# Studi Pembangkitan Kunci pada RSA dengan Menggunakan Sidik Jari

Amir Muntaha – NIM : 13505041

*Program Studi Teknik Informatika*
*Sekolah Teknik Elektro dan Informatika*
*Institut Teknologi Bandung*
*Jl. Ganesha 10, Bandung*
E-mail : if15041@students.if.itb.ac.id

## Abstrak

Dari beberapa algoritma kunci-publik yang pernah dibuat, algoritma yang paling sering digunakan adalah algoritma RSA. 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. Kedua, Kedua, jumlah kunci tidak dapat ditekan. Untuk berkomunikasi secara rahasia dengan banyak orang tidak diperlukan kunci rahasia sebanyak orang tersebut, cukup dengan dibuat dua buah kunci, yaitu kunci public bagi para responden untuk mengenkripsi pesan dan kunci privat untuk mendeskripsinya.

Namun, dalam RSA kunci publik maupun kunci privat adalah sebuah angka. Karena angka itu adalah sesuatu yang mudah dilupakan oleh manusia, maka orang yang mempunyai kunci privat tersebut biasanya menyimpanya pada sebuah file. Karena kunci privat tersebut disimpan di sebuah file, maka ada peluang bagi orang lain untuk mengambil kunci privat tersebut dan menyalah gunakanya. Maka, diperlukan metode lain untuk menjamin keamanan dari kunci public tersebut.

Makalah ini bertujuan untuk melakukan studi mengenai pembangkitan kunci privat pada RSA dengan menggunakan sidik jari yang dipunyai oleh pemilik kunci privat yang seharusnya.

Hal ini cukup berprospek dalam pengembangan selanjutnya. Dengan adanya kunci privat yang sifatnya sangat unik yang dibangkitkan dengan menggunakan sidik jari, maka tidak perlu lagi kita harus mengingat atau menyimpan kunci privat tersebut. Jadi, kemungkinan untuk kehilangan dan pencurian kunci privat akan lebih kecil, karena tidak perlu diingat maupun disimpan.

**Kata kunci**: RSA, kunci publik, kunci privat, *ciphertext*, teks asli, enkripsi, dekripsi.

## 1. Pendahuluan

Pengiriman data dan penyimpanan data melalui media elektronik memerlukan suatu proses yang dapat menjamin keamanan dan keutuhan dari data yang dikirimkan tersebut. Data tersebut harus tetap rahasia selama pengiriman dan harus tetap utuh pada saat penerimaan di tujuan. Untuk memenuhi hal tersebut, dilakukan proses penyandian (enkripsi dan dekripsi) terhadap data yang akan dikirimkan. Enkripsi dilakukan pada saat pengiriman dengan cara mengubah data asli menjadi data rahasia sedangkan dekripsi dilakukan pada saat penerimaan dengan cara mengubah data rahasia menjadi data asli. Jadi data yang dikirimkan selama proses pengiriman

adalah data rahasia, sehingga data asli tidak dapat diketahui oleh pihak yang tidak berkepentingan. Data asli hanya dapat diketahui oleh penerima dengan menggunakan kunci rahasia.

Algoritma penyandian data yang mulai sering digunakan baru-baru ini adalah kriptografi kunci-publik. Kriptogrrafi kunci publik ini memungkinkan pengguna untuk 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 algoritma 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 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.

**2. RSA**

RSA adalah salah satu dari algoritma kunci publik yang sangat sering digunakan untuk mengotentikasi keaslian suatu data digital. Keamanan enkripsi/dekripsi data dari algoritma kriptografi ini terletak pada kesulitan untuk memfaktorkan modulus n yang sangat besar. Besarnya bilangan yang digunakan mengakibatkan lambatnya operasi yang melibatkan algoritma RSA ini. Dibandingkan dengan algoritma kunci privat seperti DES, RSA membutuhkan waktu komputasi yang lebih lambat pada saat implementasi.

**Sekilas Sejarah dari RSA**

Di tahun 1978, Ron Rivest, Adi Shamir dan Leonard Adleman dari Massachusetts Institute of Technology membuat sebuah algoritma untuk teori penomoran pada sebuah kunci publik, algoritma ini dikenal dengan nama RSA. Pada perkembangannya RSA banyak digunakan karena kemudahannya dan keamanannya. Huruf RSA itu sendiri berasal dari inisial nama mereka (Rivest—Shamir—Adleman).

**Operasional RSA**

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)

Sebagai contoh permasalahan, dalam berkomunikasi menggunakan jaringan internet, adanya lubang/celah dalam keamanan menjadi masalah serius karena perkembangan e-mail, e-banking, e-business dan jenis komunikasi lainnya makin pesat untuk mentranfer data-data penting. Sebagai contoh kasus Alice dan Bob yang ingin berkomunikasi dengan privasi tinggi, pada kenyataannya ada pihak ketiga yang dapat mengakses kemunikasi mereka.

Algoritma pembangkitan kunci RSA:

1. Pilih dua bilangan prima sembarang, p dan q.
2. Hitung n = pq (sebaiknya p tidak sama dengan q, jika p sama dengan 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. Pilihlah kunci privat, d, yang relatif prima terhadap φ(n). Maksudnya relatif prima adalah bilangan terbesar yang dapat membagi d dan φ(n) untuk menghasilkan nilai 1 (pembagi ini dinyatakan dengan gcd --greatest common divisor). Algoritma Euclid's digunakan untuk mencari gcd dua bilangan tersebut.
5. Bangkitkan kunci publik dengan menggunakan persamaan ed ≡ 1 (mod φ(n)). Perhatikan bahwa ed ≡ 1 (mod φ(n)) ekivalen dengan ed ≡ 1 + kφ(n), sehingga secara sederhana d dapat dihitung dengan e = (1 + kφ(n)) / d.

Hasil dari algoritma di atas adalah:

- Kunci publik adalah pasangan (e,n)
    - Dipublikasikan bebas
    - Pengiriman balik pesan kepada pemegang kunci privat untuk mengenkripsi pesan
- Kunci privat adalah pasangan (d, n)
    - Rahasia pemegang (end user)
    - Digunakan untuk mendekripsi pesan yang ditujukan kepadanya
    - Dapat berfungsi sebagai digital signature yang beroperasi dengan menggunakan privat key

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

**Proses enkripsi pesan**

Misalkan Bob ingin mengirim pesan m ke Alice. Bob mengubah m menjadi angka n < N, menggunakan protokol yang sebelumnya telah disepakati dan dikenal sebagai padding scheme.

Maka Bob memiliki n dan mengetahui N dan e, yang telah diumumkan oleh Alice. Bob kemudian menghitung ciphertext c yang terkait pada n:

$c = n^e \bmod N$

**Proses dekripsi pesan**

Alice menerima c dari Bob, dan mengetahui private key yang digunakan oleh Alice sendiri. Alice kemudian memulihkan n dari c dengan langkah-langkah berikut:

$n = c^d \bmod N$

Perhitungan diatas akan menghasilkan n, dengan begitu Alice dapat mengembalikan pesan semula m. Prosedur dekripsi bekerja karena

$$c^d \equiv (n^e)^d \equiv n^{ed} \pmod{N}$$

Kemudian, dikarenakan ed ≡ 1 (mod p-1) dan ed ≡ 1 (mod q-1), hasil dari Fermat's little theorem.

$$n^{ed} \equiv n \pmod{p} \quad n^{ed} \equiv n \pmod{q}$$

Dikarenakan p dan q merupakan bilangan prima yang berbeda, mengaplikasikan Chinese remainder theorem akan menghasilkan dua macam kongruen

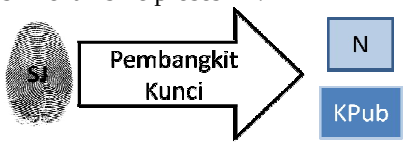
$$n^{ed} \equiv n \pmod{pq}$$

serta

$$c^d \equiv n \pmod{N}$$

### 3. Penjelasan Algoritma Pembangkitan Kunci pada RSA dengan Menggunakan Sidik Jari

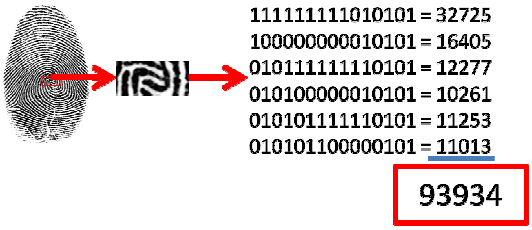
Mekanisme proses algoritma adalah dengan menggunakan masukan berupa gambar hitam putih dari sidik jari (SJ) yang dimiliki oleh seseorang yang ingin membangkitkan kunci RSA. Kemudian algoritma tersebut akan mengeluarkan nilai N yang merupakan konstanta dari RSA dan juga kunci publik (KPub) yang akan disebarkan. Sedangkan kunci privat tidak diperlihatkan karena akan diambil dari sidik jari. Untuk cara enkripsi pesan, sama seperti mekanisme enkripsi pesan dengan menggunakan RSA yang biasa. Gambar 1 menunjukkan ilustrasi mekanisme proses ini.




**Gambar 1 Mekanisme pembentukan kunci RSA**

Secara garis besar, algoritma ini terdiri atas dua bagian, yaitu proses pengambilan kunci privat dari sidik jari dan pembentukan kunci publik.

Fokus pada bagian pertama adalah proses untuk mengambil potongan gambar sidik jari, yang dalam hal ini diambil bagian tengah dari sidik jari, yang kemudian diubah menjadi *string* biner dimana 1 merepresentasikan bagian gambar yang gelap dan 0 merepresentasikan gambar yang terang. *String* biner tersebut terdiri dari 16 kolom dan 5 baris, setiap baris kemudian diubah menjadi bilangan decimal dan dijumlahkan. Gambar 2 dibawah menunjukan ilustrasi dan juga contoh pengambilan bilangan yang merupakan kunci publik.




**Gambar 2 Mekanisme pengambilan kunci privat dari sidik jari**

Kemudian pada bagian kedua adalah pembangkitan kunci publik. Proses ini merupakan kebalikan dari proses pembangkitan kunci RSA yang biasa. Jika, pembangkitan kunci pada RSA dimulai dari pencarian 2 bilangan prima, maka metode ini dinulai dengan diketahuinya kunci privat nya.

Algoritma pencarian Kunci Publik :

1. Diketahui kunci privat d dan $\varphi(n) = (p - 1)(q - 1)$
2. Pilih dua bilangan prima, p dan q dimana $\varphi(n)$ dan d relatif prima. Caranya dengan membangkitkan bilangan acak prima yang tidak berulang kombinasinya untuk p dan q, sampai kondisi terpenuhi.
3. Hitung $n = pq$ (sebaiknya p tidak sama dengan q, jika p sama dengan q maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n)
4. Bangkitkan kunci publik dengan menggunakan persamaan $ed \equiv 1 \pmod{\varphi(n)}$. Perhatikan bahwa $ed \equiv 1 \pmod{\varphi(n)}$ ekivalen dengan $ed \equiv 1 + k\varphi(n)$, sehingga secara sederhana d dapat dihitung dengan $e = (1 + k\varphi(n)) / d$.

Setelah itu didapatlah kunci publik dan juga nilai n yang akan disebarkan. Kunci privat tidak akan terlihat dari luar sistem. Oleh karena itu, ketika akan mendekripsi pesan yang telah dienkripsi dengan menggunakan kunci public, pemilik pesan harus memasukkan gambar hitam putih untuk diambil kunci privat nya sesuai dengan ilustrasi pada gambar 2 dan juga memasukkan nilai n.

### 4. Kesimpulan

Kesimpulan yang dapat diambil dari makalah ini adalah untuk membangkitkan kunci privat yang tidak mudah dilupakan, hilang maupun diambil oleh orang lain yang tidak berhak, maka kunci privat yang dibangkitkan dengan sidik jari pemilik akan lebih meningkatkan keamanan kunci privat tersebut.

### DAFTAR PUSTAKA

[1] Fatoni, Ilham.*Pembangkitan Kunci RSA Menggunakan Citra Digital*, Institut Teknologi Bandung, 2008.

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