Studi dan Implementasi Sistem Kriptografi Rabin

Anugrah Adeputra

Program Studi Teknik Informatika, Institut Teknologi Bandung, Jl.Ganesha No.10

Email: if15093@students.if.itb.ac.id

Abstraksi

Sistem Kriptografi Rabin adalah suatu teknik kriptografi asimetri/ kriptografi kunci publik yang memiliki tingkat keamanan, sebagaimana RSA, terkait dengan masalah sulitnya faktorisasi. Sistem Kriptografi Rabin pertama kali dipublikasikan pada bulan Januari 1979 oleh Michael O.Rabin. Sistem Kriptografi Rabin adalah sistem kriptografi asimetri pertama yang menerapkan konsep untuk mendapatkan keseluruhan plainteks dari suatu cipherteks yang diketahui berdasarkan pada kesulitan dalam melakukan faktorisasi.

Sistem Kriptografi Rabin memiliki kesulitan utama yaitu tiap hasil output dari fungsi Rabin dapat dibangun oleh empat buah input yang memungkinkan. Jika setiap output merupakan cipherteks, kompleksitas tambahan diperlukan untuk melakukan proses dekripsi karena adanya proses identifikasi di antara keempat input yang ada yang merupakan plainteks sesungguhnya.

Seperti teknik kriptografi kunci publik atau asimetri lainnya, Sistem Kriptografi Rabin menggunakan suatu pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik diperlukan dalam melakukan proses *encoding* nantinya dan dapat dipublikasikan, sementara kunci privat harus dimiliki hanya oleh penerima pesan.

Pada awal sejarahnya, sistem kriptografi ini dianggap hanya bersifat teoritik, namun secara praktik tidak baik untuk diterapkan akibat terdapat suatu cela yang fatal yang membuat sistem kriptografi ini tidak kuat dalam menghadapi *chosen plaintext attack*. Namun, terdapat suatu cara untuk menanggulangi hal tersebut, dan menjadikan sistem Kriptografi ini sebagai kompetitor utama dari Sistem Kriptografi RSA.

Makalah ini akan membahas beberapa hal mengenai sistem Kriptografi Rabin, yaitu dasar teori mengenai Sistem Kriptografi Rabin, Proses Pembangkitan Kunci, Enkripsi, Dekripsi, Serangan terhadap Sistem Kriptografi Rabin, serta evaluasi mengenai algoritma ini terkait dalam hal efisiensi, efektifitas, dan keamanan.

Kata Kunci: Sistem Kriptografi Rabin, Sistem Kriptografi Kunci Publik, Sistem Kriptografi Asimetri, Faktorisasi

1. Dasar Teori

Sistem Kriptografi Rabin

Sistem Kriptografi Rabin adalah suatu teknik kriptografi asimetri/ kriptografi kunci publik yang memiliki tingkat keamanan, sebagaimana RSA, terkait dengan masalah sulitnya faktorisasi. Sistem Kriptografi Rabin pertama kali dipublikasikan pada bulan Januari 1979 oleh Michael O.Rabin. Sistem Kriptografi Rabin adalah sistem kriptografi asimetri pertama yang menerapkan konsep untuk mendapatkan keseluruhan plainteks dari suatu cipherteks yang diketahui berdasarkan pada kesulitan dalam melakukan faktorisasi.

Sistem Kriptografi Rabin memiliki kesulitan utama yaitu tiap hasil output dari fungsi Rabin dapat dibangun oleh empat buah input yang memungkinkan. Jika setiap output merupakan cipherteks, kompleksitas tambahan diperlukan untuk melakukan proses dekripsi karena adanya proses identifikasi di antara keempat input yang ada yang merupakan plainteks sesungguhnya.

Seperti teknik kriptografi kunci publik atau asimetri lainnya, Sistem Kriptografi Rabin menggunakan suatu pasangan kunci, yaitu kunci publik dan kunci privat. Kunci publik diperlukan dalam melakukan proses *encoding* nantinya dan dapat dipublikasikan, sementara kunci privat harus dimiliki hanya oleh penerima pesan.

Berikut merupakan Langkah Pembangkitan Kunci dari Sistem Kriptografi Rabin:

- Pilih dua buah bilangan prima berbeda, yakni *p* dan *q*.
- Untuk mempermudah komputasi dari akar kuadrat modulo *p* dan *q*, kita bisa lakukan dengan memilih

$$p \equiv q \equiv 3 \pmod 4$$

- Nyatakan:

$$n = p \cdot q$$

n merupakan kunci publik sedangkan *p* dan *q* adalah kunci privat.

Untuk mengenkripsi suatu pesan, dibutuhkan *n* dan untuk mendekripsinya dibutuhkan faktor *p* dan *q* dari *n* harus diketahui.

Enkripsi

Untuk enkripsi, hanya kunci publik n yang digunakan. Proses yang terjadi adalah sebagai berikut:

Nyatakan $P = \{0,...,n-1\}$ sebagai ruang plainteks(berupa angka angka) dan $m \square P$ sebagai plainteks. Cipherteks didapatkan dengan rumus $\boldsymbol{c = m^2 \bmod n}$.

Dengan demikian, *c* adalah sisa kuadratik dari kuadrat dari plainteks dalam modulo *n*.

Contohnya: Jika n=77 dan P={0,....,76}, m=20, maka

$c = m^2 \bmod n = 20^2 \bmod 77 = 15$

Yang perlu diperhatikan adalah untuk mendapatkan nilai 15, dapat dibentuk dari 4 buah nilai m berbeda, yaitu: $m \in \{13,20,57,64\}$.

Hal ini benar, sebab kebanyakan cipherteks dari algoritma Rabin diproduksi dari fungsi 4 ke 1.

Dekripsi

Jika c dan r diketahui, plainteksnya $m \in \{0,...,n-1\}$ dengan

$$m^2 \equiv c \pmod{r}.$$

Untuk suatu r bilangan komposit, tidak ada metode untuk menemukan nilai m. Namun jika r merupakan bilangan prima, *Chinese* Remainder dapat digunakan. Dengan demikian, akar kuadrat

$$m_p = \sqrt{c} \bmod p$$

&

$$m_q = \sqrt{c} \bmod q$$

harus dikalkulasi.

Dalam contoh, misalkan didapatkan m_p = 1 dan m_q = 9.

Dengan melakukan *extended Euclidean algorithm*, y_p and y_q, dengan $y_p.p + y_q.q$=1, kita dapatkan $y_p = -3$ dan $y_q = 2$.

Dengan memanfaatkan *Chinese remainder theorem*, keempat akar kuadratik, yaitu: $+r, -r, +s$ dan $-s$ dari

$$c + n\mathbb{Z} \in \mathbb{Z}/n\mathbb{Z}$$

Keempat akar kuadrat terdapat dalam

$$\begin{aligned} r &= (y_p \cdot p \cdot m_q + y_q \cdot q \cdot m_p) \bmod n \\ -r &= n - r \\ s &= (y_p \cdot p \cdot m_q - y_q \cdot q \cdot m_p) \bmod n \\ -s &= n - s \end{aligned}$$

himpunan $\{0,...,n-1\}$

Salah satu dari keempat akar tersebut adalah plainteks asli. Dalam contoh: $m \in \{64,\mathbf{20},13,57\}$

Menghitung Akar Kuadrat

Dengan memilih p dan q untuk penyederhanaan seperti yang sebelumnya dijelaskan, memungkinkan kita untuk menghitung:

$$m_q = c^{\frac{(q+1)}{4}} \bmod q$$

dan

$$m_q = c^{\frac{(q+1)}{4}} \bmod q$$

$p \equiv 3 \pmod 4$ mengindikasikan bahwa nilai p+1/4 merupakan integer. Asumsi trivial untuk $c \equiv 0 \pmod p$. Dengan demikian, kita dapat mengasumsikan p tidak membagi habis c.

Maka,

$$m_p^2 \equiv c^{\frac{(p+1)}{2}} \equiv c \cdot c^{\frac{(p-1)}{2}} \equiv c \cdot \left(\frac{c}{p}\right) \pmod p,$$

di mana $(-)$ merupakan Simbol Legendre.

Dari kongruensi

$$c \equiv m^2 \pmod{pq}$$

dan sifat modulo, maka .

$$c \equiv m^2 \pmod{p}$$

C adalah sisa kuadrat dalam modulo *p*. Dengan demikian,

$$\left(\frac{c}{p}\right) = 1$$

$$m_p^2 \equiv c \pmod{p}.$$

Hubungan

$$p \equiv 3 \pmod{4}$$

bukanlah suatu keharusan, sebab akar kuadrat modulo bilangan prima lain juga dapat dihitung dengan menggunakan algoritma yang disebut "*Berlekamp's Algorithm*".

Definisi Lain

Sumber lain menjelaskan Sistem Kriptografi Rabin sebagai berikut:

- *n merupakan perkalian dua buah bilangan prima berbeda, p dan q.*
- *Terdapat suatu bilangan B, 0≤B≤n-1*
- *Fungsi Enkripsi:*
  eK(x)=x(x+B)mod n
  dan
  Fungsi Dekripsi:
  dk(y)= $\overline{— + \quad — —}$ *mod n*
- Nilai n dan B merupakan kunci publik sedangkan p dan q merupakan kunci privat

Efektifitas

Pada saat dekripsi, hasil yang didapat adalah 3 hasil salah sebagai tambahan dari satu hasil yang tepat. Sehingga hasil yang tepat harus dikira-kira. Ini merupakan sisi buruk bagi sistem kriptografi Rabin ini dan merupakan satu faktor penyebab penggunaannya yang tidak digunakan secara umum. Jika plainteks merupakan pesan teks, mengira-ngira hasil yang tepat tidaklah sulit, akan tetapi jika plainteks merupakan numerik, maka hal tersebut menjadi masalah yang harus ditanggulangi dengan suatu skema disambiguasi. Untuk menanggulangi masalah ini, dimungkinkan memilih plainteks dengan struktur khusus, atau dengan menambahkan padding.Cara yang paling umum digunakan dikenal sebagai "*Blum Disambiguation*".

Efisiensi

Adanya Disambiguitas secara tidak langsung menambah biaya komputasi, dan hal tersebutlah yang menyebabkan Rabin dianggap kurang efisien dibanding RSA. Sehingga, Rabin jarang digunakan akibat tingkat efisiensi yang kurang baik tersebut.

Keamanan

Karena Rabin tidak jauh berbeda dengan RSA, bahkan disebut pula sebagai varian dari RSA, tingkat keamanannya dapat dikatakan relatif sama. Kesulitan terbesar terdapat dalam proses faktorisasi yang dibutuhkan untuk mencari nilai *p* dan *q* yang merupakan kunci privat dari algoritma ini.

Serangan terhadap Rabin

Sebenarnya terdapat banyak teknik serangan yang dapat diterapkan pada sistem kriptografi Rabin. Beberapa di antaranya tidak efektif.

Beberapa jenis serangan yang dapat dilakukan pada sistem kriptografi Rabin tersebut adalah:

- *Factorization Attack:* Serangan yang dilakukan dengan proses pemfaktoran
- *Chosen-Ciphertext Attack:* Penyerang dapat memilih suatu cipherteks y dan mengkonstruksi plainteks yang terkait sehingga ia bisa menguraikan proses yang terjadi dalam sistem kriptografi tersebut
- *Chosen-Plaintext Attack:* Penyerang dapat memilih suatu plainteks x dan mengkonstruksi cipherteks yang terkait sehingga ia bisa menguraikan proses yang terjadi dalam sistem kriptografi tersebut
- *Encryption Exponent Attack*
- *Decryption Exponent Attack*
- *Plaintext Attack*
- *Modulus Attack*
- *Implementation Attack*

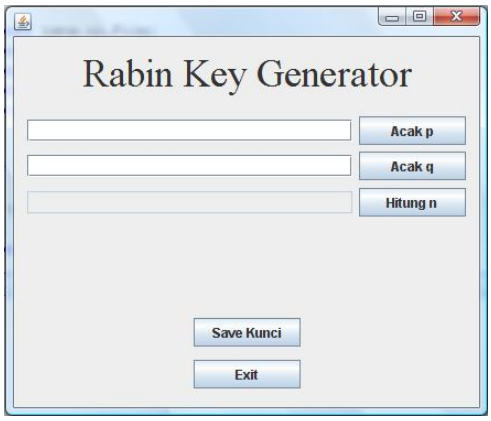
2. Implementasi

Implementasi yang dilakukan berupa Key Generator dan Aplikasi yang berfungsi untuk menunjukkan enkripsi dan dekripsi dari Sistem Kriptografi Rabin. Namun fungsi dekripsi yang diimplementasikan belum berjalan dengan baik sehingga hasil yang ditampilkan bukan merupakan hasil yang tepat.

Sedangkan untuk Key Generator, dengan maksud untuk memudahkan pengerjaan pada saat dekripsi, hanya menggenerate bilangan prima sesuai dengan ketentuan di atas, yaitu bilangan prima yang memiliki nilai remainder 3 dalam modulo 4, atau:

$$p \equiv q \equiv 3 \pmod 4$$

Berikut merupakan tampilan aplikasi Key Generator:

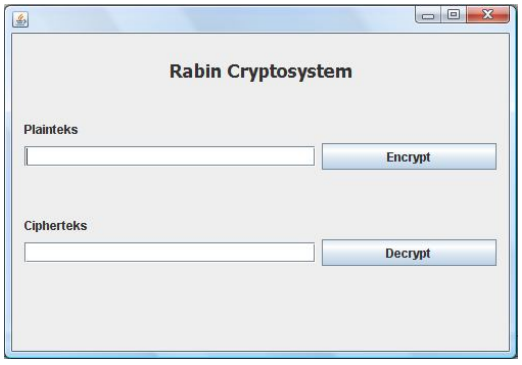


Program Key Generator dapat melakukan pengacakan nilai *p*, nilai *q* dan mengkalkulasikan nilai *n* berdasarkan perhitungan *p.q*.

Dengan menekan tombol Save Kunci, maka nilai n akan disimpan dalam file kuncipublik.pub dan nilai p dan q akan disimpan pada file kunciprivat.pri pada direktori yang sama dengan aplikasi tersebut.

Kunci itu nantinya akan dimanfaatkan oleh aplikasi Rabin untuk proses enkripsi dan dekripsi.

Berikut merupakan tampilan aplikasi Rabin:



Kesimpulan

Kesimpulan yang dapat ditarik dari studi dan sedikit implementasi yang dilakukan adalah:

1) Sistem Kriptografi Rabin adalah salah satu teknik kriptografi kunci publik yang memiliki tingkat keamanan, sebagaimana RSA, terkait dengan masalah sulitnya faktorisasi.

2) Karena merupakan fungsi 4 ke 1, Hasil dekripsi dari cipherteks pada teknik Rabin akan menghasilkan 4 buah kemungkinan plainteks. Penerima harus menentukan sendiri manakah dari keempat kemungkinan tersebut yang merupakan plainteks yang tepat. Namun hal tersebut akan sulit dilakukan apabila isi plainteks berupa numerik.

3) Teknik Rabin cukup kuat dalam menghadapi berbagai jenis serangan yang ada, namun memiliki kelemahan terhadap serangan *Chosen Plaintext.*

Daftar Pustaka

[1] Munir, Rinaldi, Diktat Kuliah IF5054 Kriptografi,Program Studi Teknik Informatika, Sekolah Teknik Elektro dan Informatika, 2006.

[2] Stinson, Douglas R., Cryptography:Theory and Practice,CRC Press. 1995.