SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER DENGAN KUNCI TERENKRIPSI RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENINGKATKAN KEAMANAN CITRA DIGITAL

Disusun dan diajukan oleh :

SITTI NUR FADILLAH

D42116004

DEPARTEMEN TEKNIK INFORMATIKA

FAKULTAS TEKNIK UNIVERSITAS HASANUDDIN

MAKASSAR

2021

LEMBAR PENGESAHAN SKRIPSI

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER DENGAN KUNCI TERENKRIPSI RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENINGKATKAN KEAMANAN CITRA DIGITAL

Disusun dan diajukan oleh

SITTI NUR FADILLAH

D421 16 004

Telah dipertahankan di hadapan Panitia Ujian yang dibentuk dalam rangka penyelesaian studi Program Sarjana Program Studi Teknik Informatika Fakultas Teknik Universitas Hasanuddin

Pada tanggal 22 Juni 2021

dan dinyatakan telah memenuhi syarat kelulusan

Menyetujui

Pembimbing Utama,	Pembimbing Pendamping,
Dr. Amil Ahmad Ilham, S.T., M.IT.	**Dr.Eng. Ady Wahyudi Paundu, ST., M.T**
NIP. 19731010 199802 1 001	**NIP. 19750313 200912 1 003**

Ketua Program Studi,

Dr. Amil Ahmad Ilham, S.T., M.IT.

NIP. 19731010 199802 1 001

PERNYATAAN KEASLIAN

Yang bertanda tangan di bawah ini:

Nama : Sitti Nur Fadillah

NIM : D421 16 004

Program Studi : Teknik Informatika

Jenjang : S1

Menyatakan dengan ini bahwa karya tulisan saya berjudul:

IMPLEMENTASI ALGORITMA KRIPTOGRAFI HILL CIPHER DENGAN KUNCI TERENKRIPSI RIVEST SHAMIR ADLEMAN (RSA) UNTUK MENINGKATKAN KEAMANAN CITRA DIGITAL

Adalah karya tulisan saya sendiri, bukan merupakan pengambilan alihan tulisan orang lain dan bahwa skripsi yang saya tulis ini benar-benar merupakan hasil karya saya sendiri.

Apabila dikemudian hari terbukti atau dapat dibuktikan bahwa sebagian atau keseluruhan isi skripsi ini hasil karya orang lain, maka saya bersedia menerima sanksi atas perbuatan tersebut.

Makassar, 22 Juni 2021

Yang Menyatakan,

SITTI NUR FADILLAH

ABSTRAK

Di era digitalisasi saat ini, sebagian besar data tersimpan secara *online* di *database*. Data yang tersimpan tidak hanya yang sifatnya publik tapi juga yang bersifat pribadi. Data yang sifatnya pribadi seringkali disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan pribadi. Banyaknya penyalahgunaan tersebut menunjukkan betapa pentingnya menyembunyikan informasi data yang sifatnya pribadi dan rahasia. Teknik menyembunyikan informasi disebut dengan kriptografi.

Umumnya sebuah sistem enkripsi hanya menggunakan teknik kriptografi simetris, di mana kunci enkripsi sama dengan kunci dekripsi. Namun cara demikian memiliki banyak kelemahan, diantaranya, kerentanan keamanan dalam pengiriman kunci, serta masalah non-repudiation. Kelemahan tersebut dapat diatasi dengan penggunaan metode enkripsi hibrid yang menggabungkan teknik enkripsi simetris dengan teknik enkripsi asimetris. Salah satu contoh algoritma enkripsi simetris adalah algoritma Hill Cipher dan enkripsi asimetris adalah Rivest Shamir Adleman (RSA). Penelitian ini bertujuan untuk membangun sistem kriptografi menggunakan algoritma Hill Cipher untuk melakukan enkripsi/dekripsi citra digital dengan agoritma RSA yang di gunakan untuk melakukan proses enkripsi/dekripsi kunci Hill Cipher sebagai penunjang keamanan data.

Melalui proses evaluasi, selain melakukan uji fungsionalitas, berhasil pula diperlihatkan keunggulan metode kriptografi hibrid Hill Cipher-RSA dibandingkan dengan metode kriptografi lainnya, Hill Cipher-Elgamal dalam hal kecepatan enkripsi dan dekripsi. Proses enkripsi dan dekripsi hibrid Hill Cipher-RSA lebih cepat 8,7 % dan 6,65 % dibandingkan dengan proses yang sama pada metode hibrid Hill Cipher-Elgamal.

Kata Kunci: Kriptografi Hibrid, Hill Cipher, Rivest Shamir Adleman (RSA), Keamanan Citra Digital

ABSTRACT

In the current era of digitalization, most of the data is stored online in databases. The data stored is not only public but also private. Personal data is often misused by irresponsible parties for personal gain. The number of abuses shows how important it is to hide personal and confidential data information. The technique of hiding information is called cryptography.

Generally an encryption system only uses symmetric cryptography techniques, where the encryption key is the same as the decryption key. However, this method has many weaknesses, including security vulnerabilities in key delivery, as well as non-repudiation problems. These weaknesses can be overcome by using a hybrid encryption method that combines symmetric encryption techniques with asymmetric encryption techniques. One example of a symmetric encryption algorithm is the Hill Cipher algorithm and asymmetric encryption is Rivest Shamir Adleman (RSA). This study aims to build a cryptographic system using the Hill Cipher algorithm to encrypt/decrypt digital images with the RSA algorithm which is used to perform the Hill Cipher key encryption/decryption process to support data security.

Through the evaluation process, in addition to testing the functionality, the Hill Cipher-RSA hybrid cryptography method was also successfully demonstrated compared to another cryptographic method, Hill Cipher-Elgamal in terms of encryption and decryption speed. The Hill Cipher-RSA hybrid encryption and decryption process is 8.7% and 6.65% faster compared to the same process in the Hill Cipher-Elgamal hybrid method.

Keywords: Hybrid Cryptography, Hill Cipher, Rivest Shamir Adleman (RSA), Digital Image Security

KATA PENGANTAR

Puji dan syukur penulis panjatkan kepada Tuhan Yang Maha Esa, yang telah memberikan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan laporan tugas akhir dengan judul "Implementasi Algoritma Kriptografi Hill Cipher dengan Kunci Terenkripsi Rivest Shamir Adleman (RSA) untuk Meningkatkan Keamanan Citra Digital". Laporan tugas akhir ini merupakan salah satu syarat untuk memperoleh gelar Sarjana Strata Satu (S1) pada Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.

Dalam proses pembuatan laporan tugas akhir ini, penulis banyak mendapat bimbingan, arahan, dan bantuan dari berbagai pihak sehingga penulis dapat menyelesaikan laporan ini tepat pada waktunya. Oleh karena itu dengan segala kerendahan hati, penulis mengucapkan terima kasih sebesar-besarnya kepada:

1. Kedua orang tua penulis, Bapak Haeruddin dan Ibu Rosliati beserta keluarga atas segala doa, dukungan, semangat, pengorbanan, dan kasih sayang yang telah diberikan.
2. Bapak Dr. Ir. Amil Ahmad Ilham, ST., M.IT selaku Ketua Departemen Teknik Informatika Fakultas Teknik Univeristas Hasanuddin atas bimbingannya selama masa perkuliahan penulis dan sebagai Dosen Pembimbing I yang telah memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.

3. Bapak Dr-Eng. Ady Wahyudi Paundu, ST., M.T selaku Dosen Pembimbing II yang telah memberikan bimbingan dan masukan yang sangat bermanfaat dalam penyusunan laporan skripsi ini.
4. Seluruh Dosen dan Staf Departemen Teknik Informatika Fakultas Teknik Universitas Hasanuddin.
5. Para sahabat penulis AIROKU (Dhinda, Cici, Noni, Putri, dan Ghina) yang telah menemani selama masa perkuliahan serta selalu memberikan nasihat, dukungan, doa dan semangat selama proses perkuliahan.
6. Teman-teman angkatan Teknik Informatika 2016 selaku rekan belajar sejak dari awal hingga akhir masa perkuliahan.
7. Serta seluruh pihak yang tak sempat kami sebutkan satu persatu yang telah banyak meluangkan tenaga, waktu, dan pikiran selama penyusunan laporan skripsi ini.

Akhirnya dengan segala kerendahan hati, penulis menyadari masih banyak kesalahan dan kekurangan dalam penyusunan laporan skripsi ini baik dari isi maupun cara penyajiannya. Oleh karena itu penulis mengharapkan adanya saran dan kritik yang bersifat membangun demi kesempurnaan laporan ini. Penulis berharap semoga laporan skripsi ini dapat memberikan manfaat bagi pembaca pada umumnya dan penulis khususnya.

Makassar, Juni 2021

Penulis

DAFTAR ISI

DAFTAR TABEL

DAFTAR GAMBAR

BAB I

PENDAHULUAN

1.1 Latar Belakang

Di era digitalisasi saat ini, sebagian besar data tersimpan secara *online* di *database*. Data yang tersimpan tidak hanya yang sifatnya publik tapi juga yang bersifat pribadi. Data yang sifatnya pribadi seringkali disalahgunakan oleh pihak yang tidak bertanggung jawab untuk mendapatkan keuntungan pribadi. Gemalto, perusahaan teknologi informasi multinasional dibidang keamanan digital melaporkan bahwa pada tahun 2017 kasus pencurian data mencapai 1.162 kasus dan tahun 2018 sebanyak 945 kasus. Jumlah data yang dibobol per harinya mencapai 6,9 juta data, berdasarkan laporan pencurian data sejak 2013 hingga 2018 yang jumlahnya sebanyak 14,6 miliar. Dari jumlah data yang dicuri tersebut, hanya 4 % yang dilindungi enkripsi oleh pemiliknya.

Dari banyaknya kasus pencurian data tersebut menunjukkan betapa pentingnya menyembunyikan informasi dari data yang sifatnya pribadi dan rahasia. Teknik menyembunyikan informasi disebut dengan kriptografi. Kriptografi berasal dari bahasa yunani yang terdiri dari kata kryptos yang berarti "*hidden*, *secret*" dan graphin yang berarti "*writing*, *study*". Jadi kriptografi adalah suatu ilmu yang mempelajari tentang bagaimana menyembunyikan informasi melalui proses enkripsi.

Enkripsi citra merupakan teknik untuk melindungi kerahasiaan citra dari pengaksesan ilegal. Enkripsi di perlukan karena dalam era digital sekarang ini

citra digital mudah disimpan atau ditransmisikan melalui saluran publik seperti internet. Pengiriman citra melalui saluran publik rawan terhadap penyadapan, dan penyimpanan citra di dalam media *storage* rawan terhadap pengaksesan oleh pihak-pihak yang tidak memiliki otoritas. Enkripsi menyandikan citra (*plainimage*) ke bentuk visual lain yang tidak bermakna (*cipher-image*).

Terdapat sejumlah algoritma kriptografi diantaranya adalah Hill Cipher. Kelebihan algoritma Hill Cipher adalah *cipher* (kode) yang dihasilkan tidak dapat dipecahkan dengan menggunakan teknik analisis frekuensi. Hal ini disebabkan karena Hill Cipher tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* sehingga sangat sulit dipecahkan oleh kriptanalis apabila dilakukan hanya dengan mengetahui berkas *ciphertext* saja. Kelemahannya adalah cukup mudah dipecahkan apabila kriptanalis mengetahui kunci dan memiliki berkas *ciphertext* dan potongan berkas *plaintext* (*known-plaintext attack*).

Untuk meningkatkan keamanan data hasil enkripsi, pada penelitian ini akan diimplementasikan algoritma Hill Ciper untuk mengenkripsi data dengan kunci terenkripsi RSA (Rivest–Shamir–Adleman). RSA adalah algoritma untuk enkripsi kunci publik (*public-key encryption*). Algoritma ini adalah algoritma pertama yang diketahui paling cocok untuk menandai (*signing*) dan untuk enkripsi (*encryption*) dan salah satu penemuan besar pertama dalam kriptografi kunci publik. RSA masih digunakan secara luas dalam protokol-protokol perdagangan elektronik, dan dipercayai sangat aman karena diberikan kunci-

kunci yang cukup panjang dan penerapan-penerapannya yang sangat *up-to-date* (mutakhir).

1.2 Rumusan Masalah

Berdasarkan latar belakang diatas, maka penulis dapat merumuskan permasalahan-permasalahan yaitu :

1. Bagaimana mengimplementasikan metode kriptografi hibrid Hill Cipher dan Rivest Shamir Adleman (RSA) pada aplikasi berbasis *desktop* untuk meningkatkan keamanan citra digital?
2. Apakah performansi metode kriptografi hibrid Hill Cipher dan RSA lebih baik dibandingkan metode kriptografi hibrid Hill Cipher dan Elgamal berdasarkan parameter waktu proses?

1.3 Tujuan Penelitian

Tujuan akhir dari penelitian ini yaitu :

1. Mengimplementasikan metode kriptografi hibrid Hill Cipher dan Rivest Shamir Adleman (RSA) pada aplikasi berbasis *desktop*.
2. Menganalisa performansi metode hibrid kriptografi Hill Cipher dan Rivest Shamir Adleman (RSA) serta melakukan perbandingan dengan metode kriptografi hibrid Hill Cipher dan Elgamal dengan parameter waktu proses.

1.4 Batasan Penelitian

Batasan masalah pada penelitian ini adalah :

1. Matriks kunci Hill Cipher menggunakan matriks ordo 3x3.
2. Data yang dienkripsi berupa gambar dengan format .png dengan ukuran 256x256 dan 512x512 pixel.

1.5 Manfaat Penelitian

Dengan dilakukannya penelitian ini, diharapkan manfaat yang didapatkan antara lain:

1. Dengan mengimplementasikan algoritma Hill Cipher dengan kunci terenkripsi RSA, pengguna dapat memberikan perlindungan lebih maksimal terhadap keamanan data dan diharapkan proses dekripsi secara ilegal semakin sulit.
2. Sebagai bahan referensi untuk penelitian-penelitian selanjutnya.

1.6 Sistematika Penulisan

BAB I PENDAHULUAN

Bab ini berisi latar belakang masalah, rumusan masalah, tujuan penelitian, manfaat penelitian, batasan masalah, sistematika penulisan.

BAB II LANDASAN TEORI

Pada bab ini akan dijelaskan teori-teori yang menunjang percobaan yang dilakukan.

BAB III METODOLOGI PENELITIAN

Bab ini berisi analisis kebutuhan sistem, perancangan sistem, dan skenario pengujian.

BAB IV HASIL PENELITIAN DAN PEMBAHASAN

Bab ini berisi hasil penelitian dan pembahasan.

BAB V PENUTUP

Bab ini berisi kesimpulan hasil penelitian dan saran.

BAB II

LANDASAN TEORI

2.1 Kriptografi

2.1.1 Definisi Kriptografi

Kriptografi berasal dari bahasa Yunani, menurut bahasa dibagi menjadi dua *kryptos* dan *graphein*, *kryptos* berarti *secret* (rahasia) dan *graphein* berarti *writing* (tulisan). Kriptografi merupakan ilmu dan seni untuk menjaga keamanan pesan ketika dikirim dari sebuah sumber informasi ke suatu tujuan pengiriman informasi (Konheim, 2007). Sistem kriptografi terdiri dari dari 5 bagian yaitu:

1) *Plaintex*t: pesan asli berupa kumpulan karakter yang dapat berupa abjad, angka atau simbol tertentu yang dapat dibaca. *Plaintext* adalah masukan bagi algoritma enkripsi. Istilah teks asli akan digunakan sebagai padanan kata *plaintext* untuk selanjutnya.
2) *Secret Key*: suatu variabel terhadap teks asli yang menjadi penentu hasil dari algoritma enkripsi. Bersama dengan teks asli, *secret key* menjadi masukan bagi algoritma enkripsi. Istilah kunci rahasia akan digunakan sebagai padanan kata *secret key* untuk selanjutnya.
3) *Ciphertext*: hasil dari algoritma enkripsi yang tidak dapat secara langsung. Tingkat kualitas *Ciphertext* diukur dari tingkat kesulitan membacanya. Istilah teks sandi akan digunkan sebagai padanan kata *ciphertext* untuk selanjutnya.

4) Algoritma Enkripsi: memiliki tugas utama melakukan perubahan terhadap teks asli menggunakan kunci rahasia sehingga menghasilkan teks sandi yang sulit dibaca.
5) Algoritma Dekripsi: bertugas memulihkan kembali teks sandi menjadi teks asli menggunaan kunci rahasia. Kunci rahasia yang digunakan untuk algoritma dekripsi dapat saja sama ataupun berbeda dengan kunci rahasia yang digunakan untuk algoritma enkripsi tergantung algoritma kriptografi yang digunakan (Sadikin, 2012).

2.1.2 Jenis-Jenis Algoritma Kriptografi

Berdasarkan dari kunci yang digunakannya, algoritma kriptografi di bagi menjadi dua bagian, yaitu algoritma simetris dan algoritma asimetris.

1. Algoritma Simetris

Algoritma Simetris adalah algoritma di mana kunci untuk proses enkripsi sama dengan dan proses dekripsi, misalnya permutasi, subtitusi, Hill Cipher (Konheim, 2007). Sehingga algoritma ini juga sering disebut algoritma klasik. Algoritma ini sudah ada lebih dari 4000 tahun yang lalu. Untuk menggunakan algoritma ini, penerima pesan harus tahu kunci yang digunakan pengirim untuk mengamankan pesan agar dapat melakukan dekripsi sehingga pesan dapat dibaca oleh penerima (Prayoga, 2018).

Jenis kriptografi ini menawarkan *processing time* yang baik, namun konsekuensi yang harus dibayar adalah kunci yang dipakai harus dijaga kerahasiaannya oleh pengirim dan penerima.

2. Algoritma Asimetris

Algoritma kriptografi asimetris adalah algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsinya. Kelebihan algoritma ini adalah kunci untuk enkripsi dibuat umum (*public key*) atau dapat diketahui oleh setiap orang, tapi kunci untuk dekripsi hanya diketahui oleh orang yang berwenang mengetahui data yang disandikan atau sering disebut kunci pribadi (*private key*) (Nahwi, 2016).

Teknik enkripsi Asimetris ini jauh lebih lambat ketimbang enkripsi dengan kunci simetris. Oleh karena itu, biasanya bukanlah pesan itu sendiri yang disandikan dengan kunci asimetris, namun hanya kunci simetrislah yang disandikan dengan kunci asimetris. Sedangkan pesannya dikirim setelah disandikan dengan kunci simetris tadi. Contoh algoritma terkenal yang menggunakan kunci Asimetris adalah RSA (Rivest Shamir Adleman) (Alasi, 2007).

2.2 Sistem Kriptografi Hibrida

Kriptografi hibrida merupakan salah satu metode kriptografi yang bekerja dengan menggabungkan kedua algoritma simetris dan asimetris untuk mengamankan pesan. Pada sistem hibrida ini , enkripsi dan dekripsi dari pesan menggunakan algoritma kriptografi kunci simetris, sedangkan algoritma kunci

simetris dienkripsi atau dideksipsi dengan kriptografi kunci publik (algoritma asimetris).

Kunci simetris telah dibuat oleh salah satu pihak dan mengenkripsi pesan dengan kunci itu. Kunci simetris telah dienkripsi dengan kunci publik penerima, dan kunci simetris akan dikirim bersama dengan pesan terenkripsi. Penerima awalnya mendekripsi kunci simetris dengan kunci privatnya, kemudian mendekripsi pesan dengan kunci simetris (Rachmawati dkk., 2018).

2.3 Algoritma Hill Cipher

2.3.1 Definisi Algoritma Hill Cipher

Hill Cipher ditemukan pada tahun 1929 oleh Lester S. Hill. Teknik kriptografi ini diciptakan dengan maksud untuk dapat menciptakan *cipher* (kode) yang tidak dapat dipecahkan menggunakan teknik analisis frekuensi.

Hill Cipher tidak mengganti setiap abjad yang sama pada *plaintext* dengan abjad lainnya yang sama pada *ciphertext* karena menggunakan perkalian matriks pada dasar enkripsi dan dekripsinya. Oleh karena itu, Hill Cipher termasuk dalam salah satu kriptosistem polialfabetik.

Berdasar jenis kunci yang dipakai, kriptografi Hill Cipher termasuk ke dalam Algoritma Simetris (*Symmetric Algorithms*), karena algoritma ini menggunakan suatu kunci yang sama untuk proses enkripsi dan dekripsi pesan (Supiyanto, 2015).

Proses enkripsi pada Hill Cipher dilakukan per blok *plaintext*. Ukuran blok tersebut sama dengan ukuran matriks kunci. Sebelum

membagi teks menjadi deretan blok-blok, *plaintext* terlebih dahulu dikonversi menjadi angka, masing-masing sehingga A=0, B=1, hingga Z=25 seperti pada Tabel 2. Secara matematis, proses enkripsi pada Hill Cipher adalah:

$$C = K.P \ mod \ 256 \qquad (2.1)$$

keterangan :

C = *Cipherimage*

P = Matriks Gambar

K = Matriks Kunci.

Tabel 2 Nilai Konversi *Plaintext*

A	B	C	D	E	F	G	H	I	J	K	L	M
0	1	2	3	4	5	6	7	8	9	10	11	12
N	O	P	Q	R	S	T	U	V	W	X	Y	Z
13	14	15	16	17	18	19	20	21	22	23	24	25

Proses dekripsi pada Hill Cipher pada dasarnya sama dengan proses enkripsinya. Namun matriks kunci harus dibalik (*inverse*) terlebih dahulu. Secara matematis, Rumus matematika dari dekripsi algoritma Hill Cipher adalah (Aldo dan Hakim, 2018):

$$K^{-1} = \frac{1}{DetA} * \text{Adj K} \qquad (2.2)$$

di mana : Det A = Determinan matriks A

Adj K = Adjoint matriks kunci

K^{-1} = *Inverse* Matriks.

Bila *inverse* matriks kunci pecahan, konversikan matriks kunci menjadi integer (bilangan bulat). Langkah terakhir hitung *plainimage* atau gambar asli dengan rumus:

$$P = K^{-1}.C \ mod \ 256 \quad (2.3)$$

keterangan :

P = *Plainimage*

K^{-1} = *inverse* matriks kunci

C = Matriks *Cipherimage*.

2.3.2 Enkripsi Algoritma Hill Cipher

Langkah-langkah untuk proses enkripsi *plaintext* dengan Hill Cipher adalah sebagai berikut:

1. Pilih suatu matriks kunci K yang berupa matriks bujur sangkar yang dipakai sebagai kunci.
2. Kelompokkan barisan angka ke dalam beberapa blok vektor P yang panjangnya sama dengan ukuran matriks K.
3. Hitung C = K . P (mod 256) untuk tiap vektor P.

2.3.3 Dekripsi Algoritma Hill Cipher

Langkah-langkah untuk proses dekripsi *ciphertext* dengan Hill Cipher adalah sebagai berikut:

1. Hitung nilai *inverse* dari kunci K.
2. Kelompokkan barisan angka ke dalam beberapa blok vektor C yang panjangnya sama dengan ukuran matriks K^{-1}.
3. Hitung P = K^{-1}. C (mod 256) untuk tiap vektor C.

2.4 Algoritma Rivest Shamir Adleman (RSA)

2.4.1 Definisi Algoritma RSA

Sandi RSA merupakan algoritma kriptografi kunci publik (asimetris). Ditemukan pertama kali pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Len Adleman. Nama RSA sendiri diambil dari ketiga penemunya tersebut. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci rahasia. RSA mendasarkan proses enkripsi dan dekripsinya pada konsep bilangan prima dan aritmetika modulo. Baik kunci enkripsi maupun dekripsi keduanya merupakan bilangan bulat. Kunci enkripsi tidak dirahasiakan dan diberikan kepada umum (sehingga disebut dengan kunci publik), namun kunci untuk dekripsi bersifat rahasia (kunci privat).

Untuk menemukan kunci dekripsi, dilakukan dengan memfaktorkan suatu bilangan bulat menjadi faktor-faktor primanya. Kenyataannya, memfaktorkan bilangan bulat menjadi faktor primanya bukanlah pekerjaan yang mudah. Karena belum ditemukan algoritma yang efisien untuk melakukan pemfaktoran. Cara yang bisa digunakan dalam pemfaktoran adalah dengan menggunakan pohon faktor. Jika semakin besar bilangan yang akan difaktorkan, maka semakin lama waktu yang dibutuhkan. Jadi semakin besar bilangan yang difaktorkan, semakin sulit pemfaktorannya, semakin kuat pula algoritma RSA (Ginting, Isnanto, dan Windasari, 2015).

Skema RSA sendiri mengadopsi dari skema *block cipher*, di mana sebelum dilakukan enkripsi, *plaintext* yang ada dibagi – bagi menjadi blok

– blok dengan panjang yang sama, di mana *plaintext* dan *ciphertext*-nya berupa integer (bilangan bulat) antara 1 hingga n, di mana n berukuran biasanya sebesar 1024 bit, dan panjang bloknya sendiri berukuran lebih kecil atau sama dengan log(n) +1 dengan basis 2 (Retno, 2017).

2.4.2 Proses Pembangkitan Kunci Algoritma RSA

Algoritma RSA menggunakan dua kunci berbeda untuk proses enkripsi dan dekripsi teks yaitu kunci publik dan kunci privat. Kunci publik dan kunci privat merupakan bilangan bilangan bulat prima. Dalam menentukan dua bilangan prima sebagai kunci adalah bilangan prima yang besar. Karena pemfaktoran bilangan dari dua bilangan prima yang besar sangat sulit, sehingga keamanan teks lebih terjamin.

Pasangan kunci adalah elemen penting dari algoritma RSA. Berikut ini langkah-langkah dalam membangkitkan kunci publik dan kunci privat algoritma RSA.

1. Pilih dua bilangan prima acak, p dan q
2. Hitung $n = p.q$
3. Hitung $\varphi(n) = (p-1)(q-1)$
4. Pilih kunci publik e, yang relatif prima terhadap $\varphi(n)$.
5. Bangkitkan kunci pribadi dengan menggunakan $e.d = 1 \ mod \ \varphi(n)$

Hasil dari algoritma tersebut akan menghasilkan dua kunci, yaitu kunci publik (e, n) dan kunci pribadi (d, n).

2.4.3 Enkripsi Algoritma RSA

Algoritma enkripsi memiliki dua masukan yaitu pesan (*plaintext*) dan kunci rahasia. Proses enkripsi RSA terlebih dahulu pesan dibagi kedalam blok-blok numerik yang lebih kecil dari n (dengan data biner, dipilih pangkat terbesar dari 2 yang kurang dari n). Jadi jika p dan q bilangan prima 100 digit, maka n akan memiliki sekitar 200 buah digit dari setiap blok pesan m, seharusnya kurang dari 200 digit panjangnya. Pesan yang terenkripsi (c), akan tersusun dari blok-blok (c) yang hampir sama panjangnya. Rumus enkripsinya adalah (Ginting dkk., 2015):

$$C = M^e \ mod \ n \tag{2.4}$$

keterangan :

C = *Ciphertext*

M = Pesan / *Plaintext*

e = kunci publik

d = kunci privat

n = modulo pembagi.

2.4.4 Dekripsi Algoritma RSA

Algoritma enkripsi memiliki dua masukan yaitu pesan rahasia (*ciphertext*) dan kunci rahasia. Proses dekripsi RSA terlebih dahulu pesan dibagi kedalam blok-blok numerik yang lebih kecil dari n (dengan data biner, dipilih pangkat terbesar dari 2 yang kurang dari n). Jadi jika p dan q bilangan prima 100 digit, maka n akan memiliki sekitar 200 buah digit dari setiap blok pesan m, seharusnya kurang dari 200 digit panjangnya. Pesan

(c), akan tersusun dari blok-blok (c) yang hampir sama panjangnya. Rumus dekripsinya adalah: (Ginting dkk., 2015)

$$M = C^d \ mod \ n \qquad (2.5)$$

keterangan :

C = *Ciphertext*

M = Pesan / *Plaintext*

e = kunci publik

d = kunci privat

n = modulo pembagi.

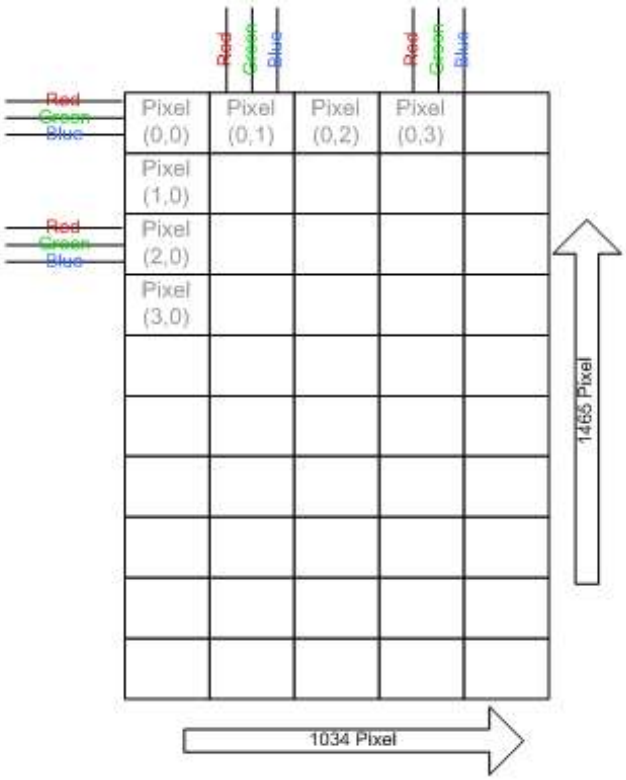
2.5 Citra Digital

Citra adalah representasi (gambaran), kemiripan atau imitasi dari suatu objek. Citra terbagi menjadi dua yaitu citra analog dan citra digital. Citra analog adalah citra yang bersifat kontiniu, seperti gambar pada monitor televisi, foto sinar-X, foto yang tercetak di kertas foto, foto lukisan dan foto pemandangan alam. Citra digital adalah citra yang dapat diolah oleh komputer (Manik, 2017).

Agar dapat diolah dengan komputer digital, maka suatu citra harus direpresentasikan secara numerik dengan nilai-nilai diskrit. Representasi citra dari fungsi kontinu menjadi nilai-nilai diskrit disebut digitalisasi. Citra yang dihasilkan inilah yang disebut citra digital (Siahaan dan Widodo, 2017).

Citra memiliki beberapa jenis format yaitu JPG, PNG, Bitmap, GIF dan lain-lain. Citra digital dapat dicontohkan dan dipetakan sebagai suatu gabungan titik-titik atau elemen gambar (*pixel*), serta citra mempunyai ukuran panjang dan lebar tiap format gambar tersebut. Adapun gambaran citra digital yang

mempunyai ukuran panjang dan lebar pertiap *pixel* nya dapat dilihat pada Gambar 2.3 (Manik, 2017).



Gambar 2.3 Citra Digital dalam *Pixel*

2.5.1 Citra Digital PNG (*Portable Network Graphics*)

Format PNG (dilafalkan "PING") dirancang untuk menggantikan format lama GIF, dan mengembangkan format TIFF. PNG (*Portable Network Graphics*) adalah salah satu format penyimpanan citra yang menggunakan metode pemadatan yang tidak menghilangkan bagian dari citra tersebut (*lossless compression*). Untuk keperluan pengolahan citra, meskipun format PNG bisa dijadikan alternatif selama proses pengolahan citra, karena format ini selain tidak menghilangkan bagian dari citra yang sedang diolah (sehingga penyimpanan berulang-ulang dari citra tidak akan

menurunkan kualitas citra) PNG (Format berkas grafik yang didukung oleh beberapa *web browser*.

PNG mendukung transparansi gambar seperti GIF, format PNG tidak memiliki hak paten dan dibaca dan ditulis secara bebas oleh pengembang *software* dan *webmaster*. PNG tidak hanya dapat disimpan sebagai 8 bit, tetapi juga 24 bit dan mencapai 64 bit. PNG memiliki level dukungan transparansi yang lebih tinggi. Kelebihan lain dari PNG dibandingkan GIF secara jelas adalah ukuran PNG yang 20 % lebih kecil dari citra GIF (Bither, 2000).