Walisongo Journal of Information Technology, Vol. 2 No. 1 (2020): 13-26
DOI : http://dx.doi.org/10.21580/wjit.2020.2.1.5402


# Komparasi Waktu Algoritma RSA Dengan RSA-CRT Base On Computer

Nur Cahyo Hendro Wibowo [1], Khotibul Umam [2], Afrikhatul Hikmah [3],
Albradru Muh Izul Khaq [4], Favian Agung Rizki [5]
[1, 2, 3, 4, 5] Universitas Islam Negeri Walisongo
[1] nciain123@gmail.com, [2] khothibul_umam@walisongo.ac.id, [3] albertizzulhaq@gmail.com

***Abstract***

*Cryptography is a branch of mathematics. Asymmetric algorithms such as RSA, including the type of cryptography that is more widely used to be implemented in everyday life because it has an algorithm that is not easy to be misused by others. However, the encryption and decryption process of RSA requires quite a long time. For this reason, RSA - CRT emerged. In this study a time comparison between the RSA algorithm and the RSA-CRT Base On Computer is done. The purpose of this study was to determine the execution time of the RSA-CRT algorithm using PHP. This research uses the Research and Development or R&D method, with the R&D method created by the product development RSA-CRT algorithm application from UIN Walisongo Semarang based on computer. Based on the data analysis, the conclusion is that although the manual calculation of the RSA-CRT algorithm takes longer than the others in this case RSA. But have a faster time when using PHP. The trial in the form of the word "Islamic State University" resulted in an execution time of 0.00062298774719238 at the RSA-CRT, while the execution time at the RSA was 0.0077469348907471.*

***Keywords :*** *Encryption, Decryption, RSA-CRT.*

**Abstrak**

Kriptografi merupakan salah satu cabang ilmu matematika. Algoritma asimetris seperti RSA termasuk jenis kriptografi yang lebih banyak digunakan untuk diimplementasikan dalam kehidupan sehari – hari karena mempunyai algoritma yang tidak mudah untuk disalah gunakan orang lain. Namun, dalam proses enkripsi dan dekripsinya RSA membutuhkan waktu yang cukup lama. Untuk itu munculah RSA – CRT. Pada Penelitian dilakukan komparasi waktu antara algoritna RSA dengan RSA-CRT Base On Computer. Tujuan penelitian ini adalah untuk mengetahui waktu eksekusi dari algoritma RSA-CRT menggunakan PHP. Metode yang digunakan adalah metode Research and Development atau R&D, dengan metode R&D tercipta pengembangan produk Aplikasi algoritma RSA-CRT dari UIN Walisongo semarang base on computer. Berdasarkan analisis data yang dilakukan, diperoleh kesimpulan bahwa meskipun secara perhitungan manual algoritma RSA-CRT membutuhkan waktu yang lebih lama dibanding yang lain dalam hal ini RSA. Namun mempunyai waktu yang lebih cepat ketika menggunakan PHP. Uji coba berupa kata "Universitas Islam Negeri" menghasilkan waktu eksekusi 0.00062298774719238 pada RSA-CRT, sedangkan waktu eksekusi pada RSA 0.0077469348907471.

**Kata Kunci :** Enkripsi, Dekripsi, RSA-CRT.

ISSN 2715-0143 (online) ISSN 2714-9048 (print)
http://journal.walisongo.ac.id/index.php/jit/index

## 1. LATAR BELAKANG

Saat ini teknologi berkembang sangat pesat. Hampir diseluruh bidang kehidupan manusia menggunakan teknologi. Teknologi memberikan pengaruh besar terhadap kehidupan manusia di antaranya dapat menyebabkan perubahan di berbagai sektor seperti pendidikan, transportasi, kedokteran, komunikasi dan lain sebagainya. Seiring perkembangan zaman, muncul berbagai macam bentuk teknologi. Seperti teknologi komunikasi, teknologi transportasi, teknologi medis dan teknologi informasi. Menurut Alba, supriana dan mahzar (2004) abad ke 21 ini adalah "abad yang penuh dengan perubahan yang sangat cepat dan semakin dipercepat jika dilihat dari sudut teknologi, terutama teknologi informasi" (Alba, Supriana, & Mahzar, 2004).

Teknologi informasi diartikan sebagai teknologi untuk memperoleh, mengolah, menyimpan dan menyebarkan berbagai jenis file informasi dengan memanfaatkan komputer dan telekomunikasi yang lahir dari dorongan – dorongan kuat untuk menciptakan inovasi dan kreatifitas baru yang dapat mengatasi segala kemalasan dan kelambatan kinerja manusia (Affandi, 2017). Sedangkan menurut (Suryana & Koesheryatin, 2014) Teknologi Informasi adalah "kajian, desain, pengembangan, implementasi, dukungan, atau manajemen sistem informasi yang berbasis komputer, khususnya aplikasi perangkat lunak dan perangkat keras". Dalam perkembangannya, pengertian teknologi informasi kemudian dikaitkan dengan penggunaan internet sebagai media pengiriman dan penerimaan informasi.

Manusia mampu memperoleh informasi secara cepat melalui teknologi informasi ini di antaranya menggunakan internet. Salah satu indikator berkembangnya teknologi adalah adanya internet. Di lain sisi perkembangan teknologi infomasi melalui internet ini juga memiliki kekurangan bagi penggunanya yaitu rentan nya informasi yang mampu disalahgunakan (mengambil maupun mengubah) oleh pihak lain yang tidak berhak atas informasi tersebut melalui internet. Banyak kasus yang berkaitan dengan masalah keamanan baik di luar negri maupun di Indonesia. Salah satu contoh kasus adalah September dan Oktober 2000. Setelah berhasil membobol bank Lippo, kembali Fabian Clone beraksi dengan menjebol web milik Bank Bali (Mono, 2010). Perlu diketahui bahwa kedua bank ini memberikan layanan *Internet banking*. Dengan kata lain, keamanan data sangat penting dalam menjaga kerahasiaan informasi yang hanya boleh diketahui isinya oleh pihak tertentu, sehingga perlu adanya penyandian data supaya pihak lain yang tidak berhak atas informasi tersebut tidak akan dapat membuka informasi yang dikirim.

"Kriptografi merupakan studi teknik matematika yang berkaitan dengan aspek keamanan informasi seperti kerahasian, integritas data, dan autentikasi" (Vanstone, Oorschot,

& Scott, 1997). Dengan kata lain, tujuan kriptografi salah satunya adalah menjaga serta mengamankan informasi yang bersifat rahasia. Di antaranya informasi berbentuk teks alphabet.

Kriptografi mempunyai dua algoritma yakni algoritma simetris di mana kunci untuk enkripsi sama dengan kunci dekripsi, dan algoritma asimetris di mana antara kunci enkripsi dan dekripsinya berbeda. Algoritma asimetris membutuhkan sepasang kunci yakni satu kunci untuk enkripsi yang disebut dengan kunci publik dan satu kunci untuk dekripsi yang disebut dengan kunci privat. Dilihat dari keamanan data, algoritma asimetri lebih baik dibandingkan dengan algoritma simetri. Kunci simetri harus dikirim melalui saluran aman serta harus sering diubah pada setiap sesi komunikasi. Sedangkan, kunci asimetri hanya kunci privat yang perlu dijaga kerahasiaannya oleh setiap entitas yang berkomuniaksi (tetapi, otentikasi kunci publik tetap harus terjamin). Tidak ada kebutuhan mengirim kunci privat sebagaimana pada sistem simetri serta pasangan kunci publik/kunci privat tidak perlu diubah, bahkan dalam periode waktu yang panjang (Munir, 2004).

Banyak algoritma yang digunakan oleh orang untuk melakukan pengamanan data tersebut di antaranya algoritma RSA, Elgamal, *Data Encryption Standar* (DES), RC4, *Advance Encryption Standar*(AES) dan lain sebagainya. RSA termasuk salah satu jenis dari algoritma asimetris. Algoritma RSA populer karena keamanannya. "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" (Munir, 2004). Meskipun dari segi keamanan algoritma ini bagus. Namun, dalam proses Enkripsi dan dekripsi data umumnya lebih lambat daripada algoritma simetri, karena enkripsi dan dekripsi menggunakan bilangan yang besar dan melibatkan operasi perpangkatan yang besar (Munir, 2004). Pada perkembangannya, muncul algoritma kriptografi jenis RSA yakni algoritma RSA-CRT. Menurut Rifki Sadikin dalam bukunya yang berjudul kriptografi untuk keamanan jaringan (Sadikin, 2012) algoritma RSA – CRT memiliki waktu proses yang lebih cepat dibandingkan dengan algoritma RSA biasa yakni sekitar empat kali lebih cepat. Dalam menotasikan algoritma tersebut, banyak bahasa pemrograman yang dapat digunakan. Seperti ASP.NET, Java, Ruby, PHP dan lain sebagainya.

Kriptografi asimetri merupakan jenis kriptografi yang memiliki kunci berbeda dalam proses enkripsi dan deskripsi. Sehingga, kriptografi jenis ini memiliki nilai keamanan yag lebih dibandingkan dengan kriptografi simetri. Salah satu kriptografi asimetri adalah RSA. RSA memiliki tiga algoritma dalam prosesnya yakni pembangkitan kunci, Enkripsi dan Deskripsi. Meskipun Algoritma RSA

ini memiliki nilai keamanan yang lebih dibandingkan dengan jenis kriptografi simetri, algoritma RSA memiliki waktu proses yang cukup lambat. Oleh karena itu, muncul RSA – CRT yakni algoritma dengan tambahan Chinese Remainder Theorema. Algoritma RSA-CRT sama seperti halnya algoritma RSA yakni memiliki tiga proses seperti pembangkitan kunci, enkripsi dan dekripsi. Perbedaan RSA – CRT ini terletak pada proses pembangkitan kunci dan dekripsinya. Pada penelitian ini, penulis membuat program kriptografi RSA-CRT menggunakan bahasa pemrograman PHP melalui teks editor sublime Teks. Penulis membuat tampilan sederhana yang terdiri dari halaman masuk, halaman depan, dan halaman utama.

## 2. TINJAUAN PUSTAKA

Peneliti menemukan beberapa bahan bacaan yang bisa dijadikan referensi di antaranya skripsi dengan judul " Aplikasi Algoritma RSA Untuk Keamanan Data pada Sistem Informasi Berbasis Web " oleh Dadan Rosnawan mahasiswa Jurusan Matematika Fakultas Matematika dan Ilmu pengetahuan Alam Universitas Negeri Semarang tahun 2011. Karya Ilmiah yang berjudul "Aplikasi Kriptografi dengan Metode Vigenere Chiper Berbasis Web " oleh Melati Mawardina dan Entik Insanudin, M.T. dari Teknik Informatika Fakultas Sains dan Teknologi UIN Sunan Gunung Djati Bandung tahun 2016. Jurnal dari QUERY: Jurnal Sistem Informasi volume :01, Nomor :01, April 2017 ISSN 2579-5342 (online) dengan berjudul " Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data di Kanwil Kementerian Agama Prov. Sumatera Utara " oleh Niti Ravika Nasution.

Referensi pertama, berisi peneliti tersebut menggunakan kriptografi RSA. Sedangkan di sini peneliti menggunkaan Algoritma RSA-CRT. Referensi kedua, peneliti tersebut membuat aplikasi Vigenere Chiper menggunakan PHP di mana algoritma ini termasuk ke dalam kriptografi simetris, sedangkan penulis menggunakan algoritma kriptografi asimetris yang mempunya tingkat keamanan yang lebih seperti yang telah dijelaskan pada bagian sebelumnya. Referensi ketiga, penulis tersebut mengombinasikan RSA-CRT dengan Random LSB dijelaskan bahwa peneliti tersebut menggunakan bahasa java. Sedangkan penulis di sini menggunakan bahasa PHP.

## 3. METODE PENELITIAN

Metode Penelitian yang digunakan adalah metode Research and Development atau R&D, metode penelitian ini pada dasarnya merupakan cara ilmiah untuk mendapatkan data dengan tujuan dan kegunaan tertentu. Cara ilmiah artinya mencakup rasional, empiris dan sistematis. Data yang diperoleh mempunyai kriteria valid. Kemudian, tujuan penelitian secara umum adalah penemuan, pembuktian dan pengembangan. Terakhir, kegunaan tertentu artinya bisa digunakan untuk memahami, memecahkan dan mengantisipasi masalah. Research

yang digunakan adalah aplikasi algoritma RSA dari STMIK Bumigora Mataram dan algoritma yang dikembangkan adalah algoritma RSA-CRT dari UIN Walisongo semarang base on computer.

## 4. LANDASAN TEORI

A. Definisi Kriptografi

Kata kriptografi berasal dari bahasa Yunani, kryptos yang berarti tersembunyi dan graphein yang berarti tulisan (Andika, 2018). Kriptografi (*cryptography*) merupakan ilmu dan seni untuk menjaga pesan agar aman. (*Cryptography is the art and science of keeping messages secure*) (Stallings, 2005).

B. Istilah dalam kriptografi

Berikut ini istilah – istilah yang ada dalam kriptografi :

1) Kriptologi : ilmu yang mempelajari tentang kriptografi dan kriptanalisis
2) Kriptanalisis : ilmu yang mempelajari cara membobol sistem kriptografi
3) Plainteks : pesan asli yang akan dikirim pengirim kepada penerima
4) Chiperteks : pesan rahasia , pesan asli yang telah melalui proses enkripsi
5) Pengirim : pihak yang mengirim pesan plainteks
6) Penerima : pihak yang menerima pesan chiperteks
7) Enkripsi : proses mengubah plainteks menjadi chiperteks
8) Dekripsi : proses mengubah chiperteks menjadi plainteks
9) Penyadap : pihak yang berusaha mengambil ataupun sekedar memanipulasi pesan.
10) Kunci : suatu bilangan yang digunakan dalam proses enkripsi dan dekripsi (Mahali, 2015). Dalam hal ini, kunci dibagi menjadi dua yakni kunci publik dan kunci privat. Kunci publik yaitu kunci yang digunakan untuk enkripsi sedangkan kunci privat merupakan kunci yang digunakan untuk deskripsi.

C. Proses Algoritma RSA

Proses – proses yang digunakan dalam algoritma RSA terdiri dari tiga proses yaitu :

1) Pembangkitan Kunci

Berikut perhitungan kriptografi RSA (Stallings, 2005) :

a) Pilih dua bilangan prima $p$ dan $q$, di mana $p \neq q$.
b) Hitung $n = p \times q$
c) Hitung $\varphi(n) = (p-1)(q-1)$
d) Pilih bilangan sembarang bulat $e$ di mana $\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$
e) Hitung $d \equiv e^{-1}\big(mod\ \varphi(n)\big)$ atau $e \times d \equiv 1\big(mod\ \varphi(n)\big)$ ekivalen dengan $e \times d = 1 + k\varphi(n)$ sehingga $d = \frac{1+k\varphi(n)}{e}$

Didapatkan kunci publik : $\{e, n\}$ dan kunci publik : $\{d, n\}$.

Langkah awal dalam algoritma RSA adalah pembangkitan kunci. Pertama, memilih dua buah bilangan prima p dan q. Lalu hitung p×q beri simbol n. Setelah itu, hitung fungsi euler φ(n)=(p-1)(q-1). Pilih sembarangan bilangan e antara 1 dan φ(n) serta relatif prima terhadap φ(n). Hitung nilai d yaitu dengan mencari invers e modulo φ(n). Didapatkan nilai e dan d. Kemudian pasangan (e,n) disebut dengan kunci publik dan pasangan (d,n) disebut kunci privat. Kunci publik dan kunci privat ini digunakan untuk enkripsi/deskripsi.

Contoh Algoritma pembangkitan kunci RSA

a) Pilih dua bilangan prima $p = 83$ dan $q = 71$, di mana $p \neq q$.
b) Hitung $n = 83 \times 71 = 5893$
c) Hitung $\varphi(n) = (83 - 1)(71 - 1) = 82 \times 70 = 5740$
d) Pilih bilangan sembarang bulat $e$ di mana $\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$, misal $e = 33$
e) Hitung $d = \frac{1+5740k}{33}$ , didapatkan $d = 2957$ karena terdapat $k = 17 \in$ bilangan bulat, $2957 = \frac{1+5740(17)}{33}$

Sehingga didapatkan kunci publik (33,5893) dan kunci privat (2957,5893).

2) Enkripsi

Selanjutnya algoritma enkripsi pada RSA (Stallings, 2005) :

a) Plainteks : $M < n$
b) Ciperteks : $C = M^e \ mod \ n$

Langkah pertama ubah palinteks ke ASCII

| Dec | Hex | Oct | Chr | Dec | Hex | Oct | HTML | Chr | Dec | Hex | Oct | HTML | Chr | Dec | Hex | Oct | HTML | Chr |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 000 | NULL | 32 | 20 | 040 |   | Space | 64 | 40 | 100 | @ | @ | 96 | 60 | 140 | ` | ` |
| 1 | 1 | 001 | Start of Header | 33 | 21 | 041 | ! | ! | 65 | 41 | 101 | A | A | 97 | 61 | 141 | a | a |
| 2 | 2 | 002 | Start of Text | 34 | 22 | 042 | " | " | 66 | 42 | 102 | B | B | 98 | 62 | 142 | b | b |
| 3 | 3 | 003 | End of Text | 35 | 23 | 043 | # | # | 67 | 43 | 103 | C | C | 99 | 63 | 143 | c | c |
| 4 | 4 | 004 | End of Transmission | 36 | 24 | 044 | $ | $ | 68 | 44 | 104 | D | D | 100 | 64 | 144 | d | d |
| 5 | 5 | 005 | Enquiry | 37 | 25 | 045 | % | % | 69 | 45 | 105 | E | E | 101 | 65 | 145 | e | e |
| 6 | 6 | 006 | Acknowledgment | 38 | 26 | 046 | & | & | 70 | 46 | 106 | F | F | 102 | 66 | 146 | f | f |
| 7 | 7 | 007 | Bell | 39 | 27 | 047 | ' | ' | 71 | 47 | 107 | G | G | 103 | 67 | 147 | g | g |
| 8 | 8 | 010 | Backspace | 40 | 28 | 050 | ( | ( | 72 | 48 | 110 | H | H | 104 | 68 | 150 | h | h |
| 9 | 9 | 011 | Horizontal Tab | 41 | 29 | 051 | ) | ) | 73 | 49 | 111 | I | I | 105 | 69 | 151 | i | i |
| 10 | A | 012 | Line feed | 42 | 2A | 052 | * | * | 74 | 4A | 112 | J | J | 106 | 6A | 152 | j | j |
| 11 | B | 013 | Vertical Tab | 43 | 2B | 053 | + | + | 75 | 4B | 113 | K | K | 107 | 6B | 153 | k | k |
| 12 | C | 014 | Form feed | 44 | 2C | 054 | , | , | 76 | 4C | 114 | L | L | 108 | 6C | 154 | l | l |
| 13 | D | 015 | Carriage return | 45 | 2D | 055 | - | - | 77 | 4D | 115 | M | M | 109 | 6D | 155 | m | m |
| 14 | E | 016 | Shift Out | 46 | 2E | 056 | . | . | 78 | 4E | 116 | N | N | 110 | 6E | 156 | n | n |
| 15 | F | 017 | Shift In | 47 | 2F | 057 | / | / | 79 | 4F | 117 | O | O | 111 | 6F | 157 | o | o |
| 16 | 10 | 020 | Data Link Escape | 48 | 30 | 060 | 0 | 0 | 80 | 50 | 120 | P | P | 112 | 70 | 160 | p | p |
| 17 | 11 | 021 | Device Control 1 | 49 | 31 | 061 | 1 | 1 | 81 | 51 | 121 | Q | Q | 113 | 71 | 161 | q | q |
| 18 | 12 | 022 | Device Control 2 | 50 | 32 | 062 | 2 | 2 | 82 | 52 | 122 | R | R | 114 | 72 | 162 | r | r |
| 19 | 13 | 023 | Device Control 3 | 51 | 33 | 063 | 3 | 3 | 83 | 53 | 123 | S | S | 115 | 73 | 163 | s | s |
| 20 | 14 | 024 | Device Control 4 | 52 | 34 | 064 | 4 | 4 | 84 | 54 | 124 | T | T | 116 | 74 | 164 | t | t |
| 21 | 15 | 025 | Negative Ack. | 53 | 35 | 065 | 5 | 5 | 85 | 55 | 125 | U | U | 117 | 75 | 165 | u | u |
| 22 | 16 | 026 | Synchronous idle | 54 | 36 | 066 | 6 | 6 | 86 | 56 | 126 | V | V | 118 | 76 | 166 | v | v |
| 23 | 17 | 027 | End of Trans. Block | 55 | 37 | 067 | 7 | 7 | 87 | 57 | 127 | W | W | 119 | 77 | 167 | w | w |
| 24 | 18 | 030 | Cancel | 56 | 38 | 070 | 8 | 8 | 88 | 58 | 130 | X | X | 120 | 78 | 170 | x | x |
| 25 | 19 | 031 | End of Medium | 57 | 39 | 071 | 9 | 9 | 89 | 59 | 131 | Y | Y | 121 | 79 | 171 | y | y |
| 26 | 1A | 032 | Substitute | 58 | 3A | 072 | : | : | 90 | 5A | 132 | Z | Z | 122 | 7A | 172 | z | z |
| 27 | 1B | 033 | Escape | 59 | 3B | 073 | ; | ; | 91 | 5B | 133 | [ | [ | 123 | 7B | 173 | { | { |
| 28 | 1C | 034 | File Separator | 60 | 3C | 074 | < | < | 92 | 5C | 134 | \ | \ | 124 | 7C | 174 | | | \| |
| 29 | 1D | 035 | Group Separator | 61 | 3D | 075 | = | = | 93 | 5D | 135 | ] | ] | 125 | 7D | 175 | } | } |
| 30 | 1E | 036 | Record Separator | 62 | 3E | 076 | > | > | 94 | 5E | 136 | ^ | ^ | 126 | 7E | 176 | ~ | ~ |
| 31 | 1F | 037 | Unit Separator | 63 | 3F | 077 | ? | ? | 95 | 5F | 137 | _ | _ | 127 | 7F | 177 | &#127; | Del |

asciichars.com

Kemudian kelompokan menjadi M=m_1,…,m_i<n. Kemudian hitung C=M^e mod n dengan Cadalah himpunan chiperteks dan Madalah himpunan Plainteks atau bisa ditulis berturut – turut sebagai berikut :

C ={c_1,c_2,…,c_i} dan M ={m_1,m_2,…,m_i}. Proses enkripsi dilakukan oleh pihak pengirim, dengan menggunakan kunci publik

(n,e) yang telah didapatkan pada pembangkitan kunci sebelumnya.

3) Dekripsi

Proses deskripsi dilakukan oleh pihak penerima chiperteks menggunakan kunci privat $(n, d)$. Berikut ini adalah proses deskripsi.

a) Chiperteks : C

b) Plainteks : $M = C^d \bmod n$

Langkah pertama, kelompokan chiperteks dengan syarat $C = c_1, \dots, c_i < n$. Hitung $M = C^d \, mod \, n$ dengan $C$ adalah $\{c_1, c_2, \dots, c_i\}$ dan $M$ adalah $\{m_1, m_2, \dots, m_i\}$.

D. RSA-CRT

RSA – CRT merupakan Algoritma RSA yang menggunakan teori CRT (*Chinese Remainder Theorem*).

1) CRT

*Chinese Remainder Theorem* atau yang biasa disebut degan CRT diperkenalkan oleh matematikawan dari Cina yaitu Sun-Tsu. Seperti disebutkan dalam bukunya stalling yang berjudul *Cryptography and Network Security (4th Edition). One of the most useful results of number theory is the Chinese remainder theorem (CRT). The CRT is so called because it is believed to have been discovered by the Chinese mathematician Sun-Tsu in around 100 A.D.(Stallings, 2005).*

Teorema ini bisa digunakan untuk mencari suatu bilangan dari pembagi dan sisa bagi.Jika kita mempunyai beberapa persamaan dengan modulus berbeda sebagai berikut:

$$x \equiv a_1 \, (mod \, m_1)$$
$$x \equiv a_1 \, (mod \, m_1)$$
$$\dots \quad \dots$$
$$x \equiv a_1 \, (mod \, m_1)$$

dimana setiap pasangan modulus adalah koprima (gcd(m_i,m_j )=1 untuk i≠ j), maka terdapat solusi untuk x. Jika x_1 dan x_2 merupakan solusi untuk x, maka x_1≡x_2 (mod M) dimana M=m_1 m_2…m_r.

Pembuktian bahwa sistem persamaan seperti diatas mempunyai solusi untuk x bersifat konstruktif, jadi menghasilkan algoritma untuk mencari solusi. Kita definisikan M_i=M/m_i , jadi M_i merupakan produk dari semua modulus kecuali m_i. Karena gcd(m_i,M_i) = 1, maka terdapat bilangan bulat N_i (inverse yang dapat dicari menggunakan extended Euclidean algorithm) dimana M_i N_i ≡ 1 (mod m_i). Maka suatu solusi untuk x adalah

$$x = \sum_{j=1}^{r} a_j M_j N_j \dots . (2.2)$$

Untuk setiap i, karena semua suku kecuali suku i dapat dibagi dengan m_i, maka hanya suku i yang tidak ≡ 0 (mod mi), jadi

x≡a_i M_i N_i≡a_i (mod m_i) ….(2.3)

seperti yang dikehendaki. Untuk menunjukkan bahwa solusi x unik modulo M, kita tunjukkan bahwa jika x_1 dan x_2 adalah solusi untuk x, maka x_1≡x_2 (mod M). Untuk setiap i, x_1 ≡x_2≡ a_i (mod m_i), atau x_1-x_2≡0(mod m_i). Jadi x_1-x_2≡0 (mod M), yang berarti x_1≡x_2 (mod M)

(Kromodimoeljo, 2009). Berikut prosedur untuk menentukan nilai x:

a) Hitung $M = m_1 \times m_2 \times \ldots \times m_i$

b) Hitung $M_1 = \frac{M}{m_1}$, $M_2 = \frac{M}{m_2}$, ..., $M_i = \frac{M}{m_i}$

c) Temukan invers perkalian $M_1^{-1}, M_2^{-1}, \ldots, M_i^{-1}$ dengan menggunakan modulus $m_1, m_2, \ldots, m_i$

d) Temukan $x$ dengan menghitung $x = (a_1 \times M_1 \times M_1^{-1} + \cdots + a_k \times M_i \times M_i^{-1}) \, mod \, M$

Contoh 12:

Temukan sebuah bilangan integer positif yang bila dibagi 3 bersisa 1, dibagi 4 bersisa 3 dan dibagi 5 bersisa 4.

Jawab :

$$x \equiv 1 \, mod \, 3$$
$$x \equiv 3 \, mod \, 4$$
$$x \equiv 4 \, mod \, 5$$

Sehingga nilai $x$ dapat ditemukan sebagai berikut :

a) Hitung $M = 3 \times 4 \times 5 = 60$

b) Hitung $M_1 = \frac{60}{3} = 20$, $M_2 = \frac{60}{4} = 15$, $M_3 = \frac{60}{5} = 12$

c) $M_1^{-1} = 2$, $M_2^{-1} = 3$, $M_3^{-1} = 3$

d) Temukan $x$ dengan menghitung

$$x = (1 \times 20 \times 2) + (3 \times 15 \times 3) + (4 \times 12 \times 3) \, mod \, 60 = 19$$

2) Proses Algoritma RSA-CRT

Proses algoritma RSA-CRT sama seperti halnya dengan proses algoritma RSA, yakni terdiri dari :

a) Pembangkitan Kunci

Pembangkitan kunci pada RSA – CRT hampir sama dengan pembangkitan kunci pada RSA. Berikut ini proses algoritma pembangkitan kuncinya :

(1) Pilih dua bilangan prima $p$ dan $q$, di mana $p \neq q$.
(2) Hitung $n = p \times q$
(3) Hitung $\varphi(n) = (p - 1)(q - 1)$
(4) Pilih bilangan sembarang bulat $e$ di mana $\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$
(5) Hitung $d \equiv e^{-1} (\mathrm{mod}\, \varphi(n))$
(6) Hitung $dP = d \; mod \; (p - 1)$
(7) Hitung $dQ = d \; mod \; (q - 1)$
(8) Hitung $qInv = q^{-1} pada \, Z_p$

Didapatkan kunci publik (e,n) dan kunci privat (dP,dQ,qInv,p,q)

Seperti halnya pada algoritma RSA, kunci publik ini akan digunakan untuk enkripsi dan kunci privat untuk deskripsi.

Contoh 13: Algoritma pembangkitan kunci RSA CRT

(1) Pilih dua bilangan prima $p = 83$ dan $q = 71$, di mana $p \neq q$.
(2) Hitung $n = 83 \times 71 = 5893$
(3) Hitung $\varphi(n) = (83 - 1)(71 - 1) = 82 \times 70 = 5740$
(4) Pilih bilangan sembarang bulat $e$ di mana

$\gcd(\varphi(n), e) = 1; 1 < e < \varphi(n)$ , misal $e = 33$

(5) Hitung $d = \frac{1+5740k}{33}$ , didapatkan $d = 2957$ karena terdapat $k = 17 \in$ bilangan bulat, $2957 = \frac{1+5740(17)}{33}$

(6) Hitung $\mathrm{dP} = 2957 \bmod (83 - 1) = 5$

(7) Hitung $\mathrm{dQ} = 2957 \bmod (71 - 1) = 17$

(8) Hitung $\mathrm{qInv} = 76$

Didapatkan Kunci public (33,5893) Kunci privat (5,17,76,83,17).

b) Enkripsi

Proses enkripsi Algoritma RSA-CRT sama dengan pada Algoritma RSA. yakni:

(1) Plainteks : $M < n$

(2) Ciperteks : $C = M^e \bmod n$

Proses enkripsi dilakukan oleh pihak pengirim, dengan menggunakan kunci publik (n,e) yang telah didapatkan pada pembangkitan kunci sebelumnya.

c) Dekripsi

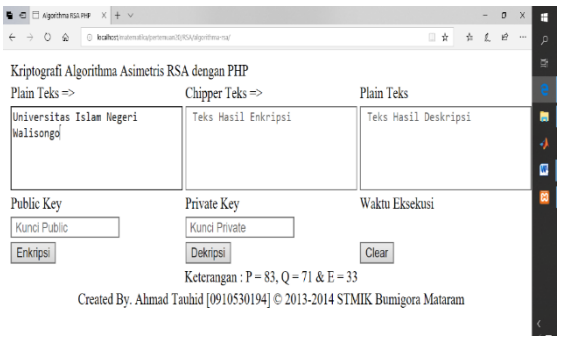
Proses deskripsi pada algoritma ini sebagai berikut (Sadikin, 2012) :

## 5. HASIL PERCOBAAN

Aplikasi Algoritma RSA base on computer dari STMIK Bumigora Mataram akan di komparsi waktu eksekusi dengan Aplikasi Algoritma RSA-CRT dari UIN Walisongo Semarang. Kedua aplikasi Algoritma tersebuat terdiri dari beberapa bagian. Bagian pertama sebagai tempat plainteks. Bagian kedua adalah tempat chiperteks yakni plainteks yang telah dienkripsi. Bagian ketiga adalah tempat chiperteks yang telah didekripsi sehingga kembali menjadi plainteks kembali. Setelah proses dekripsi dilakukan maka akan muncul waktu eksekusi. Waktu inilah yang dijadikan pedoman peneliti untuk melihat waktu proses antara algoritma RSA dengan algoritma RSA-CRT.

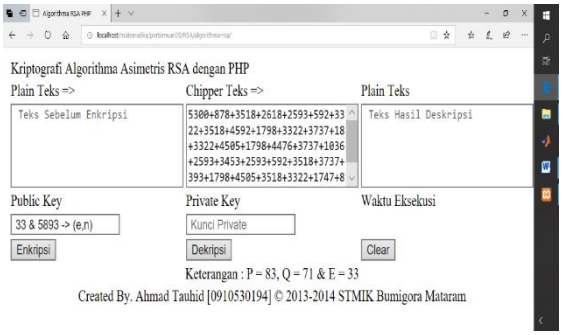
Tahap Pertama :

Pada komparasi dilakukan dengan memasukkan plainteks pada kolom plainteks dengan kata “Universitas Islam Negeri Walisongo” pada Aplikasi Algoritma *RSA base on computer* dari STMIK Bumigora Mataram, dengan hasil sebagai berikut :



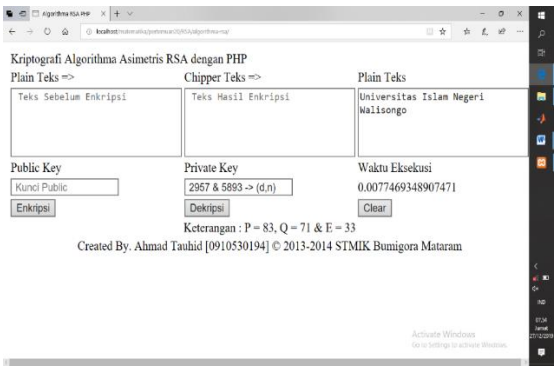

Gambar A : Input plainteks Universitas Islam Negeri Walisongo RSA

Didapat hasil chiperteks sebagai berikut :




Gambar B : Enkripsi Universitas Islam Negeri Walisongo Semarang RSA

Didapatkan plainteks kembali, dengan mengkonversi ke ASCII akan didapatkan " Universitas Islam Negeri Walisongo"

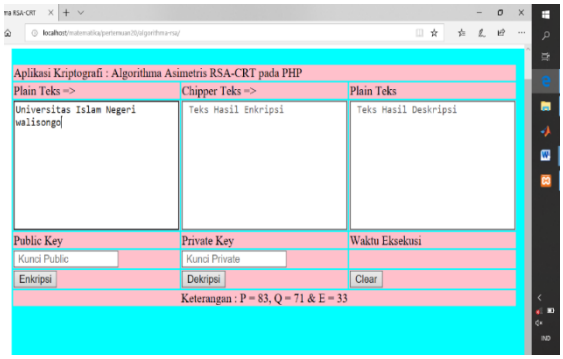



Gambar C : Dekripsi Universitas Islam Negeri Walisongo RSA

Pada hasil percobaan dengan memasukkan plainteks pada kolom plainteks dengan kata "Universitas Islam Negeri Walisongo" pada Aplikasi *Algoritma RSA base on computer* dari STMIK Bumigora Mataram diperoleh hasil Waktu eksekusi 0.0077469348907471.

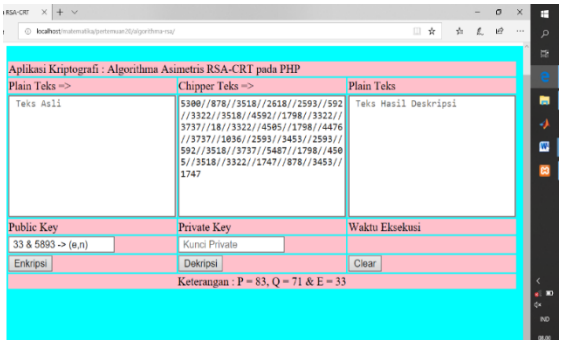
Tahap Kedua :

Pada komparasi dilakukan dengan memasukkan plainteks pada kolom plainteks dengan kata "Universitas Islam Negeri Walisongo" pada Aplikasi Algoritma RSA-CRT base on computer dari UIN Walisongo Semarang, dengan hasil sebagai berikut :

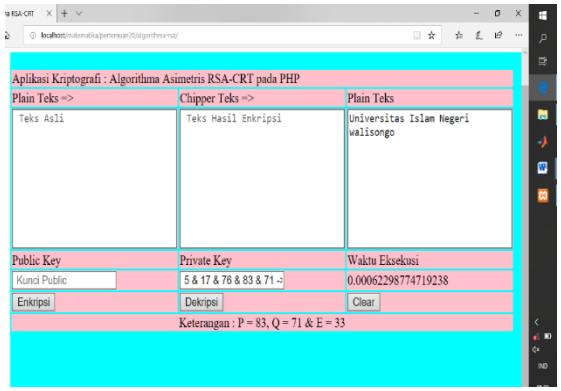



Gambar D : Input plainteks Universitas Islam Negeri Walisongo RSA CRT

Didapat hasil chiperteks sebagai berikut




Gambar E : Enkripsi Universitas Islam Negeri Walisongo RSA CRT




Gambar F : Dekripsi Universitas Islam Negeri Walisongo RSA CRT

Pada hasil percobaan dengan memasukkan plainteks pada kolom plainteks dengan kata "Universitas Islam Negeri Walisongo" pada Aplikasi *Algoritma RSA CRT base on computer* dari Aplikasi UIN Walisongo Semarang diperoleh hasil Waktu eksekusi 0.00062298774719238.

## 6. HASIL ANALISIS KOMPARASI APLIKASI ALGORITMA RSA DENGAN RSA-CRT

Dari komparasi perhitungan secara manual menggunakan algoritma RSA – CRT membutuhkan waktu yang lebih lama dibandingkan dengan perhitungan manual menggunakan algoritma RSA. Namun dengan menggunakan aplikasi RSA-CRT menggunakan bahasa PHP didapatkan waktu ekseskusi yang lebih cepat dibandingan dengan algoritma RSA menggunakan PHP. Sebagai catatan, inputan plainteks yang sama akan menghasilkan waktu eksekusi yang berbeda di waktu yang berbeda. Artinya inputan plainteks saat ini memiliki waktu eksekusi yang berbeda dengan inputan plainteks satu menit kemudian meskipun dengan plainteks yang sama. Hal ini tidak mempengaruhi kecepatan waktu eksekusi RSA-CRT lebih cepat dari pada RSA. Waktu eksekusi Algoritma RSA dan RSA-CRT

| Plainteks | Waktu ekseskusi Algoritma RSA-CRT | Waktu eksekusi Algoritma RSA |
|---|---|---|
| Universitas Islam Negeri Walisongo | 0.00062298774719238 | 0.007746948907471 |

## 7. KESIMPULAN

Dalam penelitian ini peneliti menyimpulkan bahwa kriptografi asimetri dikatakan lebih bagus dari segi keamanannya dibandigkan dengan kriptografi simetri karena proses perhitungannya lebih kompleks. Dengan kompleksnya perhitungan tersebut membuat prosesnya membutuhkan waktu yang lebih lama. Di tinjau dari waktu proses algoritma RSA-CRT memiliki kelebihan waktu proses lebih cepat dibandingan dengan RSA. Uji coba berupa kata "Universitas Islam Negeri" menghasilkan waktu eksekusi 0.00062298774719238 pada RSA-CRT Sedangkan waktu eksekusi pada RSA 0.0077469348907471.

## REFERENCES


Affandi, M. (2017). *Teknologi Informasi & Komunikasi dalam Pendidikan*. Kuningan: YNHW(Yayasan Nurul Huda Windusengkahan).

Alba, S. C., Supriana, I. I., & Mahzar, A. (2004). *Islam untuk Disiplin Ilmu MANAJEMEN INFORMATIKA*. (muharrom dan zulmaizarna Marzuki, Ed.). Departemen Agama RI Direktorat Jenderal Kelembagaan Agama Islam.

Alul, N. M. M. (2014). PENTINGNYA STABILITAS KEAMANAN DALAM ISLAM. Retrieved December 17, 2019, from https://almanhaj.or.id/3933-pentingnya-stabilitas-keamanan-dalam-islam.html%0D

Andika, D. (2018). Pengertian dan Sejarah Kriptografi. Retrieved May 1, 2019, from https://www.it-jurnal.com/pengertian-dan-sejarah-kriptografi/

Buana, T. D. U. M. (2010). *Kripto grafi*. Universitas Mercu Buana.

Erawan, L. (2014). Dasar - dasar PHP (pp. 1–47). semarang: Universitas Dian Nuswantoro.

Irawan, I. (2006). PHP? Siapa Takut! (pp. 1–108). ilmu komputer.com. Retrieved from IlmuKomputer.com

Kadir, A. (2009). *MEMBUAT APLIKASI LAPORAN MENGGUNAKAN PHP*. (H. P, Ed.) (I). Yogyakarta: C.V ANDI OFFSET(Penerbit ANDI).

Kromodimoeljo, S. (2009). *TEORI &APLIKASI KRIPTOGRAFI*. SPK IT Consulting.

Mahali, M. I. (2015). *Dasar-Dasar Keamanan (Steganografi dan Kriptografi)*. Yogyakarta.

Mawardina, M., & Insanudin, E. (2016). *Aplikasi Kriptografi dengan Metode Vigenere Chiper Berbasis Web*. Bandung.

Mono, H. (2010). Cybercrime, Bobol Rp 0,5 trilyun #1. Retrieved October 20, 2019, from https://www.kompasiana.com/mono.kompasiana.com/54ff6062a33311c34f50fb02/cybercrime-bobol-rp-05-trilyun-1%0D

Munir, R. (2004a). Algoritma RSA dan ElGamal (pp. 1–13). Bandung: Departemen Teknik Informatika Institu Teknologi Bandung.

Munir, R. (2004b). Sistem Kriptografi Kunci-Publik. Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Munir, R. (2004c). Teori Bilangan ( Number Theory ). In *Kriptografi*. Bandung: Departemen Teknik Informatika Institut Teknologi Bandung.

Nasution, N. R. (2017). Kombinasi RSA-CRT dengan Random LSB untuk Keamanan Data di Kanwil Kementerian Agama Prov. Sumatera Utara. *QUERY :Jurnal Sistem*

*Informasi*, *01*(01).

*PAS(Panduan Aplikatif dan Solusi): MUDAH MEMBUAT PORTAL BERITA ONLINE DENGAN PHP DAN MYSQL*. (2012) (I). Yogyakarta;Semarang: Penerbit ANDI; Wahana Komputer.

Pertemuan1. Algoritma dan PHP. (n.d.).

Q-Success. (2019). Usage of server-side programming languages for websites. Retrieved July 9, 2019, from https://w3techs.com/technologies/overview/programming_language/all

Qasim, A. M. Al. (2014). *Al-Qur'an Terjemah & Tajwid*. (T. S. M. Inovasi, Ed.) (I). Bandung: sygma creative media corp.

Raco, R. (2010). *Metode Penelitian Kualitatif*. (Arita L, Ed.). Jakarta: PT Grasindo.

Rosnawan, D. (2011). *Aplikasi Algoritma RSA Untuk Keamanan Data pada Sistem Informasi Berbasis Web*. Universitas Negeri Semarang.

Sadikin, R. (2012). *Kriptografi Untuk Keamanan Jaringan*. Yogyakarta: Penerbit ANDI.

SCHNEIER, B. (n.d.). *APPLIED CRYPTOGRAPHY : Protocol, Algoritmhms, and Source Code in C* (kedua).

Stallings, W. (2005). *Cryptography and Network Security (4th Edition)* (4th ed.). Prentice Hall.

Sufyani, P. (n.d.). Aritmatika Modular. Retrieved July 15, 2019, from related:file.upi.edu/Direktori/FPMIPA/JUR._PEND._MATEMATIKA/19600830 1986031-SUFYANI_PRABAWANTO/Aritmatika_Modular.pdf aritmatika modulo.pdf

Suprapto. (2008). *BAHASA PEMROGRAMAN*. Direktorat Pembinaan SMK.

Suryana, T., & Koesheryatin. (2014). *Aplikasi Internet Menggunakan HTML, CSS & JavaScript*. Jakarta: PT Elex Media Komputindo.

*This page intentionally left blank.*