Pembangkitan Kunci RSA Menggunakan Citra Digital

Ilham Fatoni 13504121
Jurusan Teknik Informatika ITB, Bandung 40132, email: if14121@students.if.itb.ac.id

Abstrak – *Dari sekian banyak algoritma kunci-publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Selama ini, baik kunci publik maupun kunci privat adalah sebuah angka. Hal ini bisa dikembangkan dengan menggunakan suatu citra digital. Dengan citra digital, suatu kunci adalah representasi digital dari citra tersebut. Dengan demikian, kunci enkripsi akan merupakan representasi digital dari suatu citra yang disisipi watermark, sedangkan kunci dekripsi merupakan citra yang sudah disisipi watermark berupa digit hasil perhitungan kunci dekripsi dari kunci enkripsi.*

Kata Kunci*: RSA, Watermarking, Citra Digital.*

1. PENDAHULUAN

Kriptografi kunci-publik memungkinkan pengguna berkomunikasi secara aman tanpa perlu berbagi kunci rahasia, sebab kunci untuk enkripsi diumumkan kepada publik sehingga dapat diketahui oleh siapapun, sementara kunci untuk dekripsi hanya diketahui oleh penerima pesan. Siapapun dapat mengirim pesan yang dienkripsi dengan kunci publik tersebut, tetapi hanya penerima pesan yang dapat mendekripsi pesan karena hanya ia yang mengetahui kunci privatnya sendiri. Ini berlawanan dengan kriptografi kunci-simetri yang hanya mempunyai satu kunci.

Keuntungan kriptografi kunci-publik ada dua. Pertama, tidak ada kebutuhan untuk mendisitribusikan kunci privat sebagaimana pada kriptografi kunci-simetri. Kunci publik dapat dikirim ke penerima melalui saluran yang sama dengan saluran yang digunakan untuk mengirim pesan. Perhatikan bahwa saluran untuk mengirim pesan umumnya tidak aman. Kedua, jumlah kunci tidak dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang tidak perlu kunci rahasia sebanyak orang tersebut, cukup membuat dua buah kunci, yaitu kunci publik bagi para responden untuk mengenkripsi pesan, dan kunci privat untuk mendekripsi pesan. Berbeda dengan kriptografi kunci-simetri dimana jumlah kunci yang dibuat adalah sebanyak jumlah pihak yang diajak berkorespondensi.

Kriptografi kunci-publik berkembang menjadi besar dan menjadi revolusi baru dalam sejarah kriptografi. Tidak seperti seperti kriptografi kunci-simetri yang didasarkan pada permutasi dan subtitusi, kriptografi kunci-publik didasarkan pada fungsi matematika. Jika kekuatan kriptografi kunci simetri terletak pada panjang kuncinya yang membutuhkan usaha sangat besar untuk menemukan kunci, maka kriptografi kunci publik kekuatannya terletak pada sulitnya memecahkan masalah matematis seperti pemfaktoran dan logaritma diskrit. Kriptografi kunci-publik mempunyai aplikasi yang lebih luas daripada kriptografi kunci-simetri.

Aplikasi kriptografi kunci-publik dapat dibagi menjadi 3 kategori :

1. Kerahasiaan data
   Seperti pada kriptografi kunci simetri, kriptografi kunci publik dapat digunakan untuk menjaga kerahasiaan data melalui mekenisme enkripsi dan dekripsi. Contoh algoritma untuk aplikasi ini adalah RSA, Knapsack, Rabin, ElGamal, ECC.
2. Tanda-tangan Digital
   Tanda-tangan digital dengan menggunakan algoritma kriptografi kunci-publik dapat digunakan untuk membuktikan otentikasi pesan maupun otentikasi pengirim. Contoh algoritmanya untuk aplikasi ini adalah RSA, DSA, dan ElGamal.
3. Pertukaran Kunci
   Algoritma kriptografi kunci-publik dapat digunakan untuk pengiriman kunci simetri. Contoh algoritmanya adalah RSA dan Diffie-Hellman.

Beberapa algoritma kriptografi kunci-publik dapat digunakan untuk ketiga macam kategori aplikasi, misalnya RSA. [1]

2. RSA

Dari sekian banyak algoritma kriptografi kunci-publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman. Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh kunci privat. Selama pemfaktoran bilangan besar menjadi faktor-faktor prima belum ditemukan algoritma yang mangkus, maka selama itu pula keamanan algoritma RSA tetap terjamin.

Algoritma RSA memiliki besaran-besaran sebagai berikut :

1.	p dan q bilangan prima	(rahasia)
2.	n = p . q	(tidak rahasia)
3.	φ(n) = (p-1)(q-1)	(rahasia)
4.	e (kunci enkripsi)	(tidak rahasia)
5.	d (kunci dekripsi)	(rahasia)
6.	m (plainteks)	(rahasia)
7.	c (cipherteks)	(tidak rahasia)

Algoritma Membangkitkan Pasangan Kunci

1. Pilih dua buah bilangan prima sembarang, p dan q.
2. Hitung n = p.q (sebaiknya p≠q, sebab jika p=q maka n = p^2 sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung ϕ(n) = (p-1)(q-1).
4. Pilih kunci publik, e, yang relatif prima terhadap ϕ(n)
5. Bangkitkan kunci privat dengan menggunakan persamaan e.d ≡ 1 (mod ϕ(n)). Perhatikan bahwa e.d ≡ 1 (mod ϕ(n)) ekivalen dengan e.d = 1 + k ϕ(n), sehingga secara sederhana d dapat dihitung dengan

$$d = \frac{1 + k\phi n}{e}$$

Hasil dari algoritma di atas :

- Kunci publik adalah pasangan (e,n)
- Kunci privat adalah pasangan (d,n)

Catatan : n tidak bersifat rahasia, sebab ia diperlukan pada perhitungan enkripsi/dekripsi.

Selama ini, baik kunci publik maupun kunci privat adalah sebuah angka. Hal ini bisa dikembangkan dengan menggunakan suatu citra digital. Dengan demikian, pasangan bilangan prima merupakan representasi digital dari dua buah citra. Lalu kunci enkripsi e disisipkan menjadi watermark bagi citra yang satu, sedangkan kunci dekripsi d disisipkan menjadi watermark bagi citra lainnya.

Digital Watermarking adalah teknik untuk menyisipkan informasi tertentu ke dalam data digital yang disebut watermark. Penyisipan watermark dilakukan sedemikian rupa sehingga watrermark tidak merusak data digital yang dilindungi. Selain itu watermark yang telah disisipkan tidak dapat dipersepsi oleh indra manusia, namun ia dapat dideteksi oleh komputer dengan menggunakan kunci yang benar. Waternark yang telah disisipkan tidak dapat dihapus dari dalam data digital, sehingga bila data digital ber-watermark disebar dan digandakan, maka otomatis waternark di dalamnya ikut terbawa. Watermark di dalam data digital dapat dideteksi atau diekstraksi kembali.

Watermarking merupakan aplikasi dari steganografi, namun ada perbedaan diantaranya keduanya. Jika pada steganografi pesan rahasia disembunyikan didalam media penampung dimana media penampung tersebut tidak berarti apa-apa (hanya sebagai pembawa), maka pada watermarking justru media penampung tersebut dilindungi kepemilikannya dengan pemberian label hak cipta (watermark). Selain itu, jika pada steganografi kekokohan (robustness) data tidak terlalu penting, maka pada watermarking kekokohan watermark merupakan properti utama sebab watermark tidak boleh rusak atau hilang meskipun media penampung dimanipulasi.

Suatu teknik watermarking yang bagus harus memenuhi persyaratan berikut :

1. Impercepbility: keberadaan watermark tidak dapat dipersepsi oleh indra visual. Hal ini bertujuan untuk menghindari gangguan pengamatan visual.
2. Key Uniqueness: kunci yang berbeda seharusnya menghasilkan watermark yang berbeda. Ini berarti penggunaan kunci yang salah dapat menyebabkan hasil ekstraksi/deteksi watermark yang salah pula.
3. Noninvertibility: secara komputasi sangat sukar menemukan watermark bila diketahui citra hanya citra ber-watermark saja.
4. Image dependency: satu kunci menghasilkan sebuah watermark tunggal, tetapi watermark bergantung pada isi citra.
5. Robustness: watermark seharusnya tetap kokoh terhadap berbagai serangan yang dilakukan pada citra ber-watermark.

Penyisipan watermark dapat dilakukan dalam dua ranah, yaitu ranah spasial dan ranah transform. Keduanya melahirkan dua macam metode watermarking, yaitu metode spasial dan metode transform. Penyisipan dalam domain spasial berarti menyisipkan watermark secara langsung ke dalam pixel citra. Keuntungan cara ini adalah murah (cepat) tetapi umumnya waternark tidak kokoh terhadap manipulasi pada citra. [1]

Keokohan waternak diperoleh jika penyisipan waternark dilakukan dalam ranah transform, artinya watermark disisipkan ke dalam koefisian transformasi. Umumnya yang menjadi ranah transform adalah ranah frekuensi dan ranah transformasi yang digunakan misalnya DFT (Discrete Fourier Transform), DCT (Discrete Cosine Transform), DWT (Discrete Wavelet Transform).[2]

3. PEMBANGKITAN KUNCI RSA

MENGGUNAKAN CITRA

Pembangkitan kunci RSA menggunakan citra digital sesuai dengan algoritma pembangkitan kunci adalah :

1. Memilih dua bilangan prima sembarang, yakni dua buah citra, lalu ambil representasi digital-nya sebagai bilangan prima. Contoh

Dua buah Citra :

Citra A : 

Representasi digital :

[23 115 51 85 76 185 40 55 248 0 10 23 02 72 52 21 51 163 85 49 24 0 101 87 51 133 22 32 0 203 184 101 154 158 255 227 114 25 232 48 24 33 17 21 19 71 21 81 112 147 17 22 42 45 66 199 68 41 54 12 61 67 28 58 49 193 57 21 42 45 21 0 75]

p =
2311551857618540552480102302725221511638549
2401018751133223202031841011541582552271142
5232482433172119712181112147172242456619968
4154126167285849193572142452107 5

Citra B : 

Representasi digital :

[22 61 93 88 97 36 64 117 154 234 89 221 68 68 226 207 111 71 16 56 15 92 39 64 85 218 217 32 242 16 21 41 45 12 66 78 99 245 136 161 57 72 46 236 32 16 0 22 42 42 11 22 32 31 177 0 170 52 52 166 96 61 55 82 20 51 84 130 73 121 65]

q =
2261938897366411715423489221686822620711171
1656159239648521821732242162141451266789924
5136161577246236321602242421122323117701705
2521669661558220518413073121 65

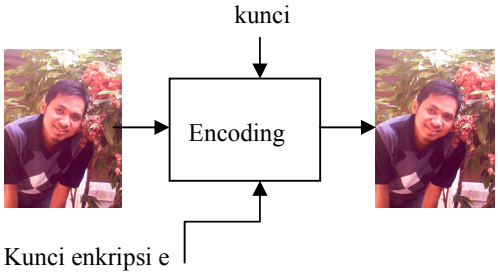
Catatan : jika representasi bukan merupakan bilangan prima, maka digunakan bilangan prima terdekat.

2. Hitung n = p.q
3. Hitung ϕ(n) = (p-1)(q-1).
4. Pilih kunci publik, e, yang relatif prima terhadap ϕ(n).
   Didapatkan e = 101
5. Bangkitkan kunci privat dengan menggunakan persamaan

$$d = \frac{1 + k\phi n}{e}$$

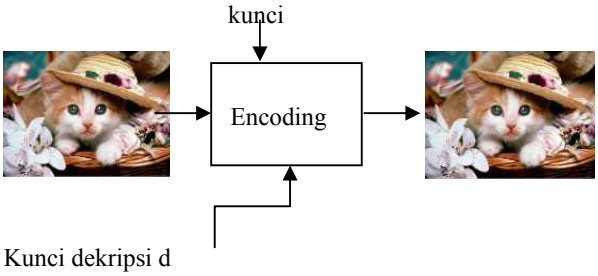
Didapatkan d =
9440193102483958495729038290583475209359477096485 7u203957823957489270958390759023756934859234529058293859485249398294349248028094783584958349603483860934860948569868393601

6. Lalu, kunci enkripsi e sebagai watermark disisipkan ke citra A, penyisipan dilakukan dengan metode dalam ranah transform, yakni menggunakan Discrete Fourier Transform (DFT).

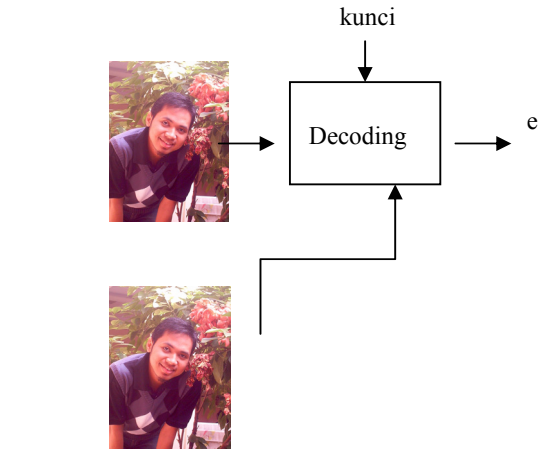


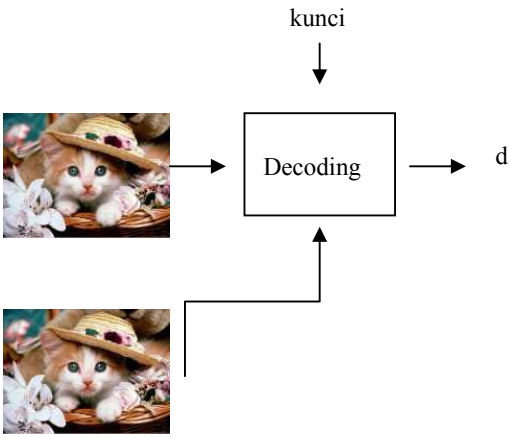
Citra keluaran tidak akan terlihat berbeda karena menggunakan invisible watermark.

7. Kemudian kunci dekripsi d disisipkan sebagai watermark ke citra B



Maka, untuk mendapatkan baik kunci enkripsi e maupun kunci dekripsi d sebagai berikut :





Jenis watermarking ini adalah invisible watermarking karena baik citra masukan maupun hasil watermark keduanya terlihat sama seolah tidak terjadi perbedaan. Hal ini sangat menguntungkan karena jika outsider melihat citra yang digunakan, tetap saja tidak bisa dijadikan kunci karena tidak memiliki watermark.

4. KESIMPULAN

Pembangkitan kunci RSA menggunakan citra digital memiliki kelebihan dan kekurangan yang sangat menonjol , yakni

Kelebihan

1. Tingkat kesulitan memecahkan kunci lebih tinggi karena untuk menemukan kunci harus menemukan kunci watermarking terlebih dahulu.
2. Walaupun citra untuk dekripsi telah diketahui, tetap tidak akan bisa digunakan untuk dekripsi karena citra tersebut harus memiliki watermark kunci dekripsi d.
3. Visibilitas kunci lebih mudah fleksibel karena sesuai dengan keinginan pemubuat bukan merupakan rangkaian bit yang tidak bermakna.
4. Memenuhi seluruh prinsip baik algoritma kunci-publik maupun watermarking

Kekurangan

1. Diperlukan perlakuan khusus jika representasi digital dari citra masukan bukan bilangan prima, yakni dengan mencari bilangan prima terdekat dengan representasi digital tersebut. Kompleksitas untuk hal ini termasuk tinggi.
2. Dalam hal kompleksitas lebih tinggi karena harus memproses citra terlebih dahulu untuk memperoleh representasi digital.

DAFTAR REFERENSI

[1] Munir, Rinaldi, *Kriptografi*, Institut Teknologi Bandung, 2006.

[3] Gonzales, Rafael C., *Digital Image Processing Second Edition,* Pearson Education, Inc, 2002.