Teknik Kriptografi Rabin, Serangan yang Dapat Dilakukan dan Perbandingannya dengan RSA

Arya Widyanarko
Program Studi Teknik Informatika, Institut Teknologi Bandung, Jl. Ganesha 10 Bandung
Email: if14030@students.if.itb.ac.id

Abstract *– Teknik kriptografi Rabin adalah teknik kriptografi kunci asimetris yang merupakan variasi dari sistem kriptografi RSA. Teknik kriptografi Rabin ini memiliki struktur kunci yang berbeda dengan RSA, baik kunci publik maupun kunci privatnya. Selain itu teknik kriptografi Rabin memanfaatkan teorema Chinese Remainder pada proses dekripsinya, berbeda dengan RSA. Teknik kriptografi Rabin seperti halnya RSA tidak hanya dapat digunakan untuk melakukan enkripsi dan dekripsi pada pesan rahasia, melainkan dapat digunakan untuk memberi tandatangan digital (digital signature) pada suatu dokumen (sign dan verify).*

Keamanan dari teknik kriptografi Rabin kelihatannya cukup tinggi jika parameter pembangkitan kunci yang digunakan memiliki ukuran yang panjang. Kesulitan yang umum dihadapi dalam memecahkan kunci privat yang digunakan adalah kesulitan dalam melakukan pemfaktoran. Namun tetap terbuka kemungkinan teknik ini untuk dapat dipecahkan. Keamanan teknik kriptografi Rabin ini akan dijabarkan dan dianalisis didalam makalah ini.

Makalah ini membahas beberapa hal mengenai teknik kriptografi Rabin, yaitu proses pembangkitan kunci, proses enkripsi, proses dekripsi. Selain itu akan dilakukan analisis beberapa jenis serangan yang dapat dilakukan terhadap teknik kriptografi ini. Yang terakhir akan dilakukan perbandingan antara teknik ini dengan RSA. RSA dipilih sebagai pembanding mengingat teknik kriptografi Rabin dianggap sebagai varian dari teknik kriptografi RSA. Kemudian akan dilakukan eksperimen dalam melakukan pembandingan kedua teknik kriptografi tersebut.

Kata Kunci*: Sistem kriptografi Rabin, RSA, Kriptografi kunci asimetris, Chinese remainder.*

1. PENDAHULUAN

Teknik kriptografi RSA adalah algoritma kriptografi kunci publik yang paling umum digunakan [2]. RSA menggunakan dua buah bilangan eksponen, *e* dan *d*, yang merupakan kunci publik dan kunci privat. Kekuatan keamanan algoritma ini terletak pada sulitnya melakukan pemfaktoran bilangan yang sangat besar menjadi faktor-faktor prima [1].

Teknik kriptografi Rabin merupakan varian dari RSA yang dikemukakan oleh M. Rabin. Perbedaan yang paling mencolok diantara RSA dan Rabin adalah proses kerjanya. RSA bekerja dengan berbasis *exponentiation congruence*, sementara Rabin dengan berbasis *quadratic congruence* [2]. Perbedaan ini terlihat pada proses pembangkitan kunci. Proses pembangkitan kunci RSA dan Rabin memiliki perbedaan yang cukup mencolok, sementara proses enkripsi dan dekripsinya pun juga berbeda.

Pada dasarnya RSA dan Rabin memiliki prinsip yang sama. Rabin menggunakan prinsip yang sama dengan prinsip pada RSA, karena itulah Rabin dikatakan sebagai varian dari algoritma RSA.

2. TEKNIK KRIPTOGRAFI RABIN

Seperti telah dikemukakan sebelumnya, walaupun Rabin dianggap sebagai varian dari RSA, namun proses yang ada didalamnya tidak sama dengan proses pada RSA. Berikut dijelaskan mengenai setiap proses pada teknik kriptografi Rabin.

2.1. Pembangkitan Kunci

Perbedaan mendasar yang ada pada proses pembangkitan kunci antara RSA dan Rabin adalah variable yang merupakan kunci public, kunci privat, dan variable yang dibutuhkan dan tidak boleh dilupakan.

Pada RSA, proses pembangkitan kunci diawali dengan membangkitkan dua bilangan prima p dan q. Kemudian dengan rumus yang ada didapatkan beberapa nilai lainnya dengan variabel n, $\Phi(n)$, e dan d. Nilai yang perlu dijaga untuk melakukan enkripsi dan dekripsi menggunakan RSA hanyalah variabel n, d dan e. Nilai lainnya seperti p, q dan $\Phi(n)$ dapat dibuang dan dilupakan [2].

Pada Rabin, nilai p dan q yang tidak digunakan pada RSA harus diingat karena merupakan bagian dari kunci untuk melakukan enkripsi dan dekripsi. Proses pembangkitan kunci pada Rabin tidak serumit RSA. Rabin hanya melibatkan sedikit saja variabel dalam pembangkitan kunci, namun memiliki kesulitan yang sama dengan RSA dalam hal pemfaktoran bilangan prima, untuk menambah keamanannya.

Berikut adalah langkah-langkah yang dilakukan untuk membangkitkan kunci Rabin:

1. Memilih dua buah bilangan prima *p* dan *q*.
2. Menghitung nilai $n = p \times q$
3. Mendapatkan nilai kunci publik dan kunci privat, dimana kunci publik adalah *n* dan kunci privat adalah *q* dan *n*.

Kedua bilangan prima *p* dan *q* harus berada dalam persamaan $4k+1$ atau $4k+3$. Walaupun dibatasi dalam persamaan, tetapi proses pemecahan kunci teknik Rabin ini tetap sulit, karena proses pemfaktoran bilangan akan membutuhkan waktu yang lama, terlebih jika menggunakan bilangan yang sangat besar.

Proses dekripsi terhadap teknik Rabin akan lebih mudah jika bilangan pembangkit kunci *p* dan *q* berada pada persamaan $4k+3$ dibandingkan dengan persamaan $4k+1$, karena itu persamaan $4k+3$ lebih dianjurkan untuk pemilihan kedua bilangan pembangkit kunci tersebut [2].

Berikut adalah *pseudo-code* algoritma proses pembangkitan kunci teknik Rabin:

```
Pembangkit_Kunci_Rabin()
{
    Pilih 2 bilangan prima p dan q
    dalam persamaan 4k+3

    n ← p x q

    kunci_publik ← n
    kunci_privat ← (q, n)

    return kunci_publik dan kunci_privat
}
```

2.2. Proses Enkripsi

Teknik Rabin merupakan algoritma kriptografi kunci publik, maka semua orang dapat melakukan enkripsi dengan satu kunci publik tertentu, namun proses dekripsi hanya dapat dilakukan dengan menggunakan kunci privat oleh orang yang bersangkutan.

Proses enkripsi pada teknik Rabin sangat sederhana. Proses enkripsi tersebut dapat dituliskan dalam rumus berikut:

$$C = P^2 \bmod n$$

C : Cipherteks
P : Plainteks
n : kunci publik

Proses enkripsi yang sederhana ini menyebabkan proses enkripsi teknik Rabin ini dapat dilakukan dalam waktu yang relatif singkat karena tidak memiliki proses yang rumit. Kesederhanaan ini merupakan keuntungan yang dimiliki teknik Rabin untuk menghadapi keterbatasan *resource* yang ada pada media kriptografi. Misalnya pada *smart card* yang memiliki memori terbatas dan membutuhkan waktu proses CPU yang singkat.

Berikut adalah *pseudo-code* algoritma proses enkripsi pada teknik Rabin:

```
Enkripsi(n,P)
{
     C ← P^2 mod n
     return C
}
```

2.3. Proses Dekripsi

Proses Dekripsi pada teknik Rabin dilakukan dengan menggunakan sebuah rumus sederhana, namun membutuhkan teorema *Chinese remainder*. Teorema ini digunakan untuk mendapatkan plainteks yang benar.

Namun yang menjadi poin penting dari teknik ini adalah teknik Rabin tidak menghasilkan jawaban plainteks tunggal. Jawaban yang dihasilkan pada teknik Rabin ini terdiri dari 4 kemungkinan jawaban, tidak menghasilkan satu jawaban yang pasti.

Berikut adalah *pseudo-code* algoritma proses dekripsi teknik kriptografi Rabin:

```
Dekripsi(p,q,C)
{
     a1 ← +(C^((p+1)/4)) mod p
     a2 ← -(C^((p+1)/4)) mod p
     b1 ← +(C^((q+1)/4)) mod q
     b2 ← -(C^((q+1)/4)) mod q

     // Chinese_Rem adalah fungsi yang
     // memanggil fungsi untuk Chinese
     // Remainder

     P1 ← Chinese_Rem(a1,b1,p,q)
     P2 ← Chinese_Rem(a1,b2,p,q)
     P3 ← Chinese_Rem(a2,b1,p,q)
     P4 ← Chinese_Rem(a2,b2,p,q)

     return P1,P2,P3,P4
}
```

Teknik Rabin selalu menghasilkan 4 kemungkinan hasil, yang diberikan semuanya kepada orang yang melakukan dekripsi terhadap pesan rahasia. Kemudian orang tersebut harus dapat menentukan mana pesan yang sebenarnya diantara keempat hasil dekripsi tersebut.

Walaupun menghasikan 4 pesan berbeda pada akhirnya, namun penerima pesan dapat memilih pesan yang benar dengan tidak terlalu sulit, karena pesan yang benar seharusnya akan terlihat jelas dibandingkan dengan ketiga hasil dekripsi yang lain.

3. SERANGAN TERHADAP RABIN

Seperti yang telah dibahas sebelumnya, teknik Rabin memiliki tingkat kesulitan tinggi untuk dipecahkan seperti halnya RSA. Kedua teknik ini mengandalkan sulitnya pemfaktoran terhadap bilangan yang sangat besar. Dengan menggunakan kunci berukuran besar, maka semakin sulit teknik Rabin dipecahkan karena hingga saat ini belum ditemukan algoritma mangkus yang dapat memecahkan masalah pemfaktoran tersebut dalam waktu singkat.

Sebenarnya ada banyak sekali serangan yang dapat diterapkan pada teknik Rabin, namun tidak semuanya dapat berjalan efektif. Misalnya serangan Faktorisasi dapat dilakukan, namun akan kesulitan dalam memecahkan kuncinya karena pemfaktoran yang besar.

Beberapa jenis serangan yang dapat dilakukan terhadap Rabin antara lain:

1) *Factorization attack*
2) *Chosen-ciphertext attack*
3) *Chosen-plaintext attack*
4) *Encryption exponent attack*
   Diantaranya *Coppersmith attack, broadcast attack*, dan *short pad attack*
5) *Decryption exponent attack*
   Diantaranya *revealed attack* dan *low exponent attack*
6) *Plaintext attack*
   Diantaranya *short message attack, cyclic attack* dan *unconcealed attack*
7) *Modulus attack*
8) *implementation attack*

Dalam makalah ini akan dibahas 2 buah serangan yang dapat dilakukan terhadap teknik Rabin dan bagaimana tingkat berbahayanya serangan tersebut. Kedua serangan tersebut adalah *Chosen-plaintext attack* dan *chosen-ciphertext attack*. Sebelumnya ada dua hal penting yang perlu diketahui.

Yang pertama adalah teknik kriptografi Rabin aman dalam menghadapi serangan-serangan yang bersifat pasif seperti serangan faktorisasi, terlebih lagi jika menggunakan ukuran kunci yang besar.

Kedua, teknik ini sangat tidak aman jika mendapat serangan berupa serangan *chosen-ciphertext attack.* Selain itu Rabin tidak aman mengghadapi serangan seperti *man-in-the-middle attack*[1].

3.1. Keamanan terhadap *Chosen-plaintext attack*

Untuk melakukan serangan *chosen-plaintext attack* dibutuhkan *adversary* untuk memecahkan sistem teknik ini. Adversary ini digunakan dengan masukkan kunci enkripsi dan cipherteks, dan memberi *output* nilai *m* dimana $m^2 = c \bmod n$. Namun cara ini kurang efektif menghadapi teknik Rabin [4]

Cara lain menggunakan teknik *chosen-plaintext attack* adalah dengan urutan sebagai berikut:

```
Chosen_Plaintext(N)
{
    Y ← 1, x ← 0,
    while(y=x or y=N-x)
    {
        // pilih bilangan random x
        x ← random()
        c ← x^2

        // kirim nilai N dan c=x^2 mod N
        // pada adversary dan mendapat
        // y dimana c=y^2 mod N
        y ← adversary(N,c)
    }
    // x^2-y^2 = 0 mod N
    // 0 ≠ (x-y)(x+y) = cN = cpq

    // hitung nilai FPB(x+y,N) dan
    // FPB(x-y,N) dan perkirakan nilai
    // p dan q
}
```

Cara diatas pun masih terhalang oleh sulitnya faktorisasi. Kekuatan yang paling sederhana dari Rabin adalah faktorisasinya.

Jika seseorang berhasil memecahkan teknik kriptografi Rabin, itu artinya permasalahan faktorisasi pun telah terpecahkan. Selama masalah faktorisasi masih belum dipecahkan, dan belum ditemukan algoritma mangkus untuk melakukannya, maka teknik Rabin aman.

3.2. Kemananan terhadap *Chosen-ciphertext attack*

Teknik kriptografi Rabin lemah dalam menghadapi serangan ini. Serangan ini adalah serangan yang paling efektif untuk memecahkan teknik Rabin.

Chosen-ciphertext attack memperlihatkan bagaimana faktorisasi dari kunci enkripsi *N*. Karena kekuatan teknik Rabin ada pada kesulitan pemfaktoran kunci *N*, maka jika pemfaktoran telah terpecahkan, teknik Rabin pun akan dengan mudah dapat dipecahkan.

Dengan teknik *chosen-ciphertext* ini faktor dari *N* dapat terbongkar, maka tantangan yang didapat oleh penyerang adalah bagaimana melakukan proses dekripsi terhadap cipherteks. Seperti yang diketahui sebelumnya bahwa hasil dekripsi teknik Rabin menghasilkan 4 kemungkinan cipherteks.

Mencari cipherteks yang benar dari 4 buah kemungkinan bukanlah hal yang terlalu sulit bagi penyerang, namun ada kalanya hal itu menjadi sulit. Walau mempersulit proses dekripsinya, namun hal ini cukup menambah tingkat keamanan yang dimiliki oleh teknik Rabin.

Berikut adalah proses yang dilakukan dalam serangan *chosen-ciphertext attack*:

1) Pemecah kode dapat menggunakan penerima pesan yang sesungguhnya sebagai *adversary* dalam proses yang ia lakukan.

2) Ambil bilangan sembarang x dan kirimkan nilai c pada penerima yang sesungguhnya, dimana:
$C = x^2 \bmod N$

3) Penerima pesan mengembalikan nilai y yang merupakan *square root* dari c.

4) Dengan kemungkinan ½, $x \neq y$ dan $x \neq -y$. Dalam kasus ini, pemecah kode dapat memfaktorkan N dengan menghitung nilai FPB dari x-y dan n.

4. EKSPERIMEN

Dengan menggunakan program[1] yang telah diunduh sebelumnya, dilakukan eksperimen untuk melakukan enkripsi dan dekripsi terhadap teknik Rabin. Karena kunci yang digunakan dibangkitkan secara acak oleh aplikasi, maka yang ditonjolkan dalam eksperimen ini bukanlah hasil enkripsi maupun dekripsi yang telah dilakukan, melainkan aspek lainnya.

Berikut adalah hasil percobaan menggunakan teknik kriptografi Rabin dalam tabel 1.

Percobaan 1	
Kunci Publik	686089581552930126005597
Kunci Privat	p : 827928751631
	q : 828681912787
Plainteks	12345
Cipherteks	499723529734691110091091
Percobaan 2	
Kunci Publik	541734920593987193492917
Kunci Privat	p : 582165469031
	q : 930551448707
Plainteks	1234567890
Cipherteks	491792154822160362718283
Percobaan 3	
Kunci Publik	703390078776054191548217
Kunci Privat	p : 698025505939
	q : 1007685353603
Plainteks	1213413861523
Cipherteks	942097118404181146690509
Percobaan 4	
Kunci Publik	1081363349416555985902477
Kunci Privat	p : 1083440446867
	q : 998082868831
Plainteks	8172615731391781861537
Cipherteks	154180730050893616437893

Table 1. Hasil eksperimen teknik Rabin

Dari keempat percobaan terhadap teknik Rabin, hasil dekripsi berhasil mengembalikan nilai plainteks yang benar. Dengan begitu kebenaran hasil dekripsi dapat terbukti. Selain itu, kunci yang digunakan dalam eksperimen masih kurang besar. Jika lebih besar lagi, maka pemfaktoran terhadap kunci akan semakin sulit untuk dilakukan.

Pada analisis yang akan dilakukan untuk membandingkan teknik kriptografi Rabin dan RSA, akan digunakan data dan dasar teori mengenai RSA yang dibahas didalam [1]. Data dan dasar teori mengenai teknik Rabin sendiri telah dibahas didalam makalah ini.

5. ANALISIS

Setelah melakukan eksperimen dan melakukan pembahasan mengenai teknik kriptografi Rabin, maka dilakukan analisis mengenai perbandingan antara teknik Rabin dengan RSA.

Seperti diketahui bahwa teknik Rabin merupakan varian dari RSA, sehingga memiliki fungsi dasar yang cukup mirip. Maka analisis perbandingan antara RSA dan Rabin ini dilihat dari berbagai aspek yang ada. Hasil analisis menurut penulis dijelaskan di bawah ini.

5.1. Kerumitan proses pembangkitan kunci

Dari sisi kerumitan proses pembangkitan kunci, RSA terlihat lebih baik dibandingkan dengan Rabin. Hal ini disebabkan karena pada Rabin, proses komputasi yang dilakukan dalam proses pembangkitan kunci hanya sedikit dan melibatkan 3 nilai, yaitu p, q dan N. Sementara pada RSA proses pembangkitan kunci dibuat lebih rumit untuk mempersulit faktorisasi terhadap kunci publik untuk memecahkan RSA.

5.2. Kecepatan proses pembangkitan kunci

Aspek kecepatan proses pembangkitan kunci cukup berimbang diantara kedua teknik kriptografi ini. Namun Rabin memiliki waktu proses pembangkitan kunci yang sedikit lebih singkat dibandingkan dengan RSA karena proses pembangkitan kunci RSA lebih kompleks dibandingkan Rabin

5.3. Penyimpanan kunci publik dan kunci privat

Pada penyimpanan kunci publik dan kunci privat, kedua teknik ini pun cukup berimbang, namun dari aspek jumlah kunci Rabin lebih baik karena pada teknik Rabin setiap kunci publik dan kunci privat hanya terdiri dari satu variabel, sementara pada RSA setiap kunci terdiri dari dua variabel yang disimpan.

5.4. Proses Enkripsi

Proses Enkripsi RSA dan Rabin masing-masing memiliki keunggulan. RSA memiliki proses enkripsi yang lebih rumit dibandingkan dengan proses Rabin. Kerumitan proses enkripsi ini tentu akan sedikit meningkatkan tingkat keamanan RSA. Dibandingkan

dengan RSA, teknik Rabin memiliki proses enkripsi yang terbilang sederhana dengan proses komputasi yang sedikit. Namun kecepatan proses teknik Rabin jelas lebih baik dibandingkan dengan RSA karena menggunakan komputasi sederhana. Selain itu untuk *resource* yang terbatas dari kapasitas proses komputasi, Rabin lebih diunggulkan

5.5. Hasil Enkripsi

Hasil enkripsi RSA dan teknik Rabin sama-sama baik dan memiliki tingka keamanan tinggi karena proses rumit yang ada dalam proses enkripsinya. Hasil enkripsi kedua teknik tersebut tidak dapat dibandingkan mana yang lebih baik karena sama-sama merupakan hasil enkripsi.

5.6. Proses Dekripsi

Dari aspek proses dekripsi, tidak jauh berbeda dengan proses enkripsi. Proses dekripsi pada RSA memiliki kompleksitas yang rumit dan membutuhkan waktu lebih lama dibandingkan dengan teknik Rabin. Namun teknik Rabin memiliki kekurangan pada proses dekripsinya, yaitu melakukan proses yang dapat dikatakan kurang efektif, karena melakukan proses *chinese remainder* hingga 4 kali, sementara hasil dekripsi yang benar hanya 1.

5.7. Hasil Dekripsi

RSA memiliki hasil dekripsi yang sangat akurat dengan plainteksnya. Kemungkinan kesalahan sangat kecil dan tidak terjadi selama melakukan eksperimen. Dalam teknik Rabin yang dijelaskan dalam makalah ini hasil dekripsi menghasilkan 4 kemungkinan plainteks. Penerima pesan harus dapat menentukan sendiri plainteks yang sebenarnya diantara keempat kemungkinan yang dihasilkan proses dekripsi.

5.8. Keamanan teknik kriptografi

Tingkat keamanan kedua teknik ini sama, karena keduanya mengandalkan kekuatan sulitnya pemfaktoran bilangan yang berukuran sangat besar. Mengingat bahwa teknik Rabin adalah varian dari RSA, maka tingkat keamanan keduanya relatif sama.

6. KESIMPULAN

Kesimpulan yang dapat ditarik dari pembahasan, eksperimen dan analisis yang telah dilakukan antara lain:

1) Teknik kriptografi Rabin merupakan varian dari RSA. Tingkat keamanan keduanya relatif sama dengan mengandalkan kekuatan sulitnya memfaktorkan bilangan yang besar.
2) Hasil dekripsi cipherteks pada teknik Rabin menghasilkan 4 kemungkinan plainteks. Penerima pesan harus menentukan sendiri plainteks yang benar.
3) Teknik Rabin kuat dalam menghadapi serangan pasif seperti *factorization attack*, namun dapat diserang dengan mudah dengan jenis serangan *chosen-plaintext attack*.
4) Teknik kriptografi Rabin lebih cocok digunakan pada *resource* yang sederhana dengan processor yang tidak dapat melakukan komputasi yang kompleks dan rumit. Contohnya pada *smart card*.

DAFTAR REFERENSI

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

[2] Forouzan, Behrouz, *Cryptography and Network Security*, McGraw-Hill, 2008.

[3] Brown, Daniel R. L., *Breaking RSA May Be As Difficult As Factoring*, 2006.

[4] Pinkas, Benny, *Rabin's Encryption Systems, Digital Signature*, 2005.

[5] Pan, Guangrui and Paliwal, Shivalee., *The Wonderful World of the RSA Cryptosystem*, 2005.

[1] Program yang digunakan dapat diunduh pada alamat http://islab.oregonstate.edu/koc/ece575/03Project/Vemula/rabin.zip