SECURE E-VOTING MENGGUNAKAN METODE RSA DAN AUTENTIKASI RFID

Annisaa Sri Indrawanti[1)], Azmuri Wahyu Azinar[2)], M. Anang Firdiansyah[3)]

[1), 2), 3)]Jurusan Teknik Informatika, Fakultas Teknologi Informasi, Institut Teknologi Adhi Tama Surabaya
Jl Arif Rahman Hakim No. 100 Surabaya
Email : annisaaindrawanti@gmail.com[1)], azmuri@yahoo.com[2)], annangfirdiansyah@gmail.com[3)]

Abstrak

E-voting adalah sebuah sistem pemilihan umum (PEMILU) online yang dibangun untuk meminimalisasi biaya dan membuat sistem pemilihan lebih efisien. Data pemilihan merupakan data sensitif yang memerlukan keamanan data. Keamanan data yang dibangun mempertimbangkan parameter confidentiality, integrity and availability (triad CIA). Pada penelitian ini, terdapat dua mekanisme untuk mengamankan data pemilihan, yaitu autentikasi user menggunakan RFID dan kriptografi data pemilihan menggunakan metode RSA. Pada hasil percobaan menunjukkan bahwa semakin panjang bit dari bilangan prima acak p dan q, semakin sulit intruder untuk menemukan kunci publik dan kunci privat dan semakin lama waktu yang dibutuhkan untuk membangkitkan kunci, mengenkripsi dan mendekripsi. Selain itu, tingkat keberhasilan autentikasi user menggunakan RFID sebesar 80% dan tingkat keberhasilan dari proses enkripsi dan dekripsi sebesar 100%.

Kata kunci: *RSA, Autentikasi RFID, E-Voting*

Abstract

E-voting is an online voting system built to minimalize cost and more efficient. The data voting needs such a data security. The data security has some parameters that have to be considered, they are confidentiality, integrity and availability (triad CIA). In this research, there are two mechanisms to securing data voting. They are RFID user authentication and data e-voting cryptography using RSA. The experimental result show that longer bit length of random prime number p and q, make more difficult intruder will know the public and private key and more time needed for key generator, encryption and decryption. Besides that, success rate of RFID user authentication is 80% and success rate of encryption and decryption are the same 100%.

Keywords: *RSA, RFID Authentication, E-Voting*

1. Pendahuluan

E-voting merupakan sebuah sistem pemilihan umum (PEMILU) *online* yang memiliki fungsi yang sama dengan sistem pemilu *online.* Pada e-*voting*, semua proses mulai dari pemilihan kandidat hingga perhitungan suara dilakukan oleh komputer [2]. Salah satu permasalahan yang muncul pada sistem pemilu manual adalah kecurangan perhitungan suara untuk memenangkan kandidat tertentu. *E-voting* dapat mengurangi tingkat kecurangan dari sistem pemilu manual. *Secure e-voting* pada penelitian ini menggunakan autentikasi RFID untuk memvalidasi *user* pemilih sebelum melakukan pemilihan. RFID (*Radio Frequency Identification)* adalah teknologi mengidentifikasi menggunakan RFID *tag* untuk mengirimkan detail informasi mengenai *user* pemilih ke RFID *reader*. Dari RFID *tag*, identitas *user* pemilih dapat dibaca [7][9]. Setiap *user* pemilih hanya dapat memilih satu kali dan dicek menggunakan ID dari RFID. Selain itu, *securee-voting* ini juga mengimplementasikan kriptografi RSA untuk mengamankan kandidat yang dipilih oleh pemilih dari *intruder*. *Intruder* adalah seseorang yang mencoba untuk

mengambil data kandidat yang dipilih oleh user pemilih. Kekuatan metode RSA terletak pada tingkat kesulitan memfaktorkan sebuah bilangan menjadi bilangan faktor prima. Faktorisasi diperlukan untuk memperoleh kunci privat [1][3].

2. Dasar teori

2.1. *Voting*

Voting, berasal dari kata *vote* yang berarti memilih. Sedangkan yang dimaksud *voting* disini adalah pemungutan suara yang berarti menggunakan hak pilih untuk memilih kandidat, untuk mendapatkan salah satu kandidat yang akan menjadi pemimpin ataupun ketua yang telah disetujui bersama. Di Indonesia sebagai negara demokrasi dengan menggunakan sistem *voting* untuk pengambilan keputusan dalam pemilihan wakil-wakil rakyat ataupun kepala daerah. Namun dengan berkembangnya kemajuan teknologi saat ini telah membawa perubahan besar pada manusia, termasuk cara untuk melakukan *voting*. Maka atas dasar perkembangan teknologi tersebut media elektronik dapat digunakan dalam *voting*, yang disebut *e-voting*. *E-voting* adalah kepanjangan dari elektronik-*voting* yaitu pengambilan keputusan bersama untuk menemukan calon pemimpin ataupun ketua dengan elektronik sebagai medianya[4].

Tujuan dari *e-voting* adalah untuk menjamin kerahasiaan, dan keamanan dalam sistem *e-voting*. Maka unsur-unsur dalam *e-voting* meliputi :

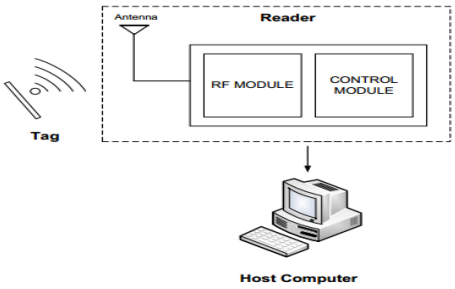
- *Eligibility* : Hanya calon pemilih yang terdaftar yang dapat mengikuti proses *voting*.
- *Unreusability* : Setiap pemilih hanya dapat melakukan satu kali *voting*.
- *Accuracy* : Pilihan tidak bisa diubah atau dihapus selama atau setelah pemilihan dan juga tidak bisa ditambahkan setelah proses pemilihan ditutup.
- *Vote an Go* : Pemilih hanya dapat melakukan pemilihan saja.
- *Privacy* : Pemilih tidak boleh tahu pilihan orang lain.
- *Fairness* : Orang lain tidak dapat mengetahui hasilnya sebelum dilakukan proses perhitungan suara[6].

2.2. Autentikasi RFID

Radio Frequency Identification atau sering disingkat RFID adalah suatu teknologi identifikasi tanpa kabel otomatis menggunakan *tag* khusus untuk mengirimkan data kepada RFID *reader*. Sehingga akan didapatkan data identitas dari seseorang yang hanya memiliki *tag* tersebut. RFID bekerja tanpa adanya sentuhan seperti *barcode* atau *magneticcard* (ATM), melainkan menggunakan frekuensi radio. Prinsip kerjanya adalah ketika *reader* menangkap gelombang radio, apabila *tag* RFID berada dalam jangkauan gelombang frekuensi radio tersebut, maka *chip* yang ada pada *tag* RFID akan dibangkitkan melalui tegangan terinduktansi dan akan memberikan respon balik, yaitu *tag* RFID akan mengirimkan nomor unik yang tersimpan didalamnya secara *wireless* ke *reader* RFID untuk dibaca. Setelah itu *reader* akan meneruskan data yang dibaca ke *host* komputer yang terhubung dengan *reader*[7].
Sistem RFID terdiri dari empat komponen, diantaranya adalah :

- *Tag* : Ini adalah *device* yang menyimpan informasi untuk identifikasi objek. *Tag* RFID sering juga disebut sebagai *transponder*.
- Antena : Untuk mentransmisikan sinyal frekuensi radio antara pembaca RFID dengan *tag* RFID.

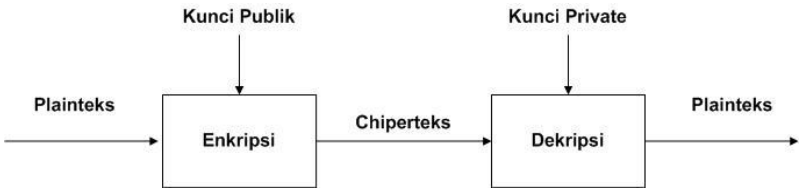
- Pembaca RFID : Adalah *device* yang kompatibel dengan tag RFID yang akan berkomunikasi secara *wireless* dengan *tag*.
- *Software* Aplikasi : Adalah aplikasi pada sebuah *workstation* atau PC yang dapat membaca data dari *tag* melalui pembaca RFID. Baik tag dan pembaca RFID dilengkapi dengan antena sehingga dapat menerima dan memancarkan gelombang elektromagnetik [6].



Gambar 8. Skema Mekanisme RFID

2.3. Metode RSA

Algoritma kriptografi RSA atau kepanjangan dari Ron Rivest, Adi Shamir and Leonard Adleman, dimana nama nama tersebut juga tokoh yang meneliti algoritma tersebut. Para peneliti ini dari MIT (*Massachussets Institute of Technology*) pada tahun 1976, dan pertama kali diperkenalkan pada bulan Agustus 1977. Algoritma ini termasuk ke dalam algoritma kriptografi asimetris (*Asymetric Cryptography*), yaitu algoritma yang menggunakan kunci yang berbeda untuk proses enkripsi dan dekripsi yaitu menggunakan *public key* dan *private key*. *Public key* digunakan untuk mengenkripsi pesan dan didekripsi dengan menggunakan *private key*. Prosesnya, pengirim (*sender*) mengenkripsi pesan dengan menggunakan *public key* milik penerima pesan (*receiver*) dan hanya penerima pesanlah yang dapat mendekripsi pesan karena hanya penerima yang mengetahui *private key* nya sendiri [5].



Gambar 9. Skema enkripsi dan dekripsi RSA

Keamanan algoritma RSA terletak pada sulitnya memfaktorkan bilangan yang besar menjadi faktor-faktor prima. Pemfaktoran dilakukan untuk memperoleh *private key* dan *public key*. Tingkat keamanan algoritma penyandian RSA sangat bergantung pada ukuran kunci sandi tersebut (dalam bit), karena makin besar ukuran kunci, maka makin besar juga kemungkinan kombinasi kunci yang bisa dijebol dengan metode mengecek kombinasi satu persatu kunci atau lebih dikenal dengan istilah *brute force attack*. Maka apabila penerapan dalam *e-voting*, *publickey* dan *private key* dibentuk dengan kombinasi kunci algoritma yang unik, otomatis panjang bit akan semakin besar, maka akan membuat penyandian RSA akan semakin kuat meminimalisir terjadinya para *hacker* untuk membobol algoritma ini[5].

2.3.1. Pembangkitan Kunci

Algoritma RSA memiliki dua buah kunci yang berbeda untuk proses enkripsi dan dekripsi. Dalam menentukan dua bilangan prima sebagai kunci adalah bilangan prima yang besar, karena pemfaktoran bilangan prima dari dua bilangan prima yang besar sangat sulit, sehingga keamanan pesan lebih terjamin. Pasangan kunci adalah elemen penting dari algortima RSA. Berikut ini adalah langkah-langkah dalam membangkitkan dua kunci algoritma RSA :

Pilih dua bilangan prima sembarang, untuk p dan q.

Hitung $n = p.q$. ……....(1)

Hitung $\emptyset(n) = (p-1)(q-1)$. ……....(2)

Pilih kunci publik e, yang relatif prima terhadap $\emptyset(n)$. Bangkitkan *private key* dengan menggunakan rumus (3):

$$e^e \ mod \ \emptyset(n) = d \text{……..(3)}$$

Hasil dari algoritma tersebut akan menghasilkan dua kunci, yaitu *publickey*(e, n) dan *private key* (d, n)[5].

2.3.2. Enkripsi RSA

Enkripsi adalah suatu proses pengamanan data dengan metode tertentu sehingga akan didapatkan suatu data enkripsi berupa *chipertext*. Dalam RSA, data yang akan dienkripsi disebut *plaintext*, dan data setelah dienkripsi disebut *chipertext*. Dengan m adalah *plaintext* dan C adalah proses enkripsi untuk menghasilkan *chipertext*. Dengan adanya *public key*(e, n) maka proses enkripsi dengan rumus (4):

$$c = m^e \ mod \ n \text{……..(4)}$$

2.3.3. Dekripsi RSA

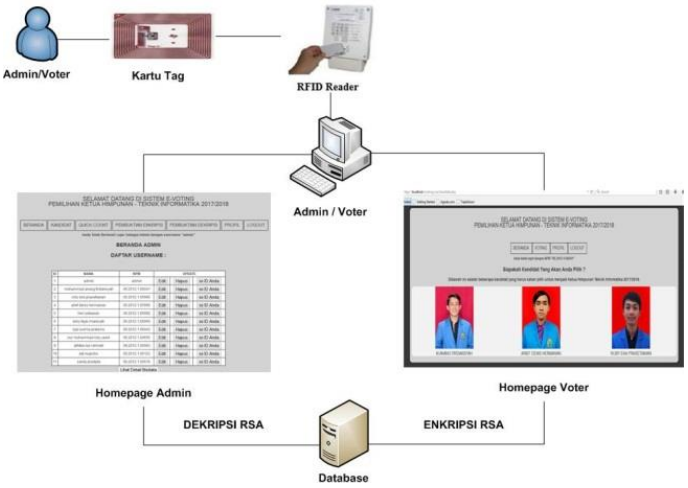
Dekripsi adalah suatu proses untuk mendapatkan nilai suatu *plaintext* seperti semula dari data *chipertext* yang ada. *Chipertext* yang diperoleh setelah proses enkripsi RSA dan didapat *private key* (d, n), maka akan didekripsi dengan rumus (5):

$$m = c^d \ mod \ n \text{…… …… …… ……(5)}$$

3. Metodologi Penelitian

3.1 *E-Voting*

E-voting adalah sebuah sistem pemilihan umum (PEMILU) *online*. PEMILU dilakukan mulai dari pemilihan kandidat hingga perhitungan suara[2]. Setiap tahapan pemilu akan diproses menggunakan komputer untuk meminimalisasi *intruder* dan *human error*. Data dari *e-voting* merupakan data sensitif yang memerlukan *triad security*, yaitu *confidentiality*, *integrity* dan *availability*[8]. Pada e-voting ini, identitas seorang *user* diautentikasi menggunakan teknologi RFID. Teknologi RFID terdiri dari RFID *tag* dan RFID *reader*. Setiap *user* memiliki satu RFID *tag* yang akan menyimpan detail informasi dari *user*, seperti ID *user*, nama dan alamat. Kemudian, setiap *user* memilih satu kandidat dan sistem *e-voting* akan mengenkripsi data kandidat yang dipilih *user* menggunakan metode RSA serta mengirimkannya ke *server*. Setelah tiba di server, data akan didekripsi menggunakan metode RSA. Diagram sistem *e-voting* secara keseluruhan ditunjukkan pada Gambar 3.

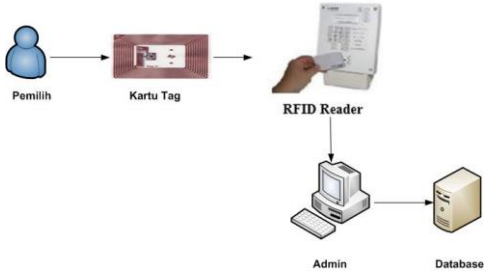


Gambar 10. Sistem *e-voting online*

Setiap pemilih yang memiliki RFID *tag* mendekatkan RFID *tag* yang dimiliki kepada RFID *reader* untuk membaca detail informasi identitas dari pemilih. Setelah RFID *reader* memperoleh detail informasi identitas pemilih, sistem *e-voting* akan menampilkan *homepage.* Kemudian, *user* dapat memilih salah satu dari kandidat yang ada.RSA mengenkripsi ID dari RFID *tag* dan kandidat yang dipilih menggunakan kunci publik RSA dan mengirimkannya ke server. *Server* akan mendapatkan ID dari RFID dan kandidat yang dipilih *user* yang telah terenkripsi. Kemudian, sistem akan mendekripsi data terenkripsi tersebut menggunakan kunci privat dari metode RSA.

3.2 Autentikasi RFID

Autentikasi adalah proses verifikasi untuk mengetahui *true user* dan mencegah *fake user*. Pada proses autentikasi ini, e-*voting* menggunakan teknologi RFID yang terdiri dari RFID *tag* dan RFID *reader*. Setiap komputer pada sistem e-*voting* akan di-*embed* oleh sebuah RFID *reader*. Proses pemilihan akan dimulai dengan autentikasi RFID. Pemilih akan mendekatkan RFID *tag* ke RFID *reader* dan gelombang frekuensi radio akan mengirimkan ID dari RFID *tag* pemilih ke RFID *reader*. Sistem *e-voting* akan membaca semua detail informasi mengenai *user* pemilih. RFID *reader* dikoneksikan melalui RS232 ke kabel serial USB.



Gambar 11. Autentikasi RFID

3.3 Metode RSA

3.3.1 Pembangkitan Kunci

Metode RSA memiliki 2 kunci yang berbeda untuk proses enkripsi dan dekripsi[10]. Metode ini menggunakan bilangan prima untuk menentukan kunci publik dan kunci privat karena tingkat kesulitan yang tinggi dalam memfaktorkan bilangan prima yang besar. Hal ini

dimanfaatkan oleh RSA dalam menjaga *confidentiality* dari pesan.Berikut ini adalah langkah-langkah pembangkitan kunci :

- Memilih bilangan prima acak *p* and *q*
- Menghitung $n = p.q$ ……(6)
- Menghitung $\emptyset(n) = (p-1)(q-1)$ ……(7)
- Memilih kunci public *e* yang relatif prima terhadap $\emptyset(n)$.
- Menghitung kunci privat *d* dengan rumus $e.d \equiv 1 (mod\ \emptyset(n))$, yang ekivalen terhadap $e.d = 1 + k\emptyset(n)$, sehingga $d = \frac{1+k\emptyset(n)}{e}$ ……(8)

Proses pembangkitan kunci menghasilkan *output* kunci publik (*e*,*n*) dan kunci privat (*d*,*n*). kunci publik (*e*, *n*) bersifat tidak rahasia, tetapi kunci privat (*d*, *n*) bersifat rahasia.

3.3.2 Enkripsi RSA

Setelah proses pembangkitan kunci menghasilkan *output* kunci publik (*e*,*n*) dan kunci privat (*d*,*n*), sistem mengenkripsi ID dari RFID dan kandidat terpilih. Berikut langkah-langkah enkripsi RSA :

- Masukkan berupa *plaintext* m
- Membagi m ke dalam beberapa blok $m_1, m_2, m_3, \ldots, m_i$
- Setiap blok m_i merepresentasikan sebuah karakter
- Mencari nilai ASCII dari setiap blok m_i
- Mengenkripsi setiap blok m_i menjadi *chipertext* c_i dengan rumus (9) :

$c_i = m_i^e \ mod\ n$ ……(9)

Enkripsi RSA akan menghasilkan *chipper text* $c_1, c_2, c_3, \ldots, c_i$.

3.3.3 Dekripsi RSA

Setelah enkripsi RSA menghasilkan *chipertext* dari ID RFID dan kandidat yang dipilih, *chipertext* akan dikirimkan ke *server*. *Chipertext* didekripsi menjadi *plaintext* dengan langkah-langkah berikut :

- Dekripsi setiap blok dari *chipertext* menggunakan rumus $m_i = c_i^d mod\ n$ ……(10)
- Hasil dekripsi menghasilkan nilai ASCII setiap blok
- Konversi nilai ASCII ke *plaintext m*
- Sistem akan menerima *plaintext* untuk menghitung jumlah pemilih dari setiap kandidat

4. Pengujian dan Pembahasan

Pada subbab ini akan dijelaskan mengenai pengujian fungsional dan pengujian performa. Pengujian fungsional dilakukan untuk melihat tingkat keberhasilan autentikasi RFID, proses enkripsi dan dekripsi RSA. Sedangkan pengujian performa dilakukan untuk melihat pengaruh panjang bit dari bilangan prima acak *p* dan *q* terhadap waktu komputasi proses pembangkitan kunci, enkripsi RSA dan dekripsi RSA yang menandai tingkat kesulitan *intruder* dalam memfaktorkan bilangan prima acak *p* dan *q*.

4.1 Pengujian Fungsionalitas

Pengujian ini dilakukan untuk melihat tingkat keberhasilan sistem meliputi autentikasi RFID, enkripsi dan dekripsi RSA. Skenario pengujian yang dilakukan adalah melakukan proses

autentikasi RFID, enkripsi dan dekripsi RSA sebanyak 10 kali dan melihat keberhasilan setiap proses. Hasil pengujian fungsionalitas ditunjukkan pada Tabel 1.

Tabel 1. Hasil pengujian fungsionalitas autentikasi RFID, enkripsi dan dekripsi

No.	Jenis pengujian fungsionalitas	Tingkat keberhasilan (kali)	Tingkat kegagalan (kali)	Jumlah	Tingkat keberhasilan
1	Autentikasi RFID	8	2	10	(8/10)x100%= 80%
2	Enkripsi	10	0	10	(10/10)x100%= 100%
3	Dekripsi	10	0	10	(10/10)x100%= 100%

Dari Tabel 1 ditunjukkan bahwa dari 10 kali percobaan, tingkat keberhasilan proses autentikasi RFID sebesar 80%, tingkat keberhasilan proses enkripsi sebesar 100% dan tingkat keberhasilan dekripsi sebesar 100%.

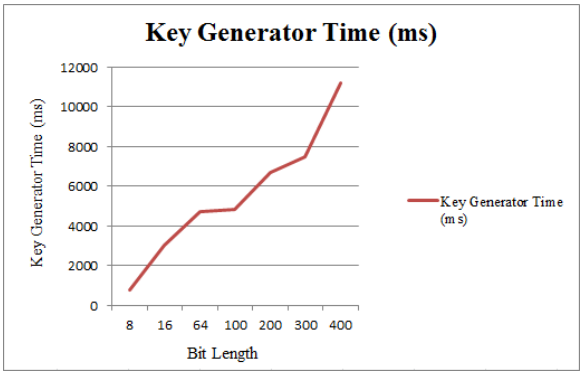
4.2 Pengujian Performa

Pengujian performa dilakukan untuk melihat pengaruh variasi panjang bit terhadap waktu komputasi dari pembangkitan kunci, enkripsi dan dekripsi. Skenario pengujian yang dilakukan adalah memvariasikan panjang bit dari bilangan acak prima dengan variasi panjang bit 8,16, 64, 100, 200, 300 dan 400 dan melihat pengaruh variasi panjang bit terhadap waktu komputasi pembangkitan kunci, enkripsi dan dekripsi. Hasil pengujian performa ditunjukkan pada Tabel 2.

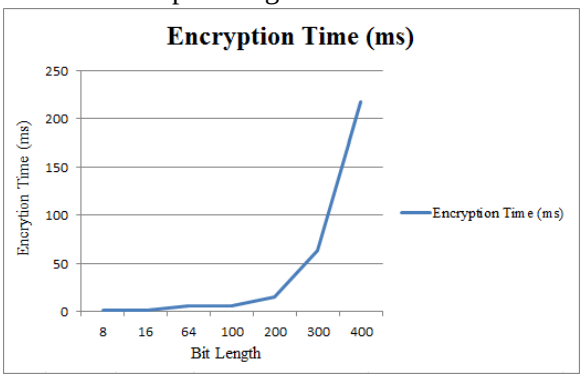
Tabel 2. Hasil pengujian performa pengaruh variasi panjang bit bilangan prima acak p dan q terhadap waktu komputasi pembangkitan kunci, enkripsi dan dekripsi

Skenario pengujian: variasi 7 jenis panjang bit yang berbeda dari bilangan prima acak *p* dan *q* dan melihat pengaruhnya terhadap waktu komputasi pembangkitan kunci (PK), enkripsi (E) dan dekripsi (D)			
Panjang bit bilangan prima acak *p* dan *q*	**Waktu komputasi (ms)**		
	PK	**E**	**D**
8	766.0 ms	1 ms	3 ms
16	3020 ms	1 ms	4 ms
64	4690 ms	6 ms	10 ms
100	4806 ms	6 ms	18 ms
200	6671 ms	15 ms	106 ms
300	7467 ms	63 ms	155 ms
400	11199 ms	217 ms	519 ms

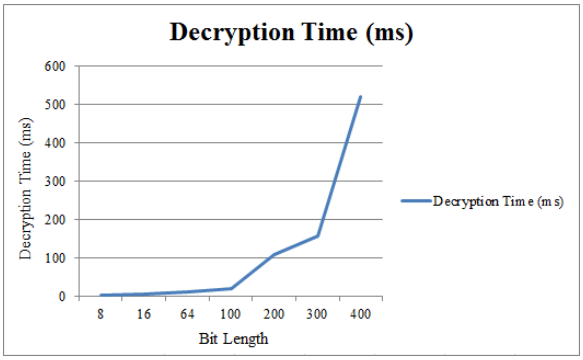
Pada Tabel 2 ditunjukkan bahwa semakin panjang bit dari bilangan prima acak *p* dan *q*, maka semakin lama waktu yang dibutuhkan untuk melakukan proses pembangkitan kunci, enkripsi dan dekripsi dan hal ini semakin menyulitkan *intruder* untuk memfaktorkan bilangan prima acak *p* dan *q*. Hal ini juga ditunjukkan dalam bentuk grafik pada Gambar 5, Gambar 6 dan Gambar 7.



Gambar 12. Pengaruh panjang bit bilangan prima acak p dan q terhadap waktu komputasi pembangkitan kunci



Gambar 13. Pengaruh panjang bit bilangan prima acak p dan q terhadap waktu komputasi enkripsi



Gambar 14. Pengaruh panjang bit bilangan prima acak p dan q terhadap waktu komputasi dekripsi

5. Kesimpulan

Dari percobaan *secure e-voting* yang dilakukan pada penelitian ini dapat disimpulkan bahwa semakin panjang bit bilangan prima acak p dan q yang diberikan, maka semakin lama waktu komputasi yang dibutuhkan dan hal ini semakin menyulitkan *intruder* untuk memfaktorkan bilangan acak prima p dan q. sistem *secure e-voting* ini juga memiliki tingkat keberhasilan dalam autentikasi *user* menggunakan RFID sebesar 80%, tingkat keberhasilan enkripsi sebesar 100% dan tingkat keberhasilan dekripsi sebesar 100%.

Daftar Pustaka

[1] Gotimukul V., Sunkara V.G, Mrudula M., Sindhu C. *Application of Session Login and One Time Password in Fund Transfer System using RSA Algorithm*. International Conference on Electronics, Communication and Aerospace Technology (ICECA). 2017.

[2] Nobert K., Melaine V., Nadja B.B., Norbert K., Olivier P., Carsten S. "Electronic Voting". *Second International Joint Conference Bregenz, Austria,* Switzerland: Springer International Publishing AG. *October 24-27*, 2017.

[3] Fausto Meneses, et. al, Jenny Tores, Alba Miranda, et. al. *"RSA Encryption Algorithm Optimization to Improve Performance and Security Level of Network Messages".* International Journal of Computer Science and Network Security Vol. 16 No. 8, pp 55-62, 2016.

[4] Neyman, Shelvie Nidya. Isnaini, Muhammad Fikri. Nurdiati, Sri. *Penerapan Sistem E-voting pada Pemilihan Kepala Daerah di Indonesia (The Application of E-voting Systems in the Local Elections in Indonesia)*. Departemen Ilmu Komputer FMIPA IPB. Bogor. Jurnal Sains Terapan Edisi III Vol. 3, 2013.

[5] R, Dicky Wizanajani. *"Perbandingan Algoritma Berbasis Elliptic Curve Cryptography Dengan RSA Dan DSA Pada Tanda tangan Digital".* Institut Teknologi Bandung. Bandung. 2006.

[6] Afrin, Tanzila. Satao, K.J. *"E-Voting System for on Duty Person Using RSA Algorithm with Kerberos Concept".* International Journal of Advanced Research in Computer Engineering & Technology (IJARCET), Vol, 2, No.7 , pp 2258-2261, 2013

[7] Saad, Amna. Roseli, Mohd Izzat Mohamat, Zullkaeply, Muhammad Saufi. *A Smart E-Voting System Using RFID Authentification Method For A Campus Electoral*. Malaysian Institute of Information Technology. Kuala Lumpur. 2013.

[8] Hutagalung, Muhammad Kifli. *Perancangan Perangkat E-Voting Berbasis E-KTP*. STMIK Triguna Dharma. Medan. 2012.

[9] Syed Ahson, Mohammad Ilyas. *RFID Handbook : Application, Technology, Security and Privacy*. United States of America: CRC Press Taylor & Francis Group. 2008.

[10] Rinaldi Munir. *"Algoritma RSA dan El Gamal".* Institut Teknologi Bandung. Bandung: Makalah IF5054 Kriptografi. 2004.