Sebelum melakukan pengiriman pesan, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama dan kunci ini haruslah rahasia bagi pihak yang tidak berkepentingan sehingga algoritma ini disebut juga algoritma kunci pribadi (*privacy key algorithm*).



Gambar 2.3 Algoritma Simetris

Contoh algoritma kunci simetris: DES (*Data Encryption Standard*), TDES (*Triple Data Encryption Standard*), RC2 (*Rivest Cipher 2*), RC4 (*Rivest Cipher 4*), RC5 (*Rivest Cipher 5*), RC6 (*Rivest Cipher 6*), IDEA (*International Data Encryption Algorithm*), AES (*Advanced Encryption Standard*), OTP (*One Time Pad*), dan lain sebagainya.

2.2.3 Algoritma RSA (Rivest Shamir Adleman)

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 (Ariyus, 2008).

Algoritma enkripsi-dekripsi dengan metoda RSA adalah sebagai berikut:

1. Ambil dua bilangan prima p dan q
2. Hitung $n = p \times q$ dan $m = (p-1)(q-1)$
3. Cari bilangan e, yang relatif prima dan harus lebih kecil dari m.
4. Hitung d dimana $d = e^{-1} \bmod m$ atau $(e \times d) \bmod m = 1$.
5. Lakukan enkripsi dengan n dan e dimana $C = P^e \bmod n$.
6. Lakukan dekripsi dengan n dan d dimana $P = C^d \bmod n$.

Misalkan Sony mengirim pesan "HELLO WORLD" kepada Setya dengan nilai numerik pesan adalah 07 04 11 11 14 26 22 14 17 11 03. Sony memilih dua bilangan prima $p = 7$ dan $q = 11$. Selanjutnya Sony menghitung nilai $n = p \times q = 7 \times 11 = 77$ dan nilai $m = 6 \times 10 = 60$. Kemudian Sony memilih kunci

umum $e = 17$ dan menghitung kunci rahasia $d = 53$. Sony melakukan enkripsi dengan kunci umum untuk menghasilkan *ciphertext*. Kemudian Setya melakukan dekripsi dengan kunci rahasia untuk menghasilkan *plaintext*. Sebagai ilustrasi dapat dilihat pada Tabel 2.1.

Tabel 2.1 Ilustrasi Algoritma RSA

Enkripsi				Dekripsi		
Plain Text (X)	*Desimal (X)*	$Y = X^e \bmod n$	*Cipher Text (Y)*	$X = Y^d \bmod n$	*Desimal (X)*	*Plain Text (X)*
H	7	$7^{17} \bmod 77$	28	$28^{53} \bmod 77$	7	H
E	4	$4^{17} \bmod 77$	16	$16^{53} \bmod 77$	4	E
L	11	$11^{17} \bmod 77$	14	$14^{53} \bmod 77$	11	L
L	11	$11^{17} \bmod 77$	14	$14^{53} \bmod 77$	11	L
O	14	$14^{17} \bmod 77$	42	$42^{53} \bmod 77$	14	O
	26	$26^{17} \bmod 77$	38	$38^{53} \bmod 77$	26	
W	22	$22^{17} \bmod 77$	22	$22^{53} \bmod 77$	22	W
O	14	$14^{17} \bmod 77$	42	$42^{53} \bmod 77$	14	O
R	17	$17^{17} \bmod 77$	19	$19^{53} \bmod 77$	17	R
L	11	$11^{17} \bmod 77$	44	$44^{53} \bmod 77$	11	L
D	3	$3^{17} \bmod 77$	75	$75^{53} \bmod 77$	3	D

2.2.4 Algoritma OTP (*One-Time Pad)*

Algoritma ini ditemukan pada tahun 1917 oleh Mayor Joseph Mauborgne dan Gilbert Vernam. Algoritma ini termasuk ke dalam kelompok algoritma kriptografi simetri. Algoritma ini diimplementasikan melalui sebuah kunci yang terdiri dari sekumpulan random karakter-karakter yang tidak berulang. Setiap huruf kunci dijumlahkan modulo 26 dengan huruf pada *plaintext*. Pada *One Time Pad*, tiap huruf kunci digunakan satu kali untuk satu pesan dan tidak digunakan kembali. Panjang stream karakter kunci sama dengan panjang pesan. *One time pad* (*pad* = kertas bloknot) berisi barisan karakter-karakter kunci yang dibangkitkan secara acak. Satu *pad* hanya digunakan sekali (*one time*) saja untuk mengenkripsi pesan, setelah itu pad yang telah digunakan dihancurkan (Prameswara, 2012).

Satu-satunya algoritma kriptografi sempurna aman dan tidak dapat dipecahkan adalah *One Time Pad*, sehingga mendapat gelar *unbreakable cipher*. Algoritma ini

menggunakan kunci yang digunakan hanya untuk satu pesan. Untuk pesan berikutnya akan digunakan kunci lain melalui proses pengacakan. Namun Algoritma ini memiliki kelemahan, kunci yang digunakan harus benar-benar acak, panjang kunci juga harus sama dengan panjang pesan (Munir, 2006).

Misalkan, kita akan mengenkripsi kata 'O N E' menggunakan algoritma *one time pad,* yaitu:

$$(P + K) \bmod 26 = C \tag{2.1}$$

Dimana P adalah plainteks, K adalah kunci, dan C adalah cipherteks. Misalkan $A = 0, B = 1, \dots, Z = 25$, sehingga:

Plainteks : O N E

Kunci : G N R

Cipherteks: U A V

Chiperteks tersebut didapat dari:

$(O + G) \bmod 26 = U$, yaitu $(14 + 6) \bmod 26 = 20$

$(N + N) \bmod 26 = O$, yaitu $(13 + 13) \bmod 26 = 0$

$(E + R) \bmod 26 = V$, yaitu $(4 + 17) \bmod 26 = 21$

Proses dekripsinya dilakukan dengan menggunakan kunci yang sama dengan yang dipakai untuk enkripsi, dengan langkah sebagai berikut:

$(U - G) \bmod 26 = O$, yaitu $(20 - 6) \bmod 26 = 14$

$(A - N) \bmod 26 = N$, yaitu $(0 - 13) \bmod 26 = 13$

$(V - R) \bmod 26 = E$, yaitu $(21 - 17) \bmod 26 = 4$

2.2 Citra Digital

Citra digital dapat didefinisikan sebagai fungsi dua variabel, $f(x, y)$, dimana x dan y adalah koordinat spasial dan nilai $f(x, y)$ yang merupakan intensitas citra pada koordinat tersebut. Teknologi dasar untuk menciptakan dan menampilkan warna pada citra digital berdasarkan pada penelitian bahwa sebuah warna merupakan kombinasi dari tiga warna dasar, yaitu merah, hijau, dan biru (*Red, Green, Blue*-RGB) (Wijaya, 2007). Sistem kordinat pada sebuah citra digital dapat dilihat pada Gambar 2.4.

Gambar 2.4 Sistem koordinat citra digital

RGB adalah suatu model warna yang terdiri dari merah, hijau, dan biru, digabungkan dalam membentuk suatu susunan warna yang luas. Setiap warna dasar, misalnya merah, dapat diberi rentang nilai. Untuk monitor komputer, nilai rentangnya paling kecil adalah 0 dan paling besar adalah 255. Pilihan skala 256 ini didasarkan pada cara mengungkap 8 digit bilangan biner yang digunakan oleh mesin komputer. Dengan cara ini, akan diperoleh warna campuran sebanyak $256 \times 256 \times 256 = 1677726$ jenis warna. Sebuah jenis warna, dapat dibayangkan sebagai sebuah vektor di ruang dimensi 3 yang biasanya dipakai dalam matematika, koordinatnya dinyatakan dalam bentuk tiga bilangan, yaitu komponen-*x*, komponen-*y* dan komponen-*z*. Misalkan sebuah vektor dituliskan sebagai $r = (x, y, z)$. Untuk warna, komponen-komponen tersebut digantikan oleh komponen R(*ed*), G(*reen*), B(*lue*). Jadi, sebuah jenis warna dapat dituliskan sebagai berikut: warna=RGB (30,75,255), putih = RGB (255,255,255), sedangkan untuk hitam= RGB(0,0,0).

Berdasarkan warna-warna penyusunnya, citra digital dapat dibagi menjadi tiga macam (Wijaya, 2007) yaitu:

a. Citra biner, yaitu citra yang hanya terdiri atas dua warna, yaitu hitam dan putih. Oleh karena itu, setiap pixel pada citra biner cukup direpresentasikan dengan 1 bit.
b. Citra *grayscale*, yaitu citra yang nilai pixel-nya merepresentasikan derajat keabuan atau intensitas warna putih. Nilai intensitas paling rendah

merepresentasikan warna hitam dan nilai intensitas paling tinggi merepresentasikan warna putih. Pada umumnya citra grayscale memiliki kedalaman *pixel* 8 bit (256 derajat keabuan), tetapi ada juga citra grayscale yang kedalaman *pixel*-nya bukan 8 bit, misalnya 16 bit untuk penggunaan yang memerlukan ketelitian tinggi.

c. Citra berwarna, yaitu citra yang nilai *pixel*-nya merepresentasikan warna tertentu Banyaknya warna yang mungkin digunakan bergantung kepada kedalaman *pixel* citra yang bersangkutan. Citra berwarna direpresentasikan dalam beberapa kanal (*channel*) yang menyatakan komponen-komponen warna penyusunnya. Banyaknya kanal yang digunakan bergantung pada model warna yang digunakan pada citra tersebut.

2.2.1 Teori Warna

Teori warna dibahas oleh Brewster yang pertama kali dikemukakan pada tahun 1831. Teori warna ini menyederhanakan warna-warna yang ada di alam menjadi 4 kelompok warna, yaitu warna primer, sekunder, tersier dan warna netral. (Terahadi, 2011).

a. Warna primer

Warna primer merupakan warna dasar yang tidak merupakan campuran dari warna-warna lain. Warna yang termasuk dalam golongan primer adalah merah, biru dan kuning. Warna primer menurut teori warna Brewster adalah warna-warna dasar. Warna-warna lain dibentuk dari kombinasi warna primer. Pada awalnya manusia mengira bahwa warna primer tersusun atas warna Merah, Kuning dan Hijau. Namun dalam penelitian lebih lanjut, dikatakan warna primer adalah merah (seperti darah), biru (seperti langit atau laut) dan kuning (seperti kuning telur). Warna primer terbagi menjadi dua jenis yaitu warna primer additif dan warna primer subtraktif.

1) Warna primer additif

Alat/media yang menggabungkan pancaran cahaya untuk menciptakan sensasi warna menggunakan sistem warna additif. Televisi adalah yang paling umum. Warna primer additif adalah merah, hijau dan biru. Campuran warna cahaya merah dan hijau, menghasilkan nuansa

warna kuning atau orange. Campuran hijau dan biru menghasilkan nuansa cyan, sedangkan campuran merah dan biru menhasilkan nuansa ungu dan magenta. Campuran dengan proporsi seimbang dari warna additif primer menghasilkan nuansa warna kelabu, jika ketiga warna ini disaturasikan penuh, maka hasilnya adalah warna putih. Ruang warna/model warna yang dihasilkan disebut dengan RGB (*Red, Green, Blue*).

2) Warna primer subtraktif

Media yang menggunakan pantulan cahaya untuk untuk menghasilkan warna memakai metode campuran warna subtraktif. Ruang warna/model warna yang dihasilkan disebut dengan CMYK (*Cyan, Magenta, Yellow, Key*). *Key* adalah warna hitam. Fungsi warna hitam adalah mengatur kecerahan suatu warna. CMYK didapatkan dari penguraian tinta.

b. Warna sekunder

Merupakan hasil pencampuran warna-warna primer dengan proporsi 1:1. Misalnya warna jingga merupakan hasil campuran warna merah dengan kuning, hijau adalah campuran biru dan kuning, dan ungu adalah campuran merah dan biru.

c. Warna tersier

Merupakan campuran salah satu warna primer dengan salah satu warna sekunder. Misalnya warna jingga kekuningan didapat dari pencampuran warna kuning dan jingga.

d. Warna netral

Warna netral merupakan hasil campuran ketiga warna dasar dalam proporsi 1:1:1. Warna ini sering muncul sebagai penyeimbang warna-warna kontras di alam. Biasanya hasil campuran yang tepat akan menuju hitam.

RGB dan CMYK merupakan standar internasional warna. Perbedaan diantara kedua standar tersebut adalah bahwa RGB adalah model warna pencahayaan (*additive color mode*). Disebut warna additive karena ketika warna primernya dikombinasikan dengan intensitas full, maka akan tercipta warna putih. Sehingga RGB dipakai untuk "*input device*" seperti scanner maupun "*output device*" seperti monitor. Memiliki warna primer merah hijau dan biru. Sementara CMYK adalah

sebuah model warna berbasis pengurangan sebagian gelombang cahaya (*subtractive color mode*). Warna primernya adalah *cyan*, *magenta*, *yellow* dan *black*. Oleh karena berbasis pengurangan cahaya, maka CMYK digunakan dalam pencetakan warna seperti printer. (Terahadi, 2011)

2.2.2 Piksel (*Pixel)*

Piksel adalah unsur gambar atau representasi sebuah titik terkecil dalam sebuah gambar grafis yang dihitung per inci. Piksel sendiri berasal dari akronim bahasa Inggris *Picture Elemen* yang disingkat menjadi *Pixel*. Pada ujung tertinggi Pada ujung tertinggi skala resolusi, mesin cetak gambar berwarna dapat menghasilkan hasil cetak yang memiliki lebih dari 2.500 titik per inci denga pilihan 16 juta warna lebih untuk setiap inci, dalam istilah komputer berarti gambar seluas satu inci persegi yang bisa ditampilkan pada tingkat resolusi tersebut sepadan dengan 150 juta bit informasi. Setiap piksel adalah sampel dari gambar asli, lebih banyak sampel biasanya memberikan representasi yang lebih akurat dari aslinya. Dalam sistem citra berwarna, warna biasanya diwakili oleh tiga atau intensitas komponen seperti RGB dan CMYK.

2.2.3 Format Citra Digital

Citra Digital memiliki beberapa format yang memiliki karakteristk tersendiri. Format pada citra digital ini umumnya berdasarkan tipe dan cara kompresi yang digunakan pada citra digital tersebut.

Menurut Wijaya (2007) ada dua format citra digital yang sering dijumpai, yaitu:

a. *Bitmap* (BMP)

Merupakan format gambar yang paling umum dan merupakan format standard windows. Ukuran filenya sangat besar karena bisa mencapai ukuran *megabyte*. File ini merupakan format yang belum terkompresi dan menggunakan sistem warna RGB (*Red, Green, Blue*) di mana masing-masing warna pixel-nya terdiri dari 3 komponen R, G, dan B yang dicampur menjadi satu.

Jumlah kemungkinan warna yang dapat ditampilkan oleh suatu piksel tergantung pada satuan bit yang dimiliki gambar tersebut. Berkas bitmap warna 24 bit mempunyai tiga komponen warna yaitu RGB dengan setiap komponen tersebut terdiri 1 *byte* (8 bit). Karena tiap *byte* memiliki kombinasi 256 warna, maka jika terdapat 3 komponen warna maka mempunyai 224 atau 16.777.216 kombinasi warna. Jika sebuah citra dengan format bitmap warna 24 bit dengan ukuran 800×600 maka besarnya ukuran berkas bitmap tersebut adalah $(800 \times 600 \times 24)$ bit. (Refiandhi, 2014)

Struktur penyimpanan pada *file* bitmap terbagi menjadi tiga bagian besar seperti yang terlihat pada Tabel 2.2.

Tabel 2.2 Struktur *file* bitmap

File Header	Info Header	Palet Information	Data Bitmap
14 *byte*	40 *byte*	1024 *byte*	N *byte*

Bagian pertama berukuran 54 *byte* terletak pada bagian awal *file* yang digunakan untuk menyimpan header dari *file* bitmap. Bagian kedua berukuran 1024 *byte* berada setelah header dan digunakan untuk menyimpan informasi palet yang disusun dengan susunan RGB (*Red*, *Green*, *Blue*). Bagian ketiga adalah *byte* dari *file* BMP yang berisi informasi gambar.

b. *Joint Photographic Expert Group* (JPEG/JPG)

Format JPEG merupakan format yang paling terkenal sampai sekarang ini. Hal ini karena sifatnya yang berukuran kecil (hanya puluhan/ratusan KB saja), dan bersifat portable. Format file ini sering digunakan pada bidang fotografi untuk menyimpan file foto hasil perekaman *analog to digital converter* (ADC).

2.2.4 Kualitas Citra Hasil Enkripsi

Kualitas citra hasil enkripsi dapat diukur secara kuantitatif menggunakan besaran PSNR (*Peak Signal to Noise Ratio*). Semakin besar nilai PSNR maka citra hasil enkripsi semakin mendekati citra aslinya. Sebaliknya,

semakin kecil nilai PSNR semakin berbeda dengan citra aslinya. Persamaan untuk menghitung PSNR adalah sebagai berikut:

$$PSNR = 20 \times \log \frac{MAX_i}{\sqrt{MSE}} \quad (2.2)$$

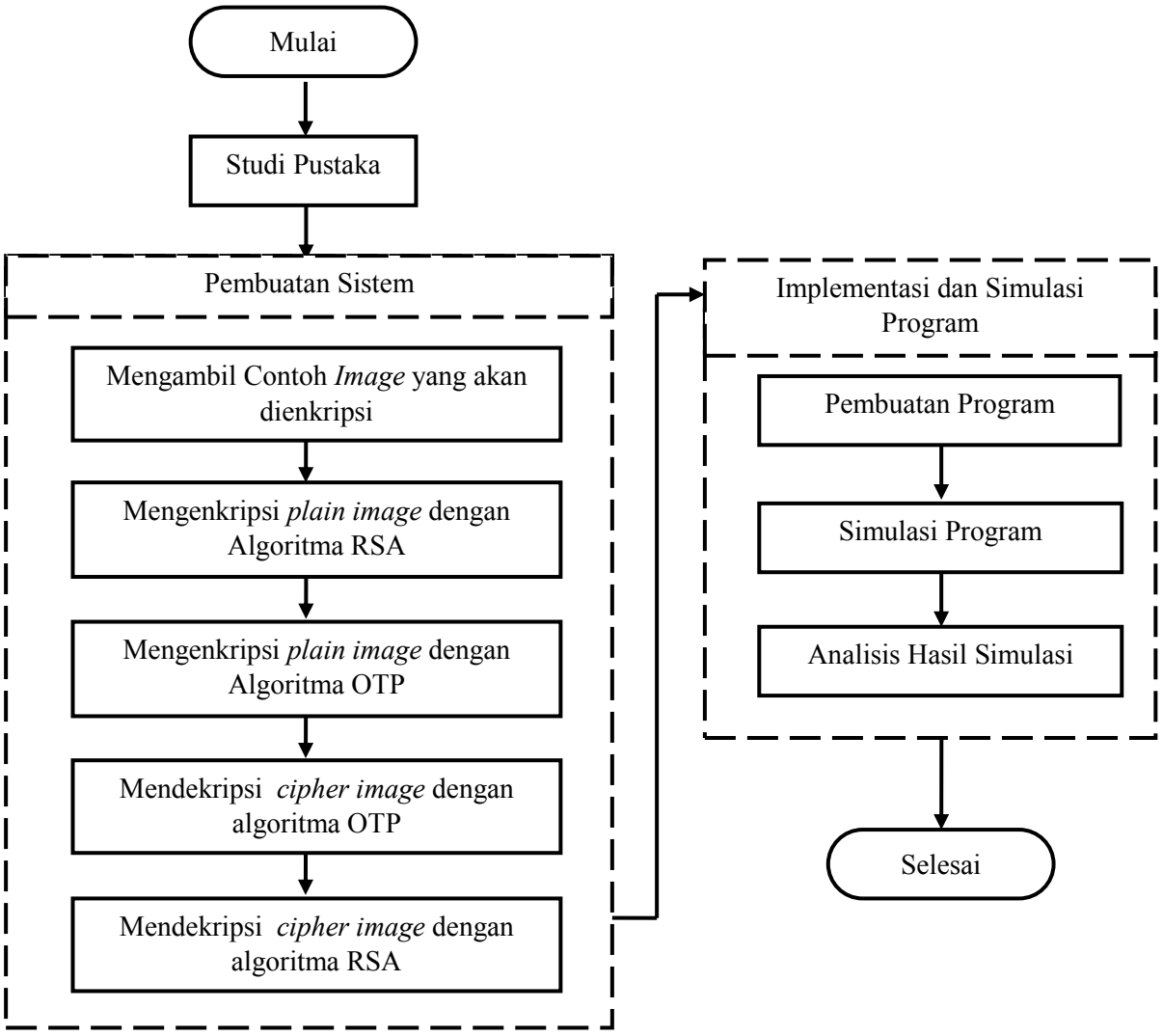
dengan MAX_i adalah nilai intensitas warna terbesar dan MSE (*Mean Square Error*) dapat dihitung dengan persamaan:

$$MSE = \frac{1}{m \times n} \sum_{i=1}^{m} \sum_{j=1}^{n} \left(C_{ij} - P_{ij} \right)^2 \quad (2.3)$$

Dalam hal ini, m dan n masing-masing adalah lebar dan tinggi citra, C dan P masing-masing adalah nilai intensitas baris ke – i dan kolom ke – j dari citra hasil enkripsi dan citra awal. PSNR mempunyai satuan decibel (dB). Ketika 2 (dua) buah citra identik, maka MSE akan bernilai 0, sehingga nilai dari PSNR tidak dapat didefenisikan.

BAB 3. METODE PENELITIAN

Dalam Bab 3 dibahas mengenai prosedur yang digunakan untuk menyelesaikan tugas akhir ini. Secara skematik, tahap-tahap yang akan dilaksanakan dalam menyelesaikan tugas akhir dapat dilihat pada Gambar 3.1



Gambar 3.1 Langkah-langkah metode penelitian

a. Studi Pustaka

Studi pustaka akan dilakukan selama pengerjaan skripsi baik saat analisis, perancangan, dan implementasi. Pada tahap studi kasus, studi pustaka dibutuhkan dalam penentuan kasus yang akan dipilih. Jenis data yang dibutuhkan dalam

penyusunan skripsi ini adalah data sekunder, yaitu data yang diperoleh dari buku-buku, serta literatur lain yang mendukung penyusunan skripsi ini. Informasi yang dijadikan referensi dalam penulisan adalah informasi yang berkaitan dengan kriptografi, khususnya kriptografi dengan menggunakan metode RSA (*Rivest Shamir Adleman*) dan OTP (*one time pad*).

b. Pembuatan Sistem

Secara garis besar penyelesaian model dengan menggunakan algoritma RSA dan OTP dibagi menjadi 2 tahap, yaitu proses enkripsi dan proses dekripsi. Proses enkripsi dilakukan melalui beberapa tahap berikut:

1) menentukan kunci publik dan kunci privat algoritma RSA;
2) mengenkripsi *plain image* dengan algoritma RSA menggunakan kunci publik sehingga menghasilkan *cipher image* 1;
3) membangkitkan kunci algoritma OTP;
4) mengenkripsi *cipher image* 1 dengan algoritma OTP sehingga menghasilkan *cipher image* 2;

Sedangkan proses dekripsi melalui langkah-langkah berikut ini:

1) mendekripsi *cipher image* 2 dengan algoritma OTP dan kunci yang sudah dibangkitkan sebelumnya sehingga menghasilkan *cipher image* 1;
2) mendekripsi *cipher image* 1 menggunakan kunci privat algoritma RSA sehingga menghasilkan *plain image*;

c. Pembuatan Program

Pada tahap pembuatan program ini akan dibuat program dengan bahasa pemrograman PHP. Merancang aplikasi merupakan tindak lanjut dari analisa data, dimana pada tahap ini dibuat contoh algoritma, baik enkripsi maupun dekripsi. Software yang akan digunakan untuk membuat program dalam skripsi ini adalah jEdit 5.1.0.

d. Simulasi Program

Setelah pembuatan program selesai, maka tahap selanjutnya adalah simulasi program tersebut. Program yang telah selesai diuji dengan menggunakan citra digital berekstensi *.bmp* dengan berbagai ukuran.

e. Analisis Hasil Simulasi

Tahap terakhir dalam pembuatan skripsi ini adalah menganalisis hasil simulasi. Pada tahap ini, akan dilakukan analisis hasil yang diperoleh dari simulasi program. Analisis dilakukan dengan membandingkan ukuran, nilai PSNR dan ketampakan visual citra digital sebelum dan sesudah proses enkripsi.