Naskah Publikasi

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA ASIMETRIS *RIVEST SHAMIR ADLEMAN*

Program Studi Informatika

Disusun oleh:
Muhammad Pandu Affandi
5150411254

PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNOLOGI INFORMASI DAN ELEKTRO
UNIVERSITAS TEKNOLOGI YOGYAKARTA

2020

Naskah Publikasi

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA ASIMETRIS *RIVEST SHAMIR ADLEMAN*

Disusun Oleh :
MUHAMMAD PANDU AFFANDI
5150411254

Pembimbing

Dr. Erik Iman Heri Ujianto, M.Kom.

Tanggal 25/09/2020

IMPLEMENTASI KRIPTOGRAFI UNTUK KEAMANAN DATA TEKS MENGGUNAKAN ALGORITMA ASIMETRIS *RIVEST SHAMIR ADLEMAN*

Muhammad Pandu Affandi, Erik Iman Heri Ujianto
Program Studi Informatika, Fakultas Teknologi Informasi dan Elektro
Universitas Teknologi Yogykarta
Jl. Ringroad Utara Jombor Sleman Yogyakarta
E-mail : pandu.affandi15@gmail.com erik.iman@uty.ac.id

ABSTRAK

Perkembangan teknologi terutama pada sistem pengamanan data dalam menjaga keamanan data informasi berkembang sangat pesat. Dalam menjaga keamanan data informasi terdapat cabang ilmu dalam pengembangannya seperti kriptografi dan steganografi. Pada penerapannya dilakukan tidak hanya pada satu teknik keamanan, melainkan bisa dilakukan dengan kombinasi dalam keamanan data informasi. Penelitian ini bertujuan untuk membuat sebuah sistem keamanan data dengan mengimplementasikan kriptografi pada teks dengan melakukan perhitungan algoritma Rivest Shamir Adleman (RSA). RSA merupakan algoritma cryptographic yang dapat digunakan untuk mengamakan data dan algoritmanya adalah blockciphertext asimetrik yang dapat mengenkripsi (encipher) dan dekripsi (decipher) teks dengan menggunakan dua kunci, yaitu private key dan public key. Hasil dari penelitian yaitu pengguna dapat mengenkripsi teks dan teks hasil enkripsi tersebut didekripsi kembali dengan menggunakan dua kunci agar keamanan data informasi tersebut dapat terjaga keamanannya karena telah dilakukan pengamanan dan penyandian menggunakan dua kunci yang berbeda.
Kata kunci : Keamanan, Enkripsi, Dekripsi, Kriptografi, Rivest Shamir Adleman.

1. PENDAHULUAN

Teknologi komputer sangat dibutuhkan oleh kehidupan manusia terutama personal maupun kelompok (organisasi). Kelompok (organisasi) tersebut sangat membutuhkan adanya komputerisasi dalam setiap kegiatan. Dari hal penggunaan komputerisasi tersebut, dibuat sebuah keamanan bagi seluruh aset-asetnya, terutama informasi-informasi dan data-data penting demi menjaga kerahasiaan informasi data tersebut. Dari keamanan data tersebut menimbulkan tuntutan akan tersedianya suatu sistem pengamanan data yang lebih baik agar dapat mengamankan data dari berbagai ancaman. Ini merupakan latar belakang berkembangnya sistem keamanan data yang berfungsi untuk melindungi data yang ditransmisikan atau dikirimkan melalui suatu jaringan komunikasi.

Algoritma *Rivest-Shamir-Adleman* (RSA) merupakan algoritma yang ditemukan oleh Ron Rivest, Adi Shamir dan Len Adleman. Algoritma ini menggunakan dua kunci yaitu *public key* dan *private key*. Algoritma *Rivest-Shamir-Adleman* dapat digunakan untuk menjaga kerahasiaan informasi data dengan menggunakan enkripsi dan dekripsi yang tidak mudah untuk dipecahkan. Algoritma ini melindungi data dari serangan konvensional (*linear dan diferensial attack*) yang menggunakan statistik untuk memecahkan sandi, dan untuk melakukan proses enkripsi dan dekripsi algoritma ini harus memasukan kata kunci yang berbeda dalam melakukan pengamanan maupun untuk membuka pengamanan tersebut.

2. LANDASAN TEORI

Dasar teori adalah seperangkat definisi, konsep serta proposisi yang telah disusun rapi serta sistematis tentang variabel-variabel dalam sebuah penelitian. Dasar teori ini akan menjadi dasar yang kuat dalam sebuah penelitian yang akan dilakukan. Pengamanan data harus diterapkan dimanapun dan kapanpun agar terhindar dari kejahatan yang dilakukan oleh pihak-pihak yang tidak bertanggung jawab.

2.1. Sistem

Menurut [1] sistem adalah rangkaian dari dua atau lebih komponen-komponen yang saling berhubungan, yang berinteraksi untuk mencapai suatu tujuan. Sebagian besar sistem terdiri dari subsistem yang lebih kecil yang mendukung sistem yang lebih besar.

2.2. HTML

Menurut [2] *HyperText Markup Language* (HTML) adalah sebuah bahasa markup yang digunakan untuk membuat sebuah halaman web, menampilkan berbagai informasi di dalam sebuah penjelajah *web Internet* dan *formating hypertext* sederhana yang ditulis kedalam berkas format ASCII agar dapat menghasilkan tampilan wujud yang terintegerasi. Dengan kata lain, berkas yang dibuat dalam perangkat lunak pengolah kata dan disimpan kedalam format ASCII normal sehingga menjadi *home page* dengan perintah-perintah HTML. Bermula dari sebuah bahasa yang sebelumnya banyak digunakan di dunia penerbitan dan percetakan yang disebut dengan SGML (*Standard Generalized Markup Language*), HTML adalah sebuah standar yang digunakan secara luas untuk menampilkan halaman web. HTML saatini merupakan standar Internet yang didefinisikan dan dikendalikan penggunaannya oleh *World Wide Web Consortium* (W3C). HTML dibuat oleh kolaborasi Caillau TIM dengan Berners-lee robert ketika mereka bekerja di CERN pada tahun 1989.

2.3. Kriptografi

Menurut [3] kriptografi merupakan sebuah teknik rahasia dalam penulisan, dengan karakter khusus, dengan menggunakan huruf dan karakter di luar bentuk aslinya, atau dengan metode-metode lain yang hanya dipahami oleh pihak-pihak yang memproses kunci, juga semua hal yang ditulis dengan cara seperti ini.

2.4. Enkripsi

Menurut [4] Enkripsi merupakan cara pengamanan data yang dikirimkan sehingga terjaga kerahasiaannya. Pesan asli disebut plaintext (teks biasa), yang diubah menjadi kode-kode yang tidak dimengerti. Enkripsi bisa diartikan dengan *cipher* atau kode.

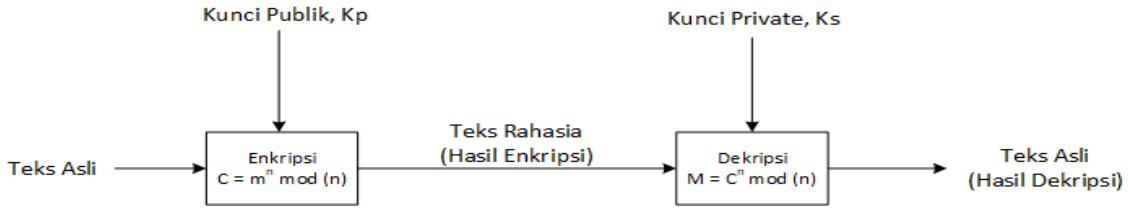
2.5. Dekripsi

Menurut [5] Dekripsi merupakan kebalikan dari enkripsi. Pesan yang telah dienkripsi dikembalikan ke bentuk asalnya. Algoritma yang digunakan untuk dekripsi tentu berbeda dengan yang digunakan untuk dekripsi.

2.6. Algoritma Asimetris

Menurut [6] pada buku pengantar ilmu kriptografi, algortima asimetri sering juga disebut dengan algoritma kunci publik, dengan arti kata kunci yang digunakan untuk melakukan enkripsi dan dekripsi berbeda. Pada algoritma asimetri kunci terbagi menjadi dua bagian, yaitu:

1. Kunci publik, kunci publik merupakan kunci yang boleh semua orang tahu (dipublikasikan).
2. Kunci Privat, Kunci yang dirahasiakan (hanya boleh diketahui oleh pemilik data).



Gambar 1: Algoritma Asimetris

2.7. CSS

CSS (Cascading Style Sheet) adalah stylesheet language sekumpulan kode pemrograman web yang berfungsi untuk mengendalikan beberapa komponen di dalam web sehingga menjadi tampak seragam, berstruktur, dan teratur [7].

2.8. PHP

Menurut [8], PHP adalah sebuah bahasa pemograman yangberjalan dalam sebuah *web-server* (*Serverside*). PHP diciptakan oleh programmer Unix dan Perl yang bernama Rasmus Lerdoft pada 1994. Script PHP adalah bahasa program yang berjalan pada sebuah web server, atau sering disebut *serverside*. Oleh karena itu, PHP dapat melakukan apa saja yang bisa dilakukan program CGI lain, yaitu mengolah data dengan tipe apapun, menciptakan halaman web yang dinamis, serta menerima dan menciptakan Cookies, dan bahkan PHP bisa melakukan lebih dari itu.

2.9. UML

Unified Modeling Language (UML) adalah bahasa pemodelan standar untuk pengembangan perangkat lunak dan sistem. Pernyataan ini adalah argumen yang cukup konklusif untuk menjadikan UML bagian dari reperator perangkat lunak. UML menjadi standar dalam industri untuk visualisasi, merancang dan mendokumentasikan sistem piranti lunak. UML menawarkan sebuah standar untuk merancang model sebuah sistem, dengan menggunakan UML, dapat membuat model untuk semua jenis aplikasi piranti lunak, dimana aplikasi tersebut dapat berjalan pada piranti keras, sistem operasi dan jaringan apapun, serta di tulis dalam bahasa pemrograman apapun. UML juga menggunakan class dan operation. Dalam konsep dasarnya, maka UML lebih cocok untuk penulisan piranti lunak dalam bahasa-bahasa berorientasi objek seperti C++, Java, C#, Matlab atau VB.NET. Walaupun demikian, UML tetap dapat digunakan untuk modeling aplikasi procedural dalam VB atau C. Seperti bahasa-bahasa lainnya, UML mendefinisikan notasi dan syntax atau semantik. Notasi UML merupakan sekumpulan bentuk khusus untuk menggambarkan berbagai diagram piranti lunak. Setiap bentuk memiliki makna tertentu, dan UML syntax mendefinisikan bagaimana bentuk-bentuk tersebut dapat dikombinasikan. Notasi UML terutama diturunkan dari 3 notasi yang telah ada sebelumnya: Grady Booch OOD (*Object Oriented Design*), Jim Rumbaugh OMT (*Object Modeling Technique*), dan Ivar Jacobson OOSE (*Object-Oriented Software Engineering*). *Unified Modeling Language* (UML) adalah alat bantu (*Tool*) untuk pemodelan sistem, "UML adalah bahasa yang dapat digunakan untuk spesifikasi, visualisasi, dan dokumentasi sistem *Object Oriented Software* pada fase pengembangan. UML merupakan unifikasi darimetode Booch, OMT, dan notasi *Objectory*, serta ide-ide terbaik metodologi lainnya, UML merupakan standar dasar dalam bidang analisis dan desain berorientasi-objek". *Unified Modeling Language* (UML) adalah sebuah bahasa pemodelan yang telah menjadi standar dalam industri software untuk visualisasi, merancang, dan mendokumentasikan sistem perangkat lunak. Bahasa Pemodelan UML lebih cocok untuk pembuatan perangkat lunak dalam bahasa pemrograman berorientasi objek (C, Java, VB.NET), namun demikian tetap dapat digunakan pada bahasa pemrograman prosedural. Di dalam *Unified Modeling Language* (UML) terdapat content untuk menganalisis suatu *software*. Diantaranya, ada *Use Case Diagram*, *Sequence Diagram*, dan *Activity Diagram* [9].

3. METODOLOGI PENELITIAN

3.1. Penelitian Pendahulu

Tahap ini merupakan tahap awal dalam metode pemecahan masalah. Pada tahap ini dilakukan studi pustaka untuk mengetahui hal-hal yang perlu diamati dan masalah yang terjadi saat ini. Dalam hal ini peneliti mengamati hal-hal yang berhubungan dengan masalah keamanan data khususnya data teks. Dengan melakukan studi ini, diharapkan peneliti mendapatkan data dan informasi yang dibutuhkan untuk tahap-tahap penelitian berikutnya.

3.2. Identifikasi Masalah

Dari hasil pengamatan dan observasi yang dilakukan peneliti dengan keadaan yang terjadi pada saat ini diidentifikasi masalah-masalah yang muncul untuk selanjutnya dipelajari. Salah satu permasalahan yang dihadapi oleh pengguna internet khususnya adalah dalam melakukan pengiriman data teks yang bersifat rahasia masih banyak kejahatan yang terjadi seperti penyadapan data dan *security threats* yang lain. Hal ini dapat merugikan pihak pengguna internet jika data yang disadap merupakan data penting yang sifatnya rahasia dan dipergunakan tidak sebagaimana mestinya.

3.3. Studi Pustaka

Studi pustaka adalah proses pengumpulan informasi yang dibutuhkan untuk melakukan penelitian. Studi pustaka dilakukan dengan melakukan pencarian bahan-bahan dan pengambilan informasi yang relevan. Sumber studi pustaka mengambil informasi dari jurnal, skripsi dan sumber lain dengan kasus mengenai implementasi kriptografi.

3.4. Tujuan Penelitian

Tujuan yang hendak dicapai dari penelitian ini adalah bertujuan untuk mengimplementasikan algoritma *Rivest-Shamir-Adleman* yang dapat menjaga keamanan data pada teks dari pihak yang tidak berwenang.

3.5. Pengumpulan Data

Data yang digunakan pada penelitian ini adalah data berupa teks. Teks ini dikumpulkan dari dokumen yang sebelumnya berbentuk format TXT atau Notepad, data yang digunakan untuk pengujian adalah dokumen teks dengan ukuran teks yang sedikit, dokumen teks dengan ukuran teks yang banyak, dokumen yang berisikan angka dan dokumen yang berisikan simbol-simbol. Data yang telah dikumpulkan sebelumnya menjadi data utama yang akan digunakan untuk pengujian sistem.

3.6. Pengelolaan Data

Pengolahan data dilakukan berdasarkan toeri-teori yang terdapat pada buku, situs internet, thesis dan jurnal yang dijadikan peneliti menjadi sebuah referensi. Setelah data kumpulkan langkah selanjutnya adalah pengolahan data dengan tahapan, yakni:

a. Menentukan nilai awal P dan Q.
b. Menentukan nilai modulus atau pembagi.
c. Menentukan kunci publik.
d. Menentukan kunci privat.
e. Menghitung proses enkripsi.
f. Menghitung proses dekripsi.

3.7. Analisis Data

Pada tahap ini, dilakukan analisis terhadap data yang telah dikumpulkan dan telah diolah melalui pengolahan data. Analisis data ini berhubungan dengan teks, angka dan simbol yang digunakan untuk proses enkripsi dan dekripsi. Dengan demikian peneliti dapat mengetahui data apa saja yang dapat dilakukan proses enkripsi dan dekripsi.

4. HASIL DAN PEMBAHASAN

4.1. Analisa Sistem

4.1.1 Analisis Sistem yang Berjalan

Analisis sistem yang berjalan saat ini pengguna yang mempunyai *file* penting khususnya *file* berbentuk teks dan pengguna ingin mengirim *file* tersebut kepada orang lain masih rawan akan kebocoran data. Hal ini menyebabkan kebocoran data dan kerugian bagi pihak pengguna yang mempunyai berkas penting.

4.1.2 Analisis Sistem yang Diusulkan

Sistem yang diusulkan yaitu dengan memanfaatkan algoritma *Rivest Shamir Adleman* (RSA) untuk mengenkripsi data berbentuk angka, simbol-simbol dan data teks dengan jumlah teks yang berbeda-beda, supaya data yang berada di dalam berkas tersebut tidak dapat diketahui oleh orang lain. Hal ini diharapkan mampu membantu pengguna untuk melakukan proses pengiriman berkas tanpa khawatir dengan data yang ada di dalam berkas tersebut tersebar.

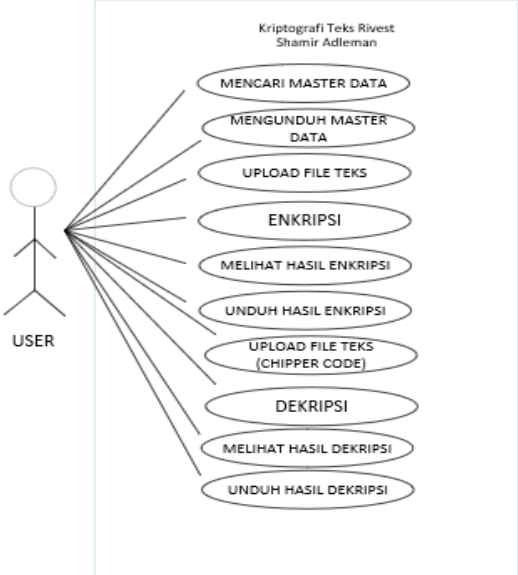
4.2. Desain Sistem

4.2.1 Perancangan Logik

Rancangan sistem merupakan pemodelan sistem dan alur kerja sistem yang berjalan. Proses perancangan menggunakan UML, yang meliputi *use case diagram, sequence diagram* dan *activity diagram.*

a. *Use Case Diagram*

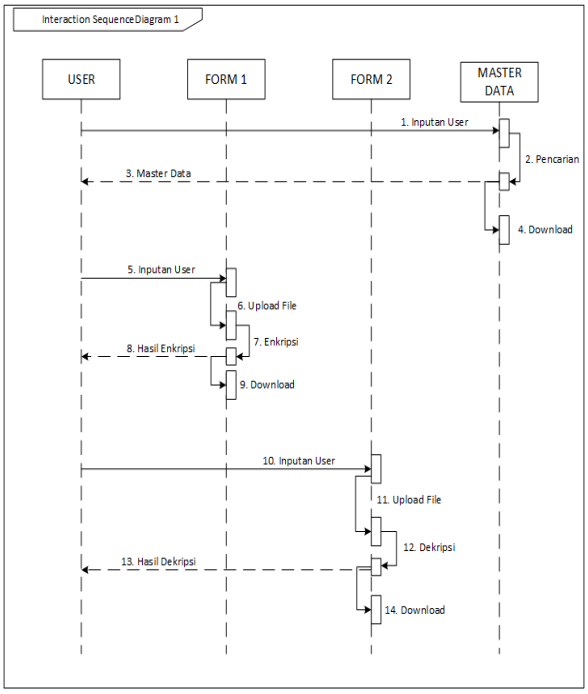
Bersifat statis dan digunakan untuk memodelkan proses-proses bisnis atau penggunaan sistem. Diagram ini memperlihatkan himpunan use case dan aktor-aktor (suatu jenis khusus dari kelas). Diagram ini sangat penting terutama untuk mengorganisasi dan memodelkan perilaku suatu sistem yang dibutuhkan. Rancangan use case diagram ditunjukan pada Gambar 2.



Gambar 2: Use Case Diagram

b. *Sequence Diagram*

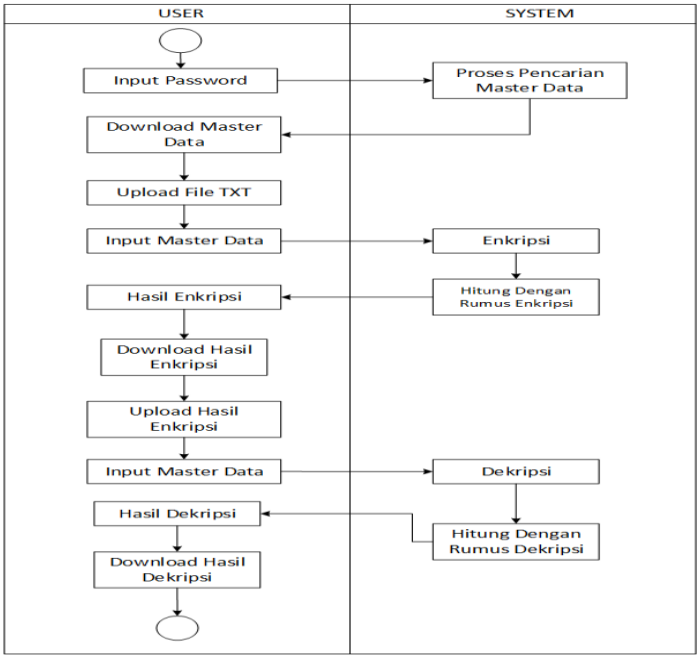
Pada *Sequence Diagram* pada sistem memodelkan pengiriman pesan antar obyek dan interaksinya. Rancangan *Sequence Diagram* ditunjukan pada Gambar 3.



Gambar 3: Sequence Diagram

c. *Activity Diagram*

Activity Diagram digunakan untuk menggambarkan aliran aktifitas dari awal hingga akhir yang terjadi antar aktor dengan sistem. Aliran aktivitas sistem implementasi kriptografi dapat dilihat pada Gambar 4.



Gambar 4: Activity Diagram

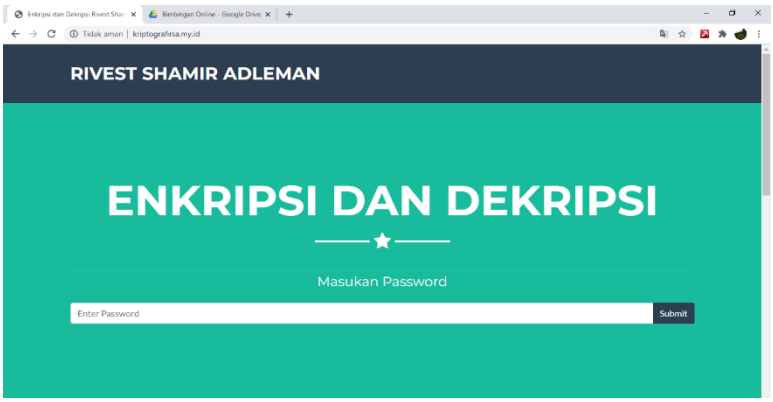
4.2.2 Perancangan Fisik

Perancangan fisik meliputi rancangan antar muka. Perancangan antar muka pengguna antara lain:

1. Rancangan halaman masuk.
2. Rancangan halaman *master data*.
3. Rancangan halaman enkripsi.
4. Rancangan halaman hasil enkripsi.
5. Rancangan halaman dekripsi.
6. Rancangan halaman hasil dekripsi.

4.3. Implementasi

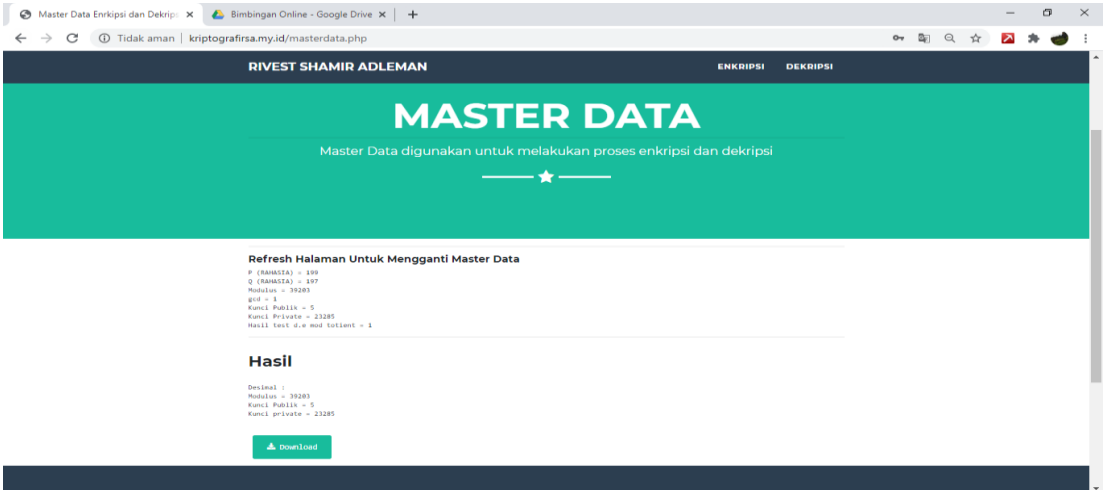
Sistem yang diterapkan diharapkan dapat membantu mempermudah pengguna dalam melakukan pengamanan data yang bersifat rahasia dan penting sehingga jika terjadi penyadapan data, pengguna tidak khawatir datanya akan diketahui isinya dan tidak dipergunakan untuk kejahatan oleh orang-orang yang tidak bertanggung jawab. Sistem ini juga dapat melakukan upload dan download supaya semua data mulai dari master data untuk proses enkripsi dan dekripsi hingga hasil enkripsi dan dekripsi tidak hilang dan terlupakan. Hak akses pada sistem ini hanya pengguna.
Halaman masuk adalah halaman yang muncul pertama kali saat program sistem dijalankan. Tampilan halaman masuk dapat dilihat pada Gambar 5 sebagai berikut.



Gambar 5: Halaman Masuk

Gambar 5 diatas merupakan tampilan halaman masuk. *Textfield* yang pertama merupakan tempat untuk menginputkan *password*. Kemudian tombol *submit* berfungsi untuk memproses inputan. Ketika *password* yang di inputkan oleh pengguna sesuai dengan *password* maka halaman akan dialihkan ke *form* selanjutnya, yaitu *form master data* untuk mendapatkan komponen-komponen enkripsi dan dekripsi.

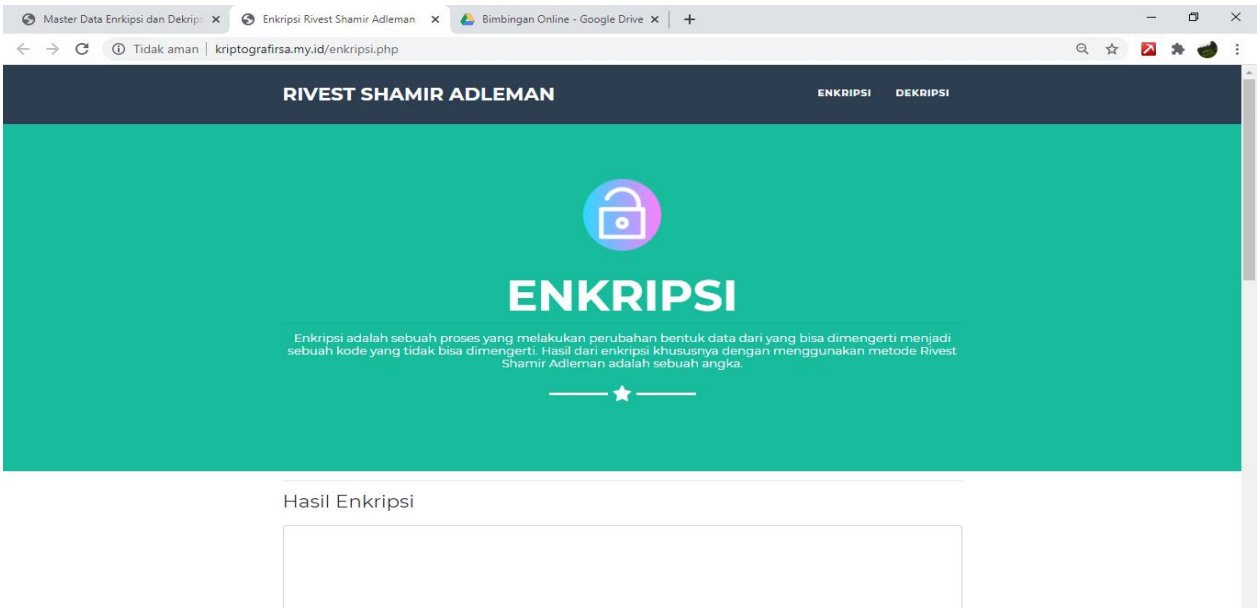
Halaman *master data* adalah halaman utama setelah *login*. *Form master data* merupakan tampilan yang terdapat setelah pengguna memasukan kata sandi. Untuk halaman *master data* dapat dilihat pada Gambar 6.



Gambar 6: Halaman Master Data

Pada Gambar 6 di atas halaman *master data* berisikan nilai P, Q, modulus, gcd, kunci publik, kunci privat dan hasil gcd. Pada halaman *master data* dapat dilakukan proses unduh atau *download* agar tidak terjadi kehilangan pada *master data*.

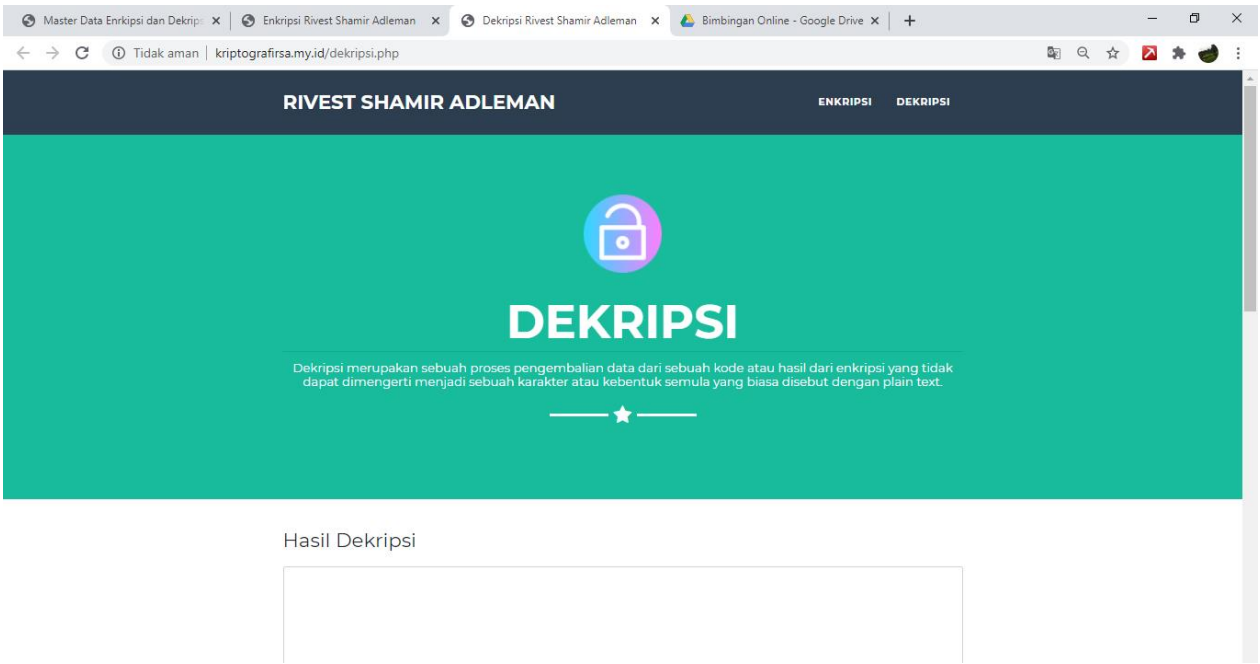
Halaman enkripsi adalah halaman yang digunakan pengguna untuk melakukan proses enrkipsi atau pengubahan teks menjadi kode yang tidak dimengerti, pada halaman ini pengguna harus meng-*upload* file berformat txt atau notepad dan memasukan *master data* yang telah diunduh sebelumnya. Halaman enkripsi dapat dilihat pada Gambar 7 sebagai berikut.



Gambar 7: Halaman Enkripsi

Hasil enkripsi terdapat pada *form* yang paling atas sehingga pengguna dapat melihat langsung hasil dari enkripsi tanpa pindah kehalaman lainnya.

Halaman dekripsi sama halnya dengan halaman enkripsi, yaitu pengguna yang telah melakukan proses enkripsi dapat melakukan proses dekripsi jika pengguna tersebut mempunyai komponen-komponen proses dekripsi yang sebelumnya diakses pada halaman *master data.* Halaman dekripsi dapat dilihat pada Gambar 8 sebagai berikut.



Gambar 8: Halaman Dekripsi

Pada Gambar 8 hasil dekripsi tedapat pada *form* paling atas sehingga pengguna dapat melihat langsung hasil dari proses dekripsi tanpa pindah ke halaman lainnya.

PENUTUP

5.1. Simpulan

Berdasarkan keseluruhan proses analisis, perancangan dan implementasi atas pengembangan sistem Implementasi Kriptografi untuk Keamanan Data Teks Menggunakan Algoritma Asimetris *Rivest Shamir Adleman* maka diperoleh kesimpulan sebagai berikut:

1. Sistem implementasi kriptografi untuk pengamanan data teks menggunakan metode Rivest Shamir Adleman mampu melakukan proses enkripsi dan dekripsi tanpa merusak datanya.
2. Sistem implementasi kriptografi menggunakan metode Rivest Shamir Adleman mampu melakukan enkripsi dan dekripsi terhadap data yang berformat txt.
3. Sistem implementasi kriptogtafi menggunakan metode *Rivest Shamir Adleman* mempunyai tingkat keamanan data yang tinggi, karna metode RSA mempunyai keamanan pada tingkat kesulitan dalam memfaktorkan bilangan non-prima menjadi faktor prima. Dan tingkat keamanan enkripsi sistem ini juga terdapat pada pengguna (orang yang melakukan proses enkripsi) karna hanya pengguna yang mengakses dan memasukan kata sandi pada sistem untuk mengakses master data yang digunakan untuk proses enkripsi dan dekripsi.

5.2. Saran

Berdasarkan analisa dan kesimpulan di atas, untuk meningkatkan kinerja sistem atas bahasan dalam hasil penelitian ini, maka peneliti mencantumkan beberapa saran, antara lain adalah:

1. Untuk pengembangan sistem, dapat ditambahkan format *file* yang lain seperti DOCX atau DOC.
2. Algoritma yang digunakan pada sistem kriptografi dapat dikembangkan untuk topik bahasan yang lebih luas, tidak hanya terbatas pada data teks, seperti untuk keamanan jaringan contohnya.

DAFTAR PUSTAKA

[1] Romney, M.B. and Steinbart, P.J. (2014), Accounting Of Information System, ed. 13 Prentice Hall.

[2] Harison and Syarif, A. (2016), Sistem Informasi Geografis Sarana Pada Kabupaten, Jurnal TEKNOIF, 4(2), 76–81.

[3] Talbot, J. and Welsh, D. (2006), Complexity And Cryptography, ed. 1st Cambridge: Cambridge University Press.

[4] Ariyus, D. (2017), Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, 1st Publis Yogyakarta: Penerbit Andi.

[5] Ariyus, D. (2017), Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, 1st Publis Yogyakarta: Penerbit Andi.

[6] Ariyus, D. (2017), Pengantar Ilmu Kriptografi: Teori Analisis & Implementasi, 1st Publis Yogyakarta: Penerbit Andi.

[7] Komputer, W. (2015), PAS: Membangun Sistem Informasi Dengan Java Netbeans Dan MySQL, 1st Publis Semarang: C.V Andi Offset Semarang.

[8] Harison and Syarif, A. (2016), Sistem Informasi Geografis Sarana Pada Kabupaten, Jurnal TEKNOIF, 4(2), 76–81.

[9] Miles, R. and Hamilton, K. (2006), Learning UML 2.0, B. McLaughlin & M. T. O'Brien, Eds. ed. 1st United States of America: O'Reilly Media, Inc.