MODEL MODIFIKASI KRIPTOGRAFI ALGORITMA RSA UNTUK KEAMANAN DATA PADA DATABASE E-VOTING

Martono

STIKOM Dinamika Bangsa, Program Studi Teknik Informatika, Jambi
Jl. Jendral Sudirman Thehok, Jambi, Telp 0741-35095
E-mail: martono@stikom-db.ac.id

Abstract

Computer security problem is a very important thing. Computer security not only focus on computer equipment but also focus on data security. One of the method to protect data is using cryptography. Cryptography is a knowledge and also an art to protect data which is has a specific algorithm to intend as confusion, by change the plaintext into a text that can't be read the meaning by other people directly (ciphertext). Cryptography algorithm that used in this research is RSA algorithm with development or modification. The RSA algorithm is include in asymmetric cryptography algorithm that have two keys, i.e. public key and private key. This research discuss about RSA cryptography algorithm modification model for data security at e-voting database and the research method that used is experiment research method and system examination method that used is black box method for validation examination and experiment method for quality examination. The result from this research to help user protect their data and improve confidential and data security especially e-voting database, so the data at database can't be read directly (because already encrypted) without decryption process.

Keywords: Computer Security, Data Security, Cryptography, Plaintext, Ciphertext, Encryption, Decryption, RSA Algorithm, Public Key, Private Key.

Abstrak

Masalah keamanan komputer merupakan sesuatu yang sangat penting. Keamanan komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga dari keamanan datanya. Salah satu cara untuk mengamankan data adalah dengan menggunakan kriptografi. Kriptografi merupakan ilmu dan sekaligus seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai confusion atau pembingungan, dengan cara mengubah teks polos (plaintext) menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia (ciphertext). Algoritma kriptografi yang digunakan dalam penelitian ini adalah algoritma RSA dengan pengembangan atau modifikasi. Algoritma RSA termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key). Dalam penelitian ini membahas tentang model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting dan metode penelitian yang digunakan adalah metode penelitian eksperimen serta metode pengujian sistem yang digunakan adalah metode black box untuk pengujian validasi dan metode eksperimen untuk pengujian kualitas. Hasil dari penelitian tersebut dapat membantu menjaga dan meningkatkan kerahasiaan dan keamanan data pada database terutama database e-voting, sehingga data pada database tersebut tidak akan dapat terbaca secara langsung (karena telah dienkripsi) tanpa melalui proses dekripsi.

Kata Kunci : Keamanan Komputer, Keamanan Data, Kriptografi, Plaintext, Ciphertext, Enkripsi, Dekripsi, Algoritma RSA, Kunci Publik (Public Key), Kunci Pribadi (Private Key).

1. Pendahuluan

Masalah keamanan komputer merupakan sesuatu yang sangat penting dalam era informasi yang serba terkomputerisasi sekarang ini. Keamanan merupakan bentuk tindakan untuk mempertahankan sesuatu hal dari berbagai macam gangguan dan ancaman. Aspek yang berkaitan dengan keamanan dalam dunia komputer, antara lain : privacy / confidentiality (usaha untuk menjaga informasi dari orang yang tidak berhak mengakses informasi tersebut), integrity (usaha untuk menjaga informasi agar tidak diubah oleh orang yang tidak berhak atas informasi tersebut), authentication (usaha atau metode untuk mengetahui keaslian dari informasi yang dikirim, apakah dikirim dan dibuka oleh orang yang benar atau berhak atas informasi tersebut), availability (berhubungan dengan ketersediaan sistem atau informasi ketika dibutuhkan). Keamanan merupakan salah satu aspek yang sangat penting dalam penggunaan komputer. Keamanan sistem komputer yang menjadi sorotan bukan hanya dari perangkat komputernya saja, namun juga keamanan bagi jaringan, software (program) aplikasi dan juga keamanan database.

Database adalah sekumpulan data atau informasi yang disimpan di dalam komputer secara sistematik yang dapat digunakan melalui sebuah program komputer tertentu untuk menjalankannya. Keamanan database menjadi pertahanan terakhir ketika suatu sistem komputer mengalami serangan dari pihak luar setelah menembus keamanan jaringan, keamanan sistem operasi dan software. Keamanan database dapat dilakukan dengan berbagai cara, dimulai dari pembatasan hak akses user terhadap database itu sendiri, penggunaan nama field yang hanya dimengerti oleh administrator sehingga tidak semua user yang diberi izin mengakses database mengerti alur database yang ada guna menghindari pencurian data, perusakan data dan lain sebagainya, hingga pengimplementasian kriptografi dengan algoritma tertentu oleh administrator terhadap record dalam database dengan tujuan membuat record yang tersimpan menjadi lebih rahasia dan sulit dibaca oleh pihak lain.

Kriptografi adalah ilmu dan sekaligus seni untuk mengamankan data yang didalamnya terdapat algoritma tertentu yang bertujuan sebagai confusion atau pembingungan, dengan cara mengubah teks polos (plaintext) menjadi teks yang tidak bisa dibaca artinya secara langsung oleh manusia (ciphertext). Pada kriptografi, terdapat proses enkripsi yang mengubah plaintext (teks polos) menjadi ciphertext, dan proses dekripsi yang mengubah ciphertext menjadi plaintext (teks polos) kembali. Salah satu contoh algoritma kriptografi adalah algoritma RSA (Rivest, Shamir, Adleman). Algoritma RSA termasuk dalam algoritma kriptografi asimetris yang mempunyai dua kunci, yaitu kunci publik (public key) dan kunci pribadi (private key). Sampai saat ini, algoritma kriptografi RSA merupakan salah satu yang paling maju dalam bidang kriptografi dan banyak digunakan karena kehandalannya.

Pengamanan data dalam database sangat dibutuhkan agar data tersebut tidak jatuh ke tangan orang yang tidak berhak atas data tersebut dan untuk menghindari perubahan data tersebut oleh pihak lain. Salah satu contoh database yang perlu diamankan adalah database dalam sistem electronic voting (e-voting). Electronic voting (e-voting) adalah penggunaan teknologi informasi pada pelaksanaan pemungutan suara. Pilihan teknologi yang digunakan dalam implementasi e-voting sangat bervariasi, seperti penggunaan smart card untuk otentikasi pemilih, penggunaan internet sebagai sistem pemungutan suara, penggunaan touch screen sebagai pengganti kertas suara, dan masih banyak variasi teknologi yang digunakan. Apapun pilihan teknologi yang digunakan dalam implementasi e-voting pasti menggunakan database sebagai sumber data dan informasi, sehingga pada database tersebut perlu dilakukan proses pengamanan agar data dalam database tersebut lebih terjamin keamanannya.

Pada tahun 2004 terjadi pembobolan situs KPU (Komisi Pemilihan Umum) yang dilakukan oleh hacker yang bernama dani firmansyah. Tujuannya menghack situs tersebut hanya ingin menguji keamanan sistem pada server tnp.kpu.go.id yang disebut mempunyai sistem pengamanan berlapis-lapis. Motivasi dani firmansyah melakukan serangan ke situs KPU tersebut hanya untuk memperingatkan kepada tim TI KPU bahwa sistem TI yang seharga Rp. 152 miliar tersebut ternyata tidak aman. Dani firmansyah berhasil menembus server tnp.kpu.go.id yang digunakan sebagai server untuk pusat tabulasi nasional pemilu oleh komisi pemilihan umum tersebut dengan cara SQL injection. Melalui SQL injection dani firmansyah berhasil merubah seluruh nama partai politik peserta pemilu di situs tnp.kpu.go.id menjadi nama-nama lucu seperti partai jambu, partai kelereng, partai cucak rowo, partai si yoyo, partai mbah jambon, partai kolor ijo, dan lain sebagainya. Hal tersebut dapat terjadi karena dengan menggunakan SQL injection dapat dilakukan update (perubahan) terhadap isi database yang terdapat pada situs tnp.kpu.go.id tersebut. Walaupun sistem yang diterapkan oleh KPU tersebut belum bisa dikatakan sebagai sebuah

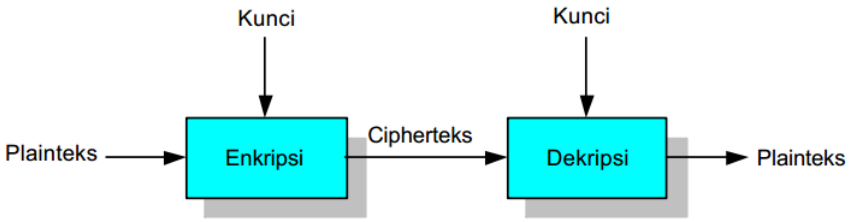
sistem e-voting karena hanya digunakan untuk menampilkan hasil tabulasi (perhitungan) perolehan suara dan belum menggunakan teknologi informasi pada pelaksanaan pemungutan suara, namun keamanan data pada database tersebut harus tetap terjaga keamanannya.

Berdasarkan contoh kasus diatas, salah satu cara yang dapat digunakan untuk menghindari hal tersebut adalah dengan menggunakan kriptografi. Oleh karena itu penulis tertarik untuk mengangkat penelitian dengan judul "Model Modifikasi Kriptografi Algoritma RSA Untuk Keamanan Data Pada Database E-Voting".

2. Tinjauan Pustaka/Penelitian Sebelumnya

2.1 Kriptografi

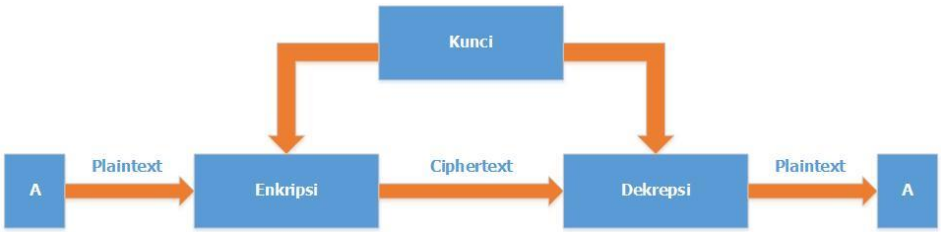
Kriptografi berasal dari bahasa Yunani, yaitu kryptos (tersembunyi) dan graphien (menulis). Kriptografi atau penyandian data merupakan seni dan ilmu untuk menjaga berita. Kriptografi merupakan suatu bidang ilmu yang mempelajari tentang bagaimana merahasiakan suatu informasi penting ke dalam suatu bentuk yang tidak dapat dibaca oleh siapapun serta mengembalikannya kembali menjadi informasi semula dengan menggunakan berbagai macam teknik yang telah ada sehingga informasi tersebut tidak dapat diketahui oleh pihak manapun yang bukan pemilik atau yang tidak berkepentingan [1]. Kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan (cryptography is the art and science of keeping messages secure) [2]. Pada kriptografi terdiri dari dua proses utama yaitu enkripsi dan dekripsi. Enkripsi adalah suatu proses mengubah pesan atau data menjadi sandi yang merupakan salah satu proses dari kriptografi. Data yang disandikan berupa file sebagai input dan dengan menggunakan suatu kunci, file tersebut diubah menjadi file enkripsi yang tidak bisa dibaca. Adapun tujuan dari enkripsi ini adalah menyembunyikan data atau informasi dari orang tidak berhak. Dekripsi adalah proses sebaliknya dari enkripsi yaitu mengembalikan sandi-sandi atau informasi yang telah dilacak ke bentuk file aslinya dengan menggunakan kunci pula [3].



Gambar 1. *Diagram Proses Enkripsi dan Dekripsi* [4]

Berdasarkan jenis kunci yang digunakan kriptografi dapat dibagi menjadi dua bagian, yaitu :

1. Kriptografi Kunci Simetris
   Pada kriptografi kunci simetris proses enkripsi maupun dekripsi pesan rahasia menggunakan kunci yang sama. Jadi sebelum melakukan pengiriman pesan rahasia, pengirim dan penerima harus memilih suatu kunci tertentu yang sama untuk dipakai bersama dalam proses enkripsi dan dekripsi. Keamanan kriptografi dengan teknik ini terletak pada kerahasiaan kunci.

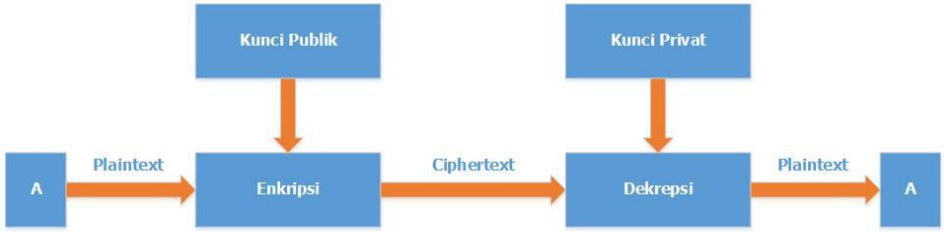


Gambar 2. *Alur Kriptografi Kunci Simetris* [5]

Pada penggunaan kriptografi kunci simetris memiliki kecepatan proses yang lebih cepat dibandingkan dengan penggunakan kiptografi kunci asimetris dikarenakan perhitungan matematika yang digunakan dalam proses enkripsi dan dekripsi adalah sama, akan tetapi memiliki masalah pada distribusi kunci agar dapat dikirimkan secara aman kepada pihak penerima dan juga masalah pada efisiensi jumlah

kunci yang harus dibuat mengikuti dengan semakin bertambahnya jumlah pengguna. Hal ini dikarenakan untuk setiap pengiriman pesan dengan pengguna yang berbeda dibutuhkan kunci yang berbeda juga. Contoh algoritma kriptografi kunci simetris adalah S-DES (Simplified-Data Encryption Standart), DES (Data Encryption Standart), IDEA, dan Blowfish.

2. Kriptografi Kunci Asimetris
   Pada kriptografi kunci asimetris proses enkripsi dan dekripsi menggunakan kunci yang berbeda. Kunci untuk proses enkripsi menggunakan kunci publik (public key), sedangkan kunci untuk proses dekripsi menggunakan kunci rahasia (private key). Kunci publik bersifat tidak rahasia dan boleh diketahui oleh orang lain, sedangkan kunci rahasia bersifat rahasia dan tidak boleh diketahui oleh orang lain. Walaupun kunci publik telah diketahui namun akan sangat sukar untuk mengetahui kunci rahasia yang digunakan. Pada teknik kriptografi kunci asimetris tidak perlu penentuan kunci secara bersama seperti yang dilakukan pada kriptografi kunci simetris.



Gambar 3. *Alur Kriptografi Kunci Asimetris* [5]

Masalah efisiensi dan distribusi kunci pada kriptografi kunci simetris dapat diatasi dengan penggunaan kriptografi kunci asimetris karena kunci yang digunakan untuk proses enkripsi dan dekripsi berbeda. Penggunaan kriptografi kunci asimetris ini memberikan jaminan keamanan kepada siapa saja dalam melakukan pertukaran informasi, meskipun diantara mereka tidak ada persetujuan keamanan data terlebih dahulu dan diantara mereka tidak saling mengenal sebelumnya. Contoh algoritma kriptografi kunci asimetris adalah Rabin, RSA (Rivest Shamir Adleman), dan ElGamal.

2.2 Algoritma RSA

Dari sekian banyak algoritma kriptografi kunci publik yang pernah dibuat, algoritma yang paling populer adalah algoritma RSA. Algoritma ini melakukan pemfaktoran bilangan yang sangat besar. Oleh karena alasan tersebut RSA dianggap aman. Untuk membangkitkan dua kunci, dipilih dua bilangan prima acak yang besar. Algoritma RSA dibuat oleh 3 orang peneliti dari MIT (Massachussets Institute of Technology) pada tahun 1976, yaitu : Ron (R)ivest, Adi (S)hamir, dan Leonard (A)dleman [6]. Kekuatan algoritma RSA terletak pada sulitnya memfaktorkan bilangan besar menjadi faktor-faktor bilangan primanya, sehingga semakin besar bilangan prima yang digunakan semakin baik atau aman [7]. Dalam kriptografi menggunakan algoritma RSA terdapat tiga proses yaitu proses pembangkitan kunci publik dan kunci privat, proses enkripsi, dan proses dekripsi [8].

Adapun langkah-langkah pada proses pembangkitan kunci publik dan kunci privat pada algoritma RSA adalah sebagai berikut :

1. Pilih 2 bilangan prima yang berbeda p dan q secara acak dan $p \neq q$, semakin besar semakin baik. Kedua bilangan prima ini, p dan q bersifat rahasia.
2. Hitung $n = p * q$ dimana nilai n digunakan untuk modulus pada kunci publik dan kunci privat. Nilai n tidak rahasia, orang lain dapat mengetahuinya.
3. Hitung $\varphi(n) = (p - 1) * (q - 1)$ digunakan untuk pencarian kunci privat. Nilai $\varphi(n)$ bersifat rahasia.
4. Hitung nilai e dengan cara memilih bilangan bulat sedemikian rupa sehingga $1 < e < \varphi(n)$ dan $GCD(\varphi(n), e) = 1$, nilai e bersifat tidak rahasia.
5. Pilih nilai d yang merupakan bilangan bulat dengan syarat nilai d memenuhi $(d * e) \bmod \varphi(n) = 1$ atau $d = (1 + k * \varphi(n)) / e$, nilai k dapat dihitung dengan cara mencoba nilai-nilai sehingga diperoleh nilai bilangan d adalah bilangan bulat. Nilai d bersifat rahasia.

Sehingga dari langkah-langkah pada proses pembangkitan kunci diatas didapatkan kunci publik (e, n) dan kunci privat (d, n). Berikut ini contoh proses pembangkitan kunci publik dan kunci privat pada algoritma RSA :

1. Nilai bilangan p adalah 17 dan q adalah 11.
2. Hitung n = p * q, sehingga nilai n = 17 * 11 = 187.
3. Hitung φ(n) = (p – 1) * (q – 1), sehingga φ(n) = (17 – 1) * (11 – 1) = 160.
4. Hitung nilai e, sehingga 1 < e < φ(n) dan GCD(φ(n), e) = 1.

Tabel 1. *Hitung Nilai e*

Mulai dari	Nilai GCD(160, e)
e = 2	Nilai GCD(160, 2) = 2
e = 3	Nilai GCD(160, 3) = 1
e = 4	Nilai GCD(160, 4) = 4
e = 5	Nilai GCD(160, 5) = 5
e = 6	Nilai GCD(160, 6) = 2
e = 7	Nilai GCD(160, 7) = 1
e = 8	Nilai GCD(160, 8) = 8
e = 9	Nilai GCD(160, 9) = 1

Berdasarkan tabel perhitungan nilai e diatas, maka nilai e yang bisa digunakan adalah 3 atau 7 atau 9, maka dipilih salah satu untuk digunakan yaitu 7.

5. Hitung nilai d dengan menggunakan persamaan d = (1 + k * φ(n)) / e.
6.

Tabel 2. *Hitung Nilai d*

Nilai k	d = (1 + k * φ(n)) / e	Hasil
k = 1	d = (1 + 1 * 160) / 7	23
k = 2	d = (1 + 2 * 160) / 7	45.86
k = 3	d = (1 + 3 * 160) / 7	68.71

Berdasarkan tabel perhitungan nilai d diatas, maka nilai d adalah 23.

7. Jadi didapatkan kunci publik (7, 187) dan kunci privat (23, 187).

Pada algoritma RSA proses enkripsi pesan plaintext P dilakukan dengan menggunakan kunci publik (e, n) dan dengan menggunakan persamaan matematis $C = M^e \bmod n$. Dengan menggunakan persamaan tersebut akan menghasilkan nilai ciphertext C yang kemudian akan dikirimkan kepada si penerima, sehingga pesan tidak dapat dibaca. Dengan demikian hanya orang yang memiliki kunci privat (d, n) yang dapat mendekripsi ciphertext C tersebut.

Pada algoritma RSA proses dekripsi pesan ciphertext C dilakukan dengan menggunakan kunci privat (d, n) dan dengan menggunakan persamaan matematis $P = C^d \bmod n$. Dengan menggunakan persamaan tersebut akan mengembalikan nilai ciphertext C menjadi plaintext P, sehingga pesan dapat diketahui isinya dan dibaca.

2.3 Penelitian Sebelumnya

Berikut ini adalah ringkasan dari beberapa penelitian sebelumnya yang berkaitan dengan kriptografi algoritma RSA :

1. Pada penelitian yang dilakukan oleh Tri Rahajoeningroem dan Muhammad Aria yang berjudul "Studi dan Implementasi Algoritma RSA Untuk Pengamanan Data Transkrip Akademik Mahasiswa" dikatakan bahwa masalah keamanan dan kerahasiaan data merupakan hal yang penting dalam suatu organisasi. Data yang bersifat rahasia tersebut perlu dibuatkan sistem penyimpanan dan pengirimannya agar tidak terbaca atau diubah oleh orang-orang yang tidak bertanggung jawab, baik saat data tersebut tersimpan sebagai file di dalam komputer maupun saat data tersebut dikirim melalui email. Untuk menyimpan data tersebut agar benar-benar aman, tentunya dilakukan sistem pengamanan yang baik, yang bebas dari jangkauan orang-orang yang tidak berhak, baik bebas dari jangkauan secara fisik maupun secara sistem. Untuk bebas secara fisik, maka faktor orang sebagai penjaga memegang peranan yang penting, sedangkan bebas secara sistem adalah dokumen tersebut tersimpan dalam kondisi yang tidak dapat dibaca oleh orang yang tidak berhak. Apalagi jika data tersebut berada dalam suatu jaringan komputer yang terhubung atau terkoneksi dengan jaringan internet. Tentu saja data yang penting tersebut tidak boleh diketahui apalagi diubah oleh pihak yang

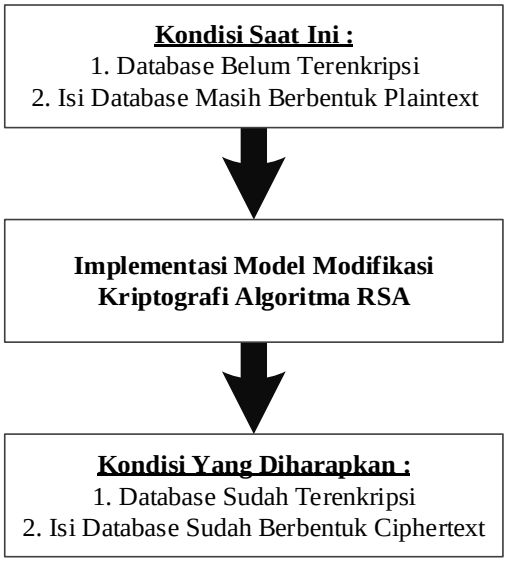
tidak berwenang. Dalam penelitian tersebut dikembangkan model sistem pengamanan data dengan proses enkripsi dan dekripsi menggunakan algoritma RSA untuk membangun sistem penyimpanan data transkrip nilai mahasiswa yang hasil simpanannya tidak dapat dibaca oleh orang, sehingga dapat disimpulkan bahwa algoritma RSA telah dapat diaplikasikan dalam pengamanan data transkrip akademik mahasiswa. [9]

2. Pada penelitian yang dilakukan oleh Indra Lasmana yang berjudul "Model Implementasi Keamanan Web Service dengan Kriptografi dan Tanda Tangan Digital Pada Sistem Informasi Akademik : Studi Kasus Universitas XYZ" dikatakan bahwa distribusi data dengan teknologi web service rentan terhadap penyadapan atau pencurian data, serta manipulasi data oleh pihak yang tidak berhak. Oleh karena itu, dibutuhkan suatu cara untuk mengamankan distribusi data pada web service agar data atau informasi tidak dapat dibaca oleh orang yang tidak berhak dan agar dapat diketahui jika data sudah dimanipulasi atau mengalami perubahan. Dengan teknik kriptografi menggunakan algoritma RSA dan tanda tangan digital menggunakan fungsi hash MD5, diharapkan dapat meningkatkan keamanan distribusi data akademik pada teknologi web service agar data atau informasi tidak bisa dibaca oleh orang yang tidak berhak, serta dapat diketahui jika terjadi manipulasi terhadap data oleh orang yang tidak berhak pada saat pengiriman data. [5]

Berdasarkan tinjauan studi diatas, maka perbedaan penelitian ini dengan penelitian sebelumnya yaitu terletak pada objek dan algoritma RSA yang akan digunakan sudah dikembangkan atau dimodifikasi. Pada penelitian ini dilakukan pengembangan atau modifikasi terhadap algoritma RSA yang akan digunakan dalam kriptografi pada database e-voting dengan tujuan untuk menjaga dan meningkatkan kerahasiaan dan keamanan data pada database tersebut.

2.4 Kerangka Konsep

Kerangka konsep yang akan digunakan dalam mengimplementasikan model modifikasi kriptografi algoritma RSA pada database e-voting guna menjaga dan meningkatkan kerahasiaan dan keamanan data terlihat pada gambar berikut ini :



Gambar 4. *Kerangka Konsep*

Gambar 4 merupakan kerangka konsep dalam penelitian ini dimana database yang sebelumnya belum terenkripsi dan isinya masih berbentuk plaintext yang dengan mudah dapat dibaca artinya secara langsung jika berhasil melihat isi dari database tersebut, oleh karena itu dalam penelitian ini akan dienkripsi dengan mengimplementasikan model modifikasi kriptografi algoritma RSA sehingga didapat hasil berupa database yang sudah terenkripsi dan isinya sudah berbentuk ciphertext yang tidak akan dapat terbaca artinya secara langsung jika berhasil melihat isi dari database tersebut tanpa melalui proses dekripsi.

3. Metodologi

3.1 Metode Penelitian

Dalam penelitian ini penulis menggunakan metode penelitian eksperimen. Metode penelitian eksperimen adalah metode penelitian yang dapat dilakukan manipulasi terhadap kondisi tertentu sesuai dengan kebutuhan atau tujuan penelitian. Dalam kondisi manipulasi terdapat dua kelompok yaitu kelompok kontrol dan kelompok pembanding. Kelompok kontrol akan diberikan perlakuan tertentu sesuai dengan tujuan penelitian dan hasil dari perlakuan tersebut akan dijadikan sebagai perbandingan terhadap kelompok pembanding.

3.2 Metode Pengumpulan Data

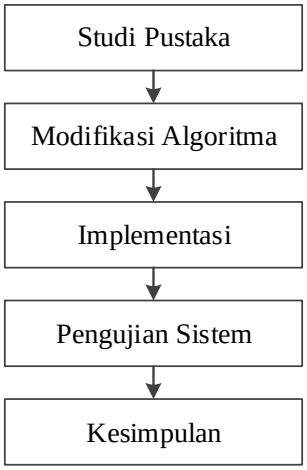
Metode pengumpulan data yang penulis gunakan dalam penelitian ini adalah studi pustaka. Dalam studi pustaka penulis mengumpulkan data dan informasi yang relevan dengan topik atau masalah yang akan diteliti. Data dan informasi tersebut penulis peroleh dari buku-buku ilmiah, karangan-karangan ilmiah, laporan penelitian, dan sumber-sumber tertulis lainnya baik cetak maupun elektronik, termasuk penelitian-penelitian terdahulu yang bersumber dari perpustakaan dan internet.

3.3 Metode Pengujian Sistem

Pengujian sistem yang penulis lakukan dalam penelitian ini meliputi pengujian validasi dan pengujian kualitas. Pengujian validasi dilakukan untuk mengetahui apakah sistem yang dibangun sudah benar sesuai dengan yang dibutuhkan. Pengujian validasi dilakukan dengan menggunakan metode black box, yaitu metode pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsionalitas dari program. Pada metode black box pengujian dilakukan dengan cara menjalankan dan mengeksekusi tiap modul program kemudian dilakukan pengamatan pada hasil atau output dari proses tersebut, apakah sudah sesuai dengan proses yang dikehendaki sehingga akan diketahui jika ada kesalahan atau bugs. Sedangkan pengujian kualitas dilakukan untuk menguji tingkat kualitas perangkat lunak atau sistem yang dihasilkan melalui metode eksperimen yang meliputi pengujian tingkat akurasi dan pengujian kinerja (waktu proses). Pengujian tingkat akurasi dilakukan untuk mengetahui apakah perangkat lunak atau sistem yang dihasilkan mempunyai tingkat keakuratan yang baik dalam hal melakukan proses enkripsi dan proses dekripsi. Pengujian kinerja (waktu proses) dilakukan untuk mengetahui apakah perangkat lunak atau sistem yang dihasilkan mempunyai kinerja (waktu proses) yang baik dalam hal melakukan proses enkripsi dan proses dekripsi.

3.4 Langkah-Langkah Penelitian

Langkah-langkah penelitian dalam penelitian ini adalah sebagai berikut :



Gambar 5. *Langkah-Langkah Penelitian*

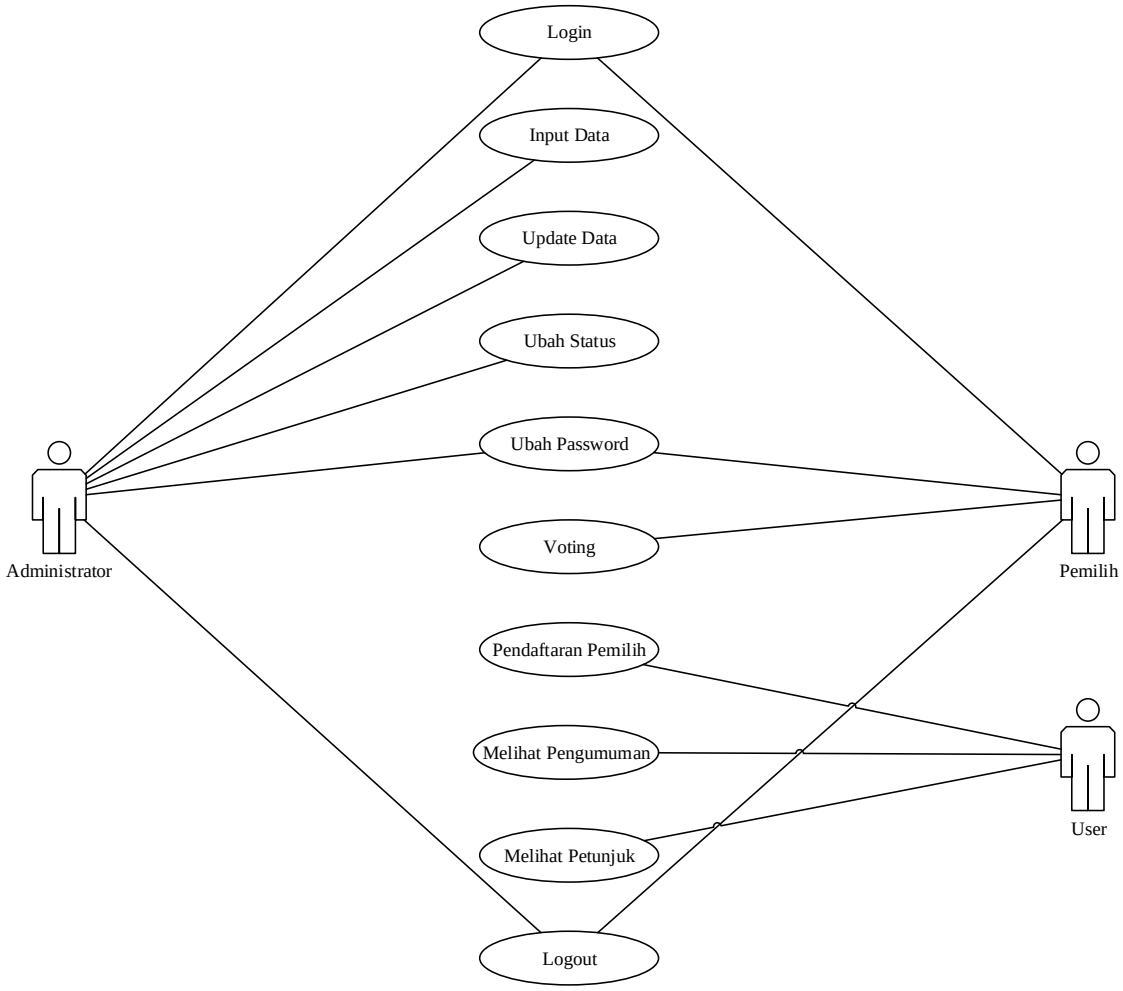
Penjelasan dari langkah-langkah penelitian tersebut adalah sebagai berikut :

1. Studi Pustaka
   Penelitian ini dimulai dengan melakukan studi pustaka yang berkaitan dengan judul yang diambil. Pada studi pustaka ini penulis mempelajari tentang keamanan data dan kriptografi yang bersumber dari buku-buku ilmiah, karangan-karangan ilmiah, laporan penelitian, dan sumber-sumber tertulis lainnya baik cetak maupun elektronik, termasuk penelitian-penelitian terdahulu yang bersumber dari perpustakaan dan internet.
2. Modifikasi Algoritma
   Setelah melakukan studi pustaka tentang keamanan data dan kriptografi, langkah selanjutnya adalah melakukan modifikasi terhadap algoritma RSA yang akan digunakan dalam kriptografi pada database e-voting.
3. Implementasi
   Setelah melakukan modifikasi terhadap algoritma RSA yang akan digunakan dalam kriptografi, langkah selanjutnya adalah mengimplementasikan hasil modifikasi tersebut ke dalam proses untuk mengamankan data pada database e-voting, sehingga keamanan data pada database tersebut dapat lebih terjamin.
4. Pengujian Sistem
   Setelah implementasi dilakukan, langkah selanjutnya adalah pengujian sistem. Pada langkah ini penulis melakukan pengujian sistem terhadap hasil implementasi dari model modifikasi kriptografi algoritma RSA pada database e-voting. Adapun pengujian sistem yang dilakukan meliputi pengujian tingkat akurasi dan pengujian kinerja (waktu proses).
5. Kesimpulan
   Setelah dilakukan pengujian sistem, maka langkah selanjutnya adalah mengambil kesimpulan yang bertujuan untuk menjelaskan kesesuaian antara pengujian sistem dengan hasil yang ingin dicapai.

4. Hasil dan Pembahasan

4.1 Analisis Sistem

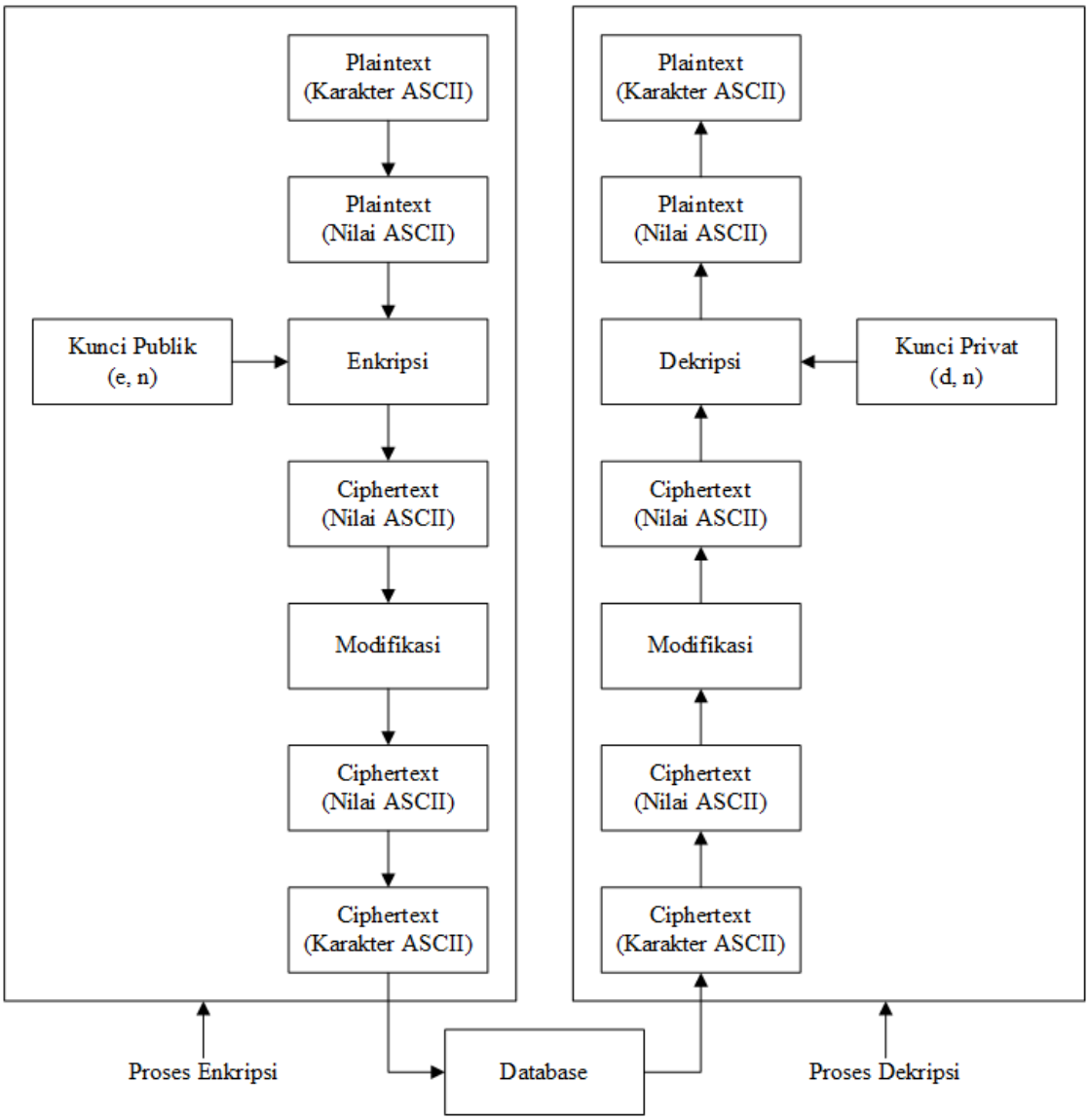
Analisis sistem akan mendeskripsikan kebutuhan sistem yang akan dibangun untuk memenuhi kebutuhan pengguna. Hasil dari analisis sistem ini akan digunakan dalam perancangan sistem. Analisis sistem dilakukan dengan pendekatan analisis berorientasi objek menggunakan Unified Modeling Language (UML). Penggunaan Unified Modeling Language (UML) ini diharapkan dapat menampilkan kebutuhan sistem berupa interaksi sistem dengan lingkungannya dan fungsionalitasnya. Diagram Unified Modeling Language (UML) yang digunakan dalam analisis sistem ini adalah use case diagram. Use case diagram digunakan untuk menggambarkan interaksi antara sistem dengan pengguna dan fungsionalitas yang diharapkan dari sebuah sistem [10]. Use case diagram digunakan selama tahap perancangan sistem untuk mendefinisikan kebutuhan sebuah sistem dan memahami bagaimana sebuah sistem seharusnya bekerja. Use case diagram dari sistem yang akan dibangun adalah sebagai berikut :



Gambar 6. *Use Case Diagram*

4.2 Perancangan Sistem

Perancangan sistem merupakan kelanjutan dari analisis sistem. Perancangan sistem dibuat berdasarkan hasil dari analisis sistem yang telah dilakukan sebelumnya. Perancangan sistem bertujuan untuk memberikan gambaran yang jelas dan rancang bangun mengenai sistem yang akan dibangun. Pada penelitian ini algoritma RSA yang digunakan untuk melakukan kriptografi telah dikembangkan atau dimodifikasi dengan tujuan untuk menjaga dan meningkatkan kerahasiaan dan keamanan data pada database. Perancangan model modifikasi kriptografi algoritma RSA yang akan digunakan dalam penelitian ini dapat dilihat pada gambar berikut :



Gambar 7. *Perancangan Model Modifikasi Kriptografi Algoritma RSA*

Perancangan model modifikasi kriptografi algoritma RSA diatas terbagi menjadi dua proses, yaitu proses enkripsi dan proses dekripsi. Penjelasan proses enkripsi untuk perancangan model modifikasi kriptografi algoritma RSA diatas adalah sebagai berikut :

1) Plaintext yang berbentuk karakter ASCII akan dirubah ke plaintext yang berbentuk nilai ASCII.
2) Plaintext yang sudah berbentuk nilai ASCII akan dienkripsi dengan menggunakan kunci publik (e, n).
3) Ciphertext hasil enkripsi yang masih berbentuk nilai ASCII akan dimodifikasi. Modifikasi yang dilakukan adalah ciphertext yang berbentuk nilai ASCII tersebut akan dibagi dengan suatu angka (misalkan angka 9), dari hasil pembagian tersebut akan diambil bilangan bulatnya dan digabungkan dengan bilangan sisa hasil pembagian dengan angka tersebut. Hasil penggabungan tersebut akan menghasilkan ciphertext yang berbentuk nilai ASCII baru.
4) Ciphertext yang berbentuk nilai ASCII baru tersebut akan dirubah ke ciphertext yang berbentuk karakter ASCII.
5) Ciphertext yang sudah berbentuk karakter ASCII tersebut akan disimpan ke dalam database.

Penjelasan proses dekripsi untuk perancangan model modifikasi kriptografi algoritma RSA diatas adalah sebagai berikut :

1) Ciphertext yang tersimpan di dalam database yang berbentuk karakter ASCII akan diambil dan dirubah ke ciphertext yang berbentuk nilai ASCII.

2) Ciphertext yang sudah berbentuk nilai ASCII tersebut akan dimodifikasi kembali sehingga bisa didekripsi. Modifikasi yang dilakukan adalah ciphertext yang berbentuk nilai ASCII tersebut akan dipisahkan menjadi dua bagian, yaitu bagian pertama berisi seluruh digit nilai ASCII kecuali satu digit paling belakang dan bagian kedua berisi satu digit nilai ASCII paling belakang. Bagian pertama dikalikan dengan angka yang digunakan dalam pembagian pada proses enkripsi sebelumnya (misalkan angka 9), kemudian hasil perkalian tersebut akan ditambahkan dengan bagian kedua yang berisi satu digit nilai ASCII paling belakang. Hasil penambahan tersebut akan menghasilkan ciphertext yang berbentuk nilai ASCII baru.
3) Ciphertext yang berbentuk nilai ASCII baru tersebut akan didekripsi dengan menggunakan kunci privat (d, n).
4) Plaintext hasil dekripsi yang masih berbentuk nilai ASCII akan dirubah ke plaintext yang berbentuk karakter ASCII.

Contoh proses enkripsi untuk perancangan model modifikasi kriptografi algoritma RSA diatas dengan plaintext yang akan dienkripsi adalah BUDI LUHUR dengan menggunakan kunci publik (7, 187) dapat dilihat pada tabel 3.

Tabel 3. *Contoh Proses Enkripsi*

P_i	Nilai ASCII P_i	$C_i = P_i^e \bmod n$	Modifikasi C_i	Karakter ASCII C_i
B	66	110	122	z
U	85	68	75	K
D	68	51	56	8
I	73	61	67	C
	32	76	84	T
L	76	32	35	#
U	85	68	75	K
H	72	30	33	!
U	85	68	75	K
R	82	91	101	e

Jadi berdasarkan tabel 3 diatas, maka ciphertext hasil enkripsi dari plaintext BUDI LUHUR yang akan disimpan ke dalam database dengan menggunakan kunci publik (7, 187) adalah zK8CT#K!Ke.

Contoh proses dekripsi untuk perancangan model modifikasi kriptografi algoritma RSA diatas dengan ciphertext yang akan didekripsi adalah zK8CT#K!Ke dengan menggunakan kunci privat (23, 187) dapat dilihat pada tabel 4.

Tabel 4. *Contoh Proses Dekripsi*

C_i	Nilai ASCII C_i	Modifikasi C_i	$P_i = C_i^d \bmod n$	Karakter ASCII P_i
z	122	110	66	B
K	75	68	85	U
8	56	51	68	D
C	67	61	73	I
T	84	76	32	
#	35	32	76	L
K	75	68	85	U
!	33	30	72	H
K	75	68	85	U
e	101	91	82	R

Jadi berdasarkan tabel 4 diatas, maka plaintext hasil dekripsi dari ciphertext zK8CT#K!Ke yang tersimpan di dalam database dengan menggunakan kunci privat (23, 187) adalah BUDI LUHUR.

4.3 Implementasi Sistem

Implementasi sistem merupakan kelanjutan dari perancangan sistem. Implementasi sistem dilakukan berdasarkan hasil dari perancangan sistem yang telah dilakukan sebelumnya. Implementasi sistem yang dimaksud adalah proses pembuatan sistem dari tahap perancangan sistem ke tahap coding yang akan

menghasilkan sistem yang telah dirancang sebelumnya. Adapun spesifikasi perangkat keras dan perangkat lunak yang digunakan adalah sebagai berikut :

1. Spesifikasi Perangkat Keras
   Spesifikasi perangkat keras yang digunakan dalam implementasi model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting ini adalah sebagai berikut :
   1) Processor Intel Core 2 Duo P8600 2.40 GHz
   2) Memori DDR2 3GB
   3) Hard Disk SATA 320GB
   4) VGA NVIDIA GeForce 9300M GS 512MB
   5) LCD 14" HD 1366 x 768

2. Spesifikasi Perangkat Lunak
   Spesifikasi perangkat lunak yang digunakan dalam implementasi model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting ini adalah sebagai berikut :
   1) Microsoft Windows 8.1 Pro
   2) Adobe Dreamweaver CC
   3) XAMPP for Windows versi 1.8.3.4
   4) Mozilla Firefox versi 29.0

4.4 Pengujian Sistem

Sebelum sebuah sistem baru diterapkan maka dibutuhkan pengujian sistem yang berguna untuk mengurangi atau bahkan menghilangkan kesalahan yang mungkin ada pada sistem tersebut dan untuk mengetahui apakah sistem tersebut telah mencapai tujuan yang diharapkan sehingga dapat dijadikan solusi dari permasalahan yang ada. Pengujian sistem yang dilakukan dalam penelitian ini meliputi :

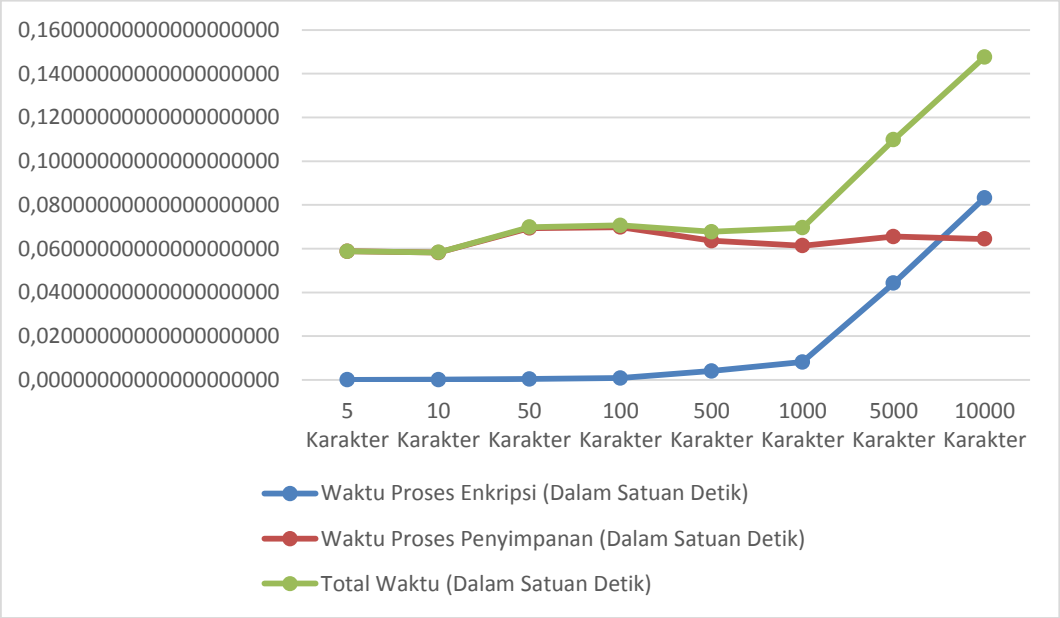
1. Pengujian Validasi
   Pengujian validasi dilakukan untuk mengetahui apakah sistem yang dibangun sudah benar sesuai dengan yang dibutuhkan. Pengujian validasi dilakukan dengan menggunakan metode black box, yaitu metode pengujian yang dilakukan hanya mengamati hasil eksekusi melalui data uji dan memeriksa fungsionalitas dari program. Pada metode black box pengujian dilakukan dengan cara menjalankan dan mengeksekusi tiap modul program kemudian dilakukan pengamatan pada hasil atau output dari proses tersebut, apakah sudah sesuai dengan proses yang dikehendaki sehingga akan diketahui jika ada kesalahan atau bugs. Berdasarkan hasil pengujian validasi, maka dapat diambil kesimpulan bahwa sistem yang dibangun sudah benar sesuai dengan yang dibutuhkan dan sudah berjalan sesuai dengan fungsionalitas yang diharapkan dari sistem tersebut.
2. Pengujian Kualitas
   Pengujian kualitas dilakukan untuk menguji tingkat kualitas perangkat lunak atau sistem yang dihasilkan melalui metode eksperimen yang meliputi pengujian tingkat akurasi dan pengujian kinerja (waktu proses). Pengujian tingkat akurasi dilakukan untuk mengetahui apakah perangkat lunak atau sistem yang dihasilkan mempunyai tingkat keakuratan yang baik dalam hal melakukan proses enkripsi dan proses dekripsi. Pengujian kinerja (waktu proses) dilakukan untuk mengetahui apakah perangkat lunak atau sistem yang dihasilkan mempunyai kinerja (waktu proses) yang baik dalam hal melakukan proses enkripsi dan proses dekripsi. Hasil pengujian kualitas pada model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting dengan menggunakan metode eksperimen adalah sebagai berikut :

Tabel 5. *Hasil Pengujian Kualitas*

No	Jumlah Karakter	Proses Enkripsi		
		Waktu Proses Enkripsi (Dalam Satuan Detik)	**Waktu Proses Penyimpanan (Dalam Satuan Detik)**	**Total Waktu (Dalam Satuan Detik)**
		1	**2**	**3**
1	5 Karakter	0.00005388259887695312	0.05875182151794433594	0.05880570411682128906
2	10 Karakter	0.00009417533874511719	0.05820584297180175781	0.05830001831054687500
3	50 Karakter	0.00041294097900390625	0.06939196586608886719	0.06980490684509277344

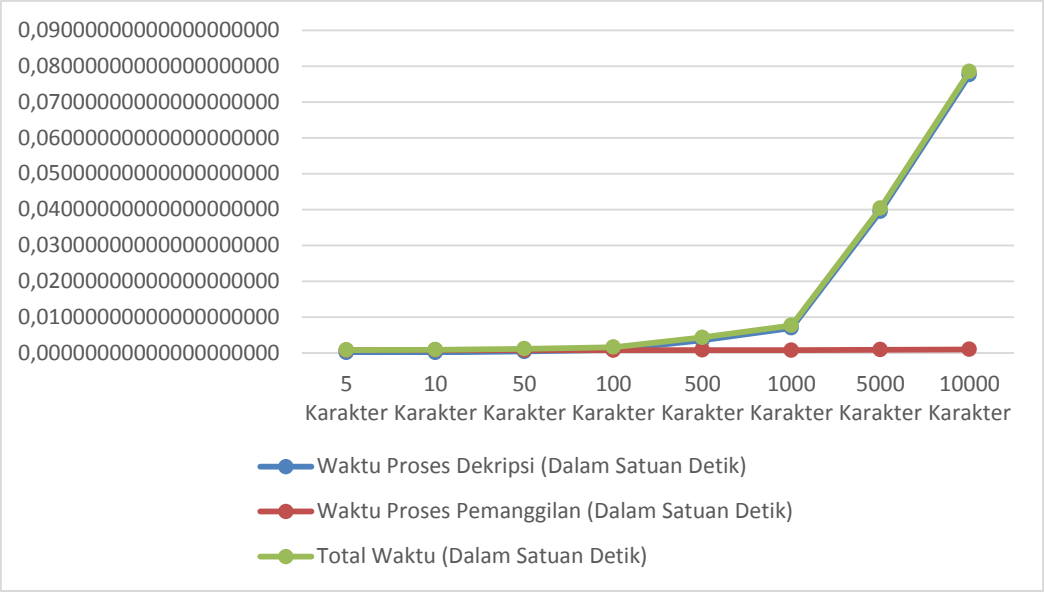
4	100 Karakter	0.00081801414489746094	0.06982398033142089844	0.07064199447631835938
5	500 Karakter	0.00404810905456542969	0.06363391876220703125	0.06768202781677246094
6	1000 Karakter	0.00812697410583496094	0.06138205528259277344	0.06950902938842773438
7	5000 Karakter	0.04421710968017578125	0.06553602218627929688	0.10975313186645507812
8	10000 Karakter	0.08321595191955566406	0.06442284584045410156	0.14763879776000976562

Berdasarkan tabel hasil pengujian kualitas diatas, maka dapat diambil kesimpulan bahwa kualitas dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting sudah sangat baik. Untuk kualitas berdasarkan tingkat akurasi sudah mencapai 100%, sedangkan untuk kualitas berdasarkan kinerja (waktu proses) dapat dilihat pada gambar berikut :



Gambar 8. *Grafik Kinerja Proses Enkripsi*

Berdasarkan gambar 8 diatas dapat diambil kesimpulan bahwa semakin banyak karakter yang dienkripsi maka waktu yang dibutuhkan untuk melakukan proses enkripsi akan semakin lama karena proses enkripsi dilakukan perkarakter sedangkan waktu yang dibutuhkan untuk melakukan proses penyimpanan ciphertext hasil proses enkripsi ke dalam database relatif sama untuk karakter yang sedikit maupun karakter yang banyak, sehingga total waktu yang dibutuhkan lebih tergantung pada waktu proses enkripsi.



Gambar 9. *Grafik Kinerja Proses Dekripsi*

Berdasarkan gambar 9 diatas dapat diambil kesimpulan bahwa semakin banyak karakter yang didekripsi maka waktu yang dibutuhkan untuk melakukan proses dekripsi akan semakin lama karena proses dekripsi dilakukan perkarakter sedangkan waktu yang dibutuhkan untuk melakukan proses pemanggilan ciphertext dari dalam database relatif sama untuk karakter yang sedikit maupun karakter yang banyak, sehingga total waktu yang dibutuhkan lebih tergantung pada waktu proses dekripsi.

4.5 Implikasi Penelitian

Implikasi penelitian adalah akibat langsung atau konsekuensi atas temuan atau hasil dari suatu penelitian. Implikasi penelitian bertujuan untuk membandingkan antara hasil penelitian terdahulu dengan hasil penelitian yang dilakukan. Implikasi penelitian dapat ditinjau dari beberapa aspek, yaitu :

1. Aspek Sistem
   Ditinjau dari aspek sistem maka implikasi penelitian dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting ini adalah dapat menjaga dan meningkatkan kerahasiaan dan keamanan data pada database tersebut, sehingga dapat memberikan rasa aman kepada semua pihak terkait terhadap ancaman pencurian ataupun perubahan data. Penggunaan kekuatan kunci harus selalu diperhatikan karena algoritma RSA dianggap sebagai algoritma kunci publik yang kuat dimana banyak perusahaan menggunakan teknik kriptografi dengan algoritma tersebut, sehingga hal ini akan membuat orang yang tidak bertanggung jawab berusaha untuk membongkar sistem keamanan pada algoritma tersebut.
2. Aspek Manajerial
   Ditinjau dari aspek manajerial maka implikasi penelitian dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting ini adalah perlu dilakukan peningkatan kompetensi sumber daya manusia dengan upaya pelatihan bagi pengguna sistem.
3. Aspek Penelitian Lanjut
   Ditinjau dari aspek penelitian lanjut maka implikasi penelitian dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting ini adalah perlu dilakukan penelitian lanjutan guna melakukan penyempurnaan. Penelitian lanjutan yang perlu dilakukan adalah memperluas ruang lingkup implementasi model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting yang lebih luas lagi, seperti pada database e-voting untuk pemilihan presiden dan wakil presiden suatu negara, serta mencari algoritma yang lebih baik atau algoritma tambahan yang dapat dikombinasikan dengan algoritma RSA yang telah peneliti kembangkan ini, sehingga memperoleh hasil penelitian yang lebih baik lagi.

5. Kesimpulan

5.1 Simpulan

Berdasarkan hasil penelitian tentang model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting diatas, maka dapat diambil kesimpulan sebagai berikut :

1. Solusi yang dapat diterapkan untuk menjaga dan meningkatkan kerahasiaan dan keamanan data pada database e-voting adalah dengan mengimplementasikan model modifikasi kriptografi algoritma RSA, sehingga dapat memberikan rasa aman kepada semua pihak terkait terhadap ancaman pencurian ataupun perubahan data.
2. Berdasarkan hasil pengujian validasi yang telah dilakukan didapat bahwa sistem yang dibangun sudah benar sesuai dengan yang dibutuhkan dan sudah berjalan sesuai dengan fungsionalitas yang diharapkan dari sistem tersebut.
3. Berdasarkan hasil pengujian kualitas yang telah dilakukan didapat bahwa kualitas dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting sudah sangat baik.
4. Untuk kualitas berdasarkan tingkat akurasi dalam hal melakukan proses enkripsi dan proses dekripsi sudah mencapai 100%, sedangkan untuk kualitas berdasarkan kinerja (waktu proses) dalam hal melakukan proses enkripsi dan proses dekripsi sudah relatif baik.

5.2 Saran

Berdasarkan hasil penelitian, implikasi penelitian, dan rencana implementasi dari model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting diatas, maka dapat diberikan saran sebagai berikut :

1. Penggunaan kekuatan kunci harus selalu diperhatikan (semakin panjang kunci yang digunakan semakin baik) karena algoritma RSA dianggap sebagai algoritma kunci publik yang kuat dimana banyak perusahaan menggunakan teknik kriptografi dengan algoritma tersebut, sehingga hal ini akan membuat orang yang tidak bertanggungjawab berusaha untuk membongkar sistem keamanan pada algoritma tersebut.
2. Untuk peneliti berikutnya dapat memperluas ruang lingkup implementasi model modifikasi kriptografi algoritma RSA untuk keamanan data pada database e-voting yang lebih luas lagi, seperti pada database e-voting untuk pemilihan presiden dan wakil presiden suatu negara.
3. Untuk peneliti berikutnya dapat mencari algoritma yang lebih baik atau algoritma tambahan yang dapat dikombinasikan dengan algoritma RSA yang telah peneliti kembangkan ini, sehingga memperoleh hasil penelitian yang lebih baik lagi.

6. Daftar Rujukan

[1] Rahmadhana Tanjung. “Perancangan Aplikasi Penyandian Data Text Menggunakan Metode Symmetric Stream Cipher”. Jurnal Pelita Informatika Budi Darma, Vol.IX No.3, (April, 2015) : 155-161.

[2] Reinhard M. Simbolon. “Perancangan Perangkat Lunak Enkripsi Pesan Dengan Metode Paillier Cryptosystem”. Jurnal Pelita Informatika Budi Darma, Vol.V No.3, (Desember, 2013) : 23-30.

[3] Munawar. “Perancangan Algoritma Sistem Keamanan Data Menggunakan Metode Kriptografi Asimetris”. Jurnal Komputer dan Informatika (KOMPUTA), Vol.I No.1, (Maret, 2012) : 11-17.

[4] Rinaldi Munir. “Pengantar Kriptografi”. 3rd ed. Bandung : Informatika. 2013.

[5] Indra Lasmana. “Model Implementasi Keamanan Web Service dengan Kriptografi dan Tanda Tangan Digital Pada Sistem Informasi Akademik : Studi Kasus Universitas XYZ”. Tesis, Universitas Budi Luhur, 2014.

[6] Dony Ariyus. “Pengantar Ilmu Kriptografi”. 2nd ed. Yogyakarta : Andi. 2012.

[7] Muhammad Safri Lubis, et.al. “Penggunaan Algoritma RSA dengan Metode The Sieve of Eratosthenes dalam Enkripsi dan Deskripsi Pengiriman Email”. Seminar Nasional Aplikasi Teknologi Informasi (SNATI), (Juni, 2013) : 28-33.

[8] Muhammad Arief, et.al. “Kriptografi RSA Pada Aplikasi File Transfer Client - Server Based”. Jurnal Ilmiah Teknologi Informasi Terapan, Vol.I No.3, (Agustus, 2015) : 45-51.

[9] Tri Rahajoeningroem and Muhammad Aria. “Studi dan Implementasi Algoritma RSA Untuk Mengamankan Data Transkrip Akademik Mahasiswa”. Majalah Ilmiah UNIKOM, Vol.8 No.1, (Mei, 2011) : 77-90.

[10] Muhamad Muslihudin, et.al. “Analisis dan Perancangan Sistem Informasi Menggunakan Model Terstruktur dan UML”. 1st ed. Yogyakarta : Andi. 2016.