KOMBROF
Jurnal Teknologi Informasi Papua

Analisis Teorema Sisa Cina dalan Dekripsi Data Text Terenkripsi RSA

Ishak Semuel Beno
Program Studi Matematika, Fakultas MIPA, Universitas Cenderawasih, Jayapura, Indonesia
E-mail: i.s.beno@fmipa.uncen.ac.id

Article Info
Article History
Received:
Revised:
Published:

Keywords:
RSA cryptography, encryption, decryption, CRT-based RSA

Abstract
In the field of secured communication, the choice of an efficient decryption algorithm plays an important role in ensuring data confidentiality and integrity. This study presents a comparative analysis of standard RSA decryption techniques and CRT-based decryption in the context of ciphertext decryption generated via RSA encryption. The goal is to evaluate the performance of each in terms of execution time and recovery efficiency.
The study begins by outlining the theoretical basis of RSA cryptography and the Chinese Remainder Theorem (CRT), their significance in the encryption and decryption processes. Furthermore, it is carried out by simulating a cyptertext using a sample of Indonesian plaintext sentence " *Sa suka kriptografi skali karna sangat matematik* ", which is represented in numerical form using ASCII code.
The simulation involves applying the standard RSA decryption and a CRT-based decryption algorithms, followed by measuring the execution time for each approach. The results obtained from the simulation show the superiority of the CRT-based decryption method compared to standard RSA decryption. CRT-based descriptions prove to be more efficient and faster due to the parallel nature of processing and the reduced processing costs it offers.
This research contributes to understanding the benefits and practical realisation of using CRT-based description techniques in RSA cryptography. This advantage utilises prime factors and parallelisation of calculations to improve the description process.

Artikel Info
Sejarah Artikel
Diterima:
Direvisi:
Dipublikasi:

Kata kunci:
Kriptografi RSA, enkripsi, dekripsi, RSA berbasis CRT

Abstrak
Dalam bidang keamanan komunikasi, pilihan algoritma dekripsi yang efisien memainkan peranan penting dalam memastikan kerahasiaan dan integritas data. Penelitian ini menyajikan analisis perbandingan teknik dekripsi RSA standar dan dekripsi berbasis TSC dalam konteks dekripsi *ciphertext* yang dihasilkan melalui enkripsi RSA. Tujuannya adalah untuk mengevaluasi kinerja masing-masing dalam hal waktu eksekusi dan efisiensi komputasi.
Studi dimulai dengan menguraikan dasar teoritis kriptografi RSA dan Teorema Sisa Cina (TSC), menyoroti signifikansinya dalam proses enkripsi dan dekripsi. Selanjutnya dilakukan simulasi dengan menggunakan sampel kalimat tersamar "*Sa suka kriptografi skali karna sangat matematik*", yang direpresentasikan dalam bentuk numerik menggunakan kode ASCII.
Simulasi melibatkan penerapan algoritma dekripsi RSA standar dan algoritma dekripsi berbasis TSC, diikuti dengan mengukur waktu eksekusi untuk setiap pendekatan. Hasil yang diperoleh dari simulasi menunjukkan keunggulan metode dekripsi berbasis TSC dibandingkan dekripsi RSA standar. Dekripsi berbasis TSC terbukti lebih efisien dan lebih cepat karena sifat komputasi paralel dan pengurangan beban komputasi yang ditawarkannya.
Penelitian ini memberikan kontribusi untuk memahami manfaat dan implikasi praktis dari penggunaan teknik dekripsi berbasis TSC dalam kriptografi RSA. Ini menyoroti keuntungan memanfaatkan sifat faktor prima dan paralelisasi perhitungan untuk meningkatkan proses dekripsi.

I. PENDAHULUAN

Enkripsi *Rivest-Shamir-Adleman (RSA)* adalah salah satu skema enkripsi yang paling banyak digunakan dalam kriptografi modern. Ini didasarkan pada prinsip matematika aritmatika modular dan kesulitan memfaktorkan bilangan bulat besar (Zhao and Qi, 2007). Enkripsi RSA digunakan untuk mengamankan komunikasi dan transaksi melalui internet, misalnya perbankan online, e-commerce, dan email.

Meskipun digunakan secara luas, enkripsi RSA tidak sepenuhnya aman. Secara khusus, ada serangan-serangan yang dikenal dapat digunakan untuk memecahkan enkripsi RSA dan memulihkan pesan teks asli. Salah satu serangan tersebut adalah serangan *Chinese Remainder Theorem (CRT)* (Menezes, van Oorschot and Vanstone, 1997)yang selanjutnya dalam penelitian ini disebut Teorema Sisa Cina (TSC).

TSC adalah alat matematika yang dapat digunakan untuk mempercepat perhitungan yang melibatkan bilangan besar. Ini didasarkan pada gagasan bahwa jika kita mengetahui sisa suatu bilangan ketika dibagi dengan beberapa bilangan yang lebih kecil, kita dapat menentukan bilangan itu sendiri. CRT dapat digunakan untuk menyelesaikan sistem kongruensi linier, yang merupakan persamaan dalam bentuk "$ax \equiv b \ (mod\ n)$", di mana a, b, dan n adalah bilangan bulat.

Dalam beberapa tahun terakhir, para peneliti telah mengeksplorasi penggunaan TSC sebagai metode untuk memecahkan jenis enkripsi RSA tertentu. Khususnya, jika pesan teks biasa yang sama dienkripsi dengan dua kunci publik berbeda yang memiliki faktor yang sama, CRT dapat digunakan untuk memulihkan pesan teks terang asli *(original plaintext)* dan menerobos enkripsi. Serangan ini dapat dilakukan dengan cara yang relatif efisien, menjadikannya ancaman potensial terhadap enkripsi RSA.

Tujuan dari artikel penelitian ini adalah untuk mengeksplorasi penggunaan Teorema Sisa Cina sebagai metode penerobos enkripsi RSA. Kami akan memberikan penjelasan rinci tentang bagaimana TSC dapat menjadi Teknik deksripsi yang dapat dimanfaatkan *cybercrimnals* dalam Kondisi tertentu untuk melakukan serangan terhadap Teknik kriptografi RSA. Penjelasan ini termasuk analisis matematis dan algoritma yang terlibat. Juga akan dibahas batasan serangan dan potensi penanggulangan yang dapat digunakan untuk mencegahnya. Terakhir, kami akan menyajikan hasil eksperimen dan simulasi yang dilakukan untuk menguji keefektifan serangan TSC, dan mendiskusikan implikasi hasil ini untuk keamanan enkripsi RSA.

II. METODE PENELITIAN

Penelitian ini diawali dengan studi leteratur secara komprehensif tentang algoritma kriptografi RSA dalam pengamanan data, secara khusus studi ini menampilkan analisis matematis terkait Teknik kriptografi RSA. Selain itu, Teknik TSC juga akan dipaparkan dengan rinci dari sisi algoritma matematisnya, sehingga menjadi dasar dalam diskusi komprehensif penelitian ini.

A. Kriptografi Rivest-Shamir-Adleman (RSA)

Enkripsi RSA adalah algoritme kriptografi yang banyak digunakan yang bergantung pada kesulitan memfaktorkan angka besar untuk memastikan keamanan komunikasi dan transaksi online. Enkripsi RSA bekerja dengan menggunakan sepasang kunci, yakni kunci public *(public key)* yang diketahui semua orang dan kunci privat *(private key)* yang dirahasiakan oleh pemiliknya. Kunci publik digunakan untuk mengenkripsi pesan, sedangkan kunci privat digunakan untuk mendekripsi pesan (Tan et al., 2011).

Langkah-langkah dasar yang ditempuh dalam proses enkripsi RSA adalah sebagai berikut:

1. Pengirim memilih pesan yang akan dienkripsi dan mengubahnya menjadi nilai numerik.
2. Pengirim kemudian menggunakan kunci publik penerima untuk mengenkripsi nilai numerik.
3. Pesan terenkripsi dikirim ke penerima.
4. Penerima menggunakan kunci privatnya untuk mendekripsi pesan terenkripsi kembali ke nilai numerik aslinya, yang kemudian dapat diubah kembali menjadi pesan aslinya.

Keamanan enkripsi RSA bergantung pada fakta umum bahwa sulit secara komputasi untuk memfaktorkan N ke dalam faktor primanya dan menghitung $\phi(N)$ hanya dengan N. Ini berarti bahwa penyerang yang mengetahui kunci publik (N, e) harus memfaktorkan N untuk menentukan kunci privat d dan mendekripsi ciphertext. Memfaktorkan bilangan besar dianggap sebagai masalah yang sulit, bahkan dengan komputer dan algoritme yang canggih. Namun, kemajuan dalam teknologi komputasi dan teknik matematika baru telah menyebabkan perkembangan serangan yang dapat mengeksploitasi kelemahan tertentu dalam enkripsi RSA dan berpotensi membahayakan keamanannya.

Kriptografi RSA banyak digunakan dalam berbagai aplikasi, termasuk komunikasi email aman (PGP), penelusuran web aman (SSL/TLS), transfer file aman (SFTP), tanda tangan digital, dan protokol pertukaran kunci (Suga, 2012; Ginting, Isnanto and Windasari, 2015). Ini menyediakan cara yang aman untuk mentransmisikan informasi melalui jaringan

publik dengan memastikan kerahasiaan dan integritas melalui proses enkripsi dan dekripsi.

Enkripsi RSA didasarkan pada konsep matematika - eksponensial modular - yang dapat digunakan untuk secara efisien menghitung pangkat besar modolu dari dua bilangan. Berikut adalah bukti matematis singkat tentang cara kerja kriptografi RSA, yg dapat dijabarkan dalam setiap tahapannya:

1. Pembuatan Pasangan Kunci *(penerima)*
   - Pilih dua bilangan prima yang relatif berukuran sama besar p dan q, dan hitung hasilnya $n = pq$.
   - Hitung fungsi *totient Euler* dari *N* sebagai $\phi(n) = (p-1)(q-1)$.
   - Pilih bilangan bulat acak e sehingga gcd $[e, \phi(n)] = 1$ dan $1 < e < \phi(n)$, dan e adalah koprima $\phi(n)$.
   - Hitung eksponen privat d dalam interval $1 < d < \phi$ sehingga $ed = 1 \pmod{\phi(N)}$, atau dengan kata lain, $d = e^{-1} \bmod \phi(n)$.
   - Kunci publik adalah (e, n) dan kunci privat adalah (d, n).
2. Enkripsi *(pengirim)*
   - Dapatkan kunci publik penerima (e, n).
   - Enkripsikan pesan teks asli M menggunakan kunci publik, $C = E_{(e,n)}(M) = M^e \bmod n$.
3. Dekripsi (*penerima*)
   - Menerima $C = M^e \bmod n$.
   - Dekripsikan C menggunakan kunci privat $D_d(C) = C^d \bmod n = M$

B. Teorema Sisa Cina (TSC)

Teorema Sisa Cina adalah teorema yang memberikan solusi unik untuk kongruensi linier simultan dengan koprima modulus. Dalam bentuk dasarnya, teorema sisa Cina akan menentukan bilangan p yang, jika dibagi dengan beberapa pembagi tertentu, akan menghasilkan sisa. Dengan kata lain, teorema ini menyatakan bahwa jika sebuah sistem dikatakan kongruensi linier dalam bentuk $x \equiv a_i \ (mod\ n_i)$, di mana x adalah variabel yang tidak diketahui, a_i adalah sisanya, dan n_i adalah bilangan bulat koprima berpasangan, maka ada solusi unik untuk x modulo produk dari semua n_i (Kim et al., 2011).

Teorema 1. *Misalkan $m_1, m_2, \dots m_n$ adalah merupakan pasangan bilangan relatif prima, yaitu $gcd(m_i, m_j) = 1$ untuk semua i dan j kurang dari atau sama dengan n dimana $i \neq j$. Maka, sistem kongruensi:*

$$X \equiv a_1 \big(mod(m_1)\big)$$
$$X \equiv a_2 \big(mod(m_2)\big)$$
$$\vdots \qquad \vdots$$
$$X \equiv a_n \big(mod(m_n)\big)$$

memiliki solusi yang unik modulo bilangan bulat $m_1, m_2, \dots m_n$.

Bukti formal TSC ini dapat dilihat dalam (Ding, Pei and Salomaa, 1996)

III. HASIL DAN PEMBAHASAN

A. Simulasi Enkripsi-Dekripsi RSA

Untuk mensimulasikan proses pembuatan kunci, enkripsi, dan dekripsi menggunakan kriptografi RSA, kita akan mengikuti tahapan yang telah dijabarkan sebelumnya untuk menentukan komponen-komponen enkripsi dan dekripsi. Berikut simulasi prosesnya dengan menggunakan frasa "***Sa suka kriptografi skali karna sangat matematik***", dimulai dengan pemilihan dua bilangan prima yang sangat besar $p = 426438818303$ dan $q = 239848433481$.

Pertama, untuk memulai simulasi, frasa *"Sa suka kriptografi skali karna sangat matematik"* perlu dikonversi ke dalam representasi numeriknya menggunakan kode ASCII dalam table berikut:

S	a		s	u	k	a		k
83	97	32	115	117	107	97	32	107
r	i	p	t	o	g	r	a	f
114	105	112	116	111	103	114	97	102
i		s	k	a	l	i		k
105	32	115	107	97	108	105	32	107
a	r	n	a		s	a	n	g
97	114	110	97	32	115	97	110	103
a	t		m	a	t	e	m	a
97	116	32	109	97	116	101	109	97
t	i	k						
116	105	107						

Selanjutnya dengan menggunakan nilai prima p dan q, dan memilih nilai e (mis. e =65537), dapat ditentukan beberapa nilai lainnya:

1. $n = 102110225956749542141843$,
2. $\phi(n) = 102110225956748218690560$,
3. $d = 27179316567567952573761$.

Proses ini memberikan 2 pasangan kunci RSA, kunci publik (e, n) dan kunci privat (d, n), secara berturut-turut $(e, n) = (65537, 102110225956749542141843)$ dan $(d, n) = (27179316567567952573761, 102110225956749542141843)$.

Selanjutnya representasi numerik dari frasa yang telah dikonversi ke dalam kode ASCII dapat dienkripsi menggunakan kunci publik yang dihasilkan, sehingga memberikan teks tersamar, c, berikut:

```
609491669719937727309599005
027660034248157289034089134
```

114529072675095832115246743
817763441827147060861610790
453270798534038801590898784
434628695577938713647998825
838137172764255580618057058
619431066888552556932717146
94048742570334846303

Pada proses dekripsi RSA, pesan tersamar, C ini dipangkatkan dengan kunci privat d dan dikalikan dengan modulo n, yakni, C^d mod n, yang memberikan hasil komputasi, 5.99999999999999995515864e+70. Nilai ini sangat besar untuk ditunjukkan sebagaimana nilai C.

Namun, nilai perhitungan tersebut setelah dikonversikan ke dalam nilai numerik kode ASCII, diperoleh:

83	97	32	115	117	107	97	32	107
114	105	112	116	111	103	114	97	102
105	32	115	107	97	108	105	32	107
97	114	110	97	32	115	97	110	103
97	116	32	109	97	116	101	109	97
116	105	107						

yang tidak lain adalah representasi numerik dari pesan asli, yakni *"Sa suka kriptografi skali karna sangat matematik"*

B. Simulasi Dekripsi TSC

Mendekripsi pesan tersamar *(ciphertext)* menggunakan Teorema Sisa Cina (TSC), diperlukan komponen kunci privat (d, p, q) untuk menurunkan plaintext. Berikut proses dekripsinya:

1. Gunakan ciphertext yang sama pada proses sebelumnya.
2. Komponen kunci privat:
   - $d = 27179316567567952573761$
   - $p = 426438818303$
   - $q = 239848433481$
3. Hitung Invers Modular:
   - $q_{inv} = q^{-1} \, mod \, p = 107028463628$
   - $p_{inv} = p^{-1} \bmod q = 228201012031$
4. Hitung Eksponensial:
   - $m_1 = C^{d \, mod \, (p-1)} \bmod p$
     $m_1 = 346686531586$
   - $m_2 = C^{d \, mod \, (q-1)} \bmod q$
     $m_2 = 77529881066$
5. Terapkan TSC, hitung:
   - $\mathrm{h} = \left(q_{inv} * (m_1 - m_2)\right) \bmod \mathrm{p}$
     $h = 113445998768$
   - $plaintext = m_2 + h * q$
     $= 25331947167078189188896$

Selanjutnya dengan mengubah representasi numerik dari teks asli yang didekripsi kembali ke frase asli menggunakan kode ASCII:

83 97 32 115 117 107 97 32 107 114 105 112 116 111 103 114 97 102 105 32 115 107 97 108 105 32 107 97 114 110 97 32 115 9 7 110 103 97 116 32 109 97 116 101 109 97 116 105 107

Plaintext yang didekripsi menggunakan Teorema Sisa Cina adalah "*Sa suka kriptografi skali karna sangat matematik*", yang sesuai dengan frasa aslinya.

C. Diskusi

Kriptografi RSA adalah teknik enkripsi yang banyak digunakan berdasarkan algoritma RSA, yang dinamai menurut penemunya *Ron Rivest, Adi Shamir, dan Leonard Adleman*. Teknik ini merupakan bentuk kriptografi asimetris atau kriptografi kunci publik, yang memungkinkan komunikasi yang aman dan perlindungan data melalui jaringan yang tidak aman.

Dalam kriptografi RSA, dua kunci digunakan untuk mengenkripsi (kunci publik) dan kunci privat untuk dekripsi. Kunci publik dibagikan secara bebas dan dapat diketahui oleh siapa saja, sedangkan kunci privat dirahasiakan oleh pemiliknya.

Secara matematis, enkripsi RSA melibatkan operasi eksponensial modular, yang membutuhkan waktu yang sangat lama dan mahal secara komputasi untuk jumlah faktorisasi besar. Kompleksitas waktu enkripsi RSA biasanya $O\big(log(e)\big)$, di mana e adalah eksponen publik. Oleh karena itu, waktu enkripsi meningkat secara logaritma dengan ukuran eksponen, seperti yang ditunjukkan dalam hasil simulasi studi ini di mana membutuhkan $\approx 6x10^{70}$ iterasi untuk dapat mendekripsikan pesan asli.

Di sisi lain, dengan menggunakan Teorema Sisi Cina, seseorang dapat menerobos/ mendekripsikan pesan tersamar untuk memeproleh teks asli *(plaintext)* dengan memanfaatkan efisiensi dan kecepatan TSC dalam proses dekripsi.

Dengan memanfaatkan komputasi terpisah untuk setiap faktor utama modulus, CRT memungkinkan pemrosesan paralel dan mengurangi beban komputasi. Dalam simulasi, proses dekripsi berbasis CRT lebih cepat dibandingkan dengan dekripsi RSA standar, terutama ketika berhadapan dengan bilangan prima besar dan eksponensial modular kompleks.

Selain itu, CRT mengurangi ukuran modulus dengan melakukan eksponensial modulo bilangan prima yang lebih kecil, membuat perhitungan lebih efisien. Dalam simulasi,

penggunaan CRT memungkinkan kita untuk melakukan perhitungan modulo p dan q daripada modulus penuh, sehingga dekripsi lebih cepat.

IV. KESIMPULAN DAN SARAN

A. Simpulan

Dari hasil penelitian ini dapat ditarik beberapa kesimpulan, sebagai berikut:

1. *Waktu Eksekusi*: metode dekripsi berbasis TSC umumnya menawarkan keunggulan kinerja dibandingkan dekripsi RSA standar. Dengan memanfaatkan Teorema ini, pendekatan berbasis TSC memecah komputasi menjadi eksponensial modular yang lebih kecil, mengurangi beban komputasi secara keseluruhan.
2. *Efisiensi*: dekripsi berbasis TSC mendapat manfaat dari sifat paralel dari perhitungan yang terlibat. TSC melakukan perhitungan terpisah modulo faktor utama, memungkinkan pemrosesan simultan dan eksekusi lebih cepat dibandingkan dengan dekripsi RSA standar, yang beroperasi pada seluruh modulus.
3. *Dampak Ukuran Modulus*: ukuran modulus berperan penting dalam menentukan perbedaan kinerja antara kedua metode dekripsi. Ketika modulus meningkat menjadi lebih besar, keuntungan dari pendekatan berbasis TSC menjadi lebih jelas karena berkurangnya kompleksitas komputasi dari eksponensial modular dengan eksponen yang lebih kecil.
4. *Pertimbangan Implementasi*: Efisiensi algoritma yang digunakan dalam implementasi juga mempengaruhi waktu eksekusi. Dengan memanfaatkan algoritma yang dioptimalkan untuk eksponensial modular dan operasi invers modular dapat lebih meningkatkan kinerja kedua metode dekripsi.

B. Saran

Penelitian ini menggunakan data text tersamar sebagai bahan kajian proses enkripsi-dekripsi. Namun, dalam praktik pengamanan data konfidensialn, tipe-tipe berformat lain seperti, audio dan video juga dapat dienkripsi. Sehingga, disarankan pada penelitian lain dapat menggunakan jenis data terenkripsi yang lain.

Selain itu, dapat juga dilakukan studi analisis matematik menggunakan metode lain seperti *General Number Field Sieve (GNFS)* sebagai tool untuk memfaktor bilangan-bilangan prima berukuran sangat besar.

DAFTAR RUJUKAN

Ding, C., Pei, D. and Salomaa, A., 1996. *Chinese Remainder Theorem: Applications in Computing, Coding, Cryptography*. World Scientific.

Ginting, A., Isnanto, R.R. and Windasari, I.P., 2015. Implementasi Algoritma Kriptografi RSA untuk Enkripsi dan Dekripsi Email. *Jurnal Teknologi dan Sistem Komputer*, [online] 3(2), p.253. https://doi.org/10.14710/jtsiskom.3.2.2015.253-258.

Kim, S.K., Kim, T.H., Han, D.G. and Hong, S., 2011. An efficient CRT-RSA algorithm secure against power and fault attacks. *Journal of Systems and Software*, 84(10), pp.1660–1669. https://doi.org/10.1016/j.jss.2011.04.026.

Menezes, A.J., van Oorschot, P.C. and Vanstone, S.A., 1997. *HANDBOOK of APPLIED CRYPTOGRAPHY*. 1st ed. CRC Press.

Suga, Y., 2012. SSL/TLS status survey in Japan - Transitioning against the renegotiation vulnerability and short RSA key length problem. In: *Proceedings of the 2012 7th Asia Joint Conference on Information Security, AsiaJCIS 2012*. pp.17–24.
https://doi.org/10.1109/AsiaJCIS.2012.10.

Tan, W., Wang, X., Lou, X. and Pan, M., 2011. Analysis of RSA based on quantitating key security strength. In: *Procedia Engineering*. pp.1340–1344. https://doi.org/10.1016/j.proeng.2011.08.248.

Zhao, Y.-D. and Qi, W.-F., 2007. Small Private-Exponent Attack on RSA with Primes Sharing Bits. In: *Information Security: 10th International Conference*. Valparaıso, Chile: Springer Berlin Heidelberg. pp.222–229.