
IMPLEMENTASI ALGORITMA RSA UNTUK PENGAMANAN DATA MOA PADA PT. BUNGKUS TEKNOLOGI INDONESIA

Rianto Pangihutan Pangaribuan*, Azanuddin, S.Kom., M.Kom**, Ita Mariami, SE.,Msi***

* Sistem Informasi, STMIK Triguna Dharma

** Sistem Informasi, STMIK Triguna Dharma

Article Info

Article history:

-

Keyword:

Kriptografi
Pengamanan Data
RSA
Data MoA

ABSTRACT

Secara yuridis kerjasama dikenal dengan istilah Nota Kesepahaman (dalam bahasa hukum disebut MoU) dan Perjanjian (dalam bahasa hukum disebut MoA). Terdapat beberapa perusahaan maupun instansi pemerintahan yang sudah menjalin kerjasama (MoU) dan sampai dalam kesepakatan (MoA) dengan PT. Bungkus Teknologi Indonesia. Setelah melakukan kesepakatan, PT. Bungkus Teknologi Indonesia menyimpan surat perjanjian tersebut menjadi arsip elektronik atau disebut juga dengan dokumen digital. Dokumen digital ini bersifat rahasia dan hanya dapat di kelola oleh Direktur dari PT. Bungkus Teknologi Indonesia. Namun dokumen digital tersebut belum disertai dengan sistem keamanan, sehingga dikhawatirkan akan terjadi manipulasi data yang dilakukan oleh orang yang tidak berwenang dan bertanggung jawab atas dokumen tersebut.

Untuk membantu PT. Bungkus Teknologi Indonesia dalam mengamankan data digital MoA dapat dilakukan dengan membuat sebuah sistem security dengan algoritma RSA.

Dengan berhasilnya dibangunnya sistem security untuk mengamankan data digital ini, PT. Bungkus Teknologi Indonesia sangat terbantu dalam menjaga keamanan data MoA tanpa perlu khawatir terjadinya manipulasi data oleh pihak yang tidak bertanggung jawab.

Copyright © 2020 STMIK Triguna Dharma.
All rights reserved.

Corresponding Author:

Nama : Rianto Pangihutan Pangaribuan
Program Studi : Sistem Informasi
Kampus : STMIK Triguna Dharma
Email : riantopangaribuan718@gmail.com

1. PENDAHULUAN

PT. Bungkus Teknologi Indonesia adalah suatu perusahaan *start-up* yang sedang berkembang pesat saat ini. Produk yang telah dibuat sampai saat ini diantaranya: *marketplace*, aplikasi pembelajaran, dan *try-out*. Beberapa perusahaan maupun instansi pemerintahan yang sudah menjalin kerjasama (MoU) dan sampai dalam kesepakatan (MoA) dengan PT. Bungkus Teknologi Indonesia. PT. Bungkus Teknologi Indonesia menyimpan surat perjanjian tersebut menjadi arsip elektronik atau disebut juga dengan dokumen digital. Dokumen digital ini bersifat rahasia dan hanya dapat di kelola oleh Direktur dari PT. Bungkus Teknologi Indonesia. Oleh karena itu pihak PT. Bungkus Teknologi Indonesia berusaha untuk melakukan pengamanan

pada dokumen digital tersebut, supaya terhindar dari penyalahgunaan dan manipulasi data oleh pihak yang tidak berkepentingan.

Sedangkan model pengaman data atau dokumen digital pada MoA yang diterapkan oleh PT. Bungkus Teknologi Indonesia masih secara manual, yaitu dengan mengganti nama atau ekstensi dari dokumen tersebut. maka dari itu diperlukan sebuah sistem keamanan untuk mengamankan data digital MoA menggunakan Algoritma RSA.

2. KAJIAN PUSTAKA

2.1. MoU dan MoA

MoU (*Memorandum of Understanding*) atau yang sering di sebut juga nota kesepahaman adalah suatu dokumen legal dimana isinya menjelaskan mengenai perjanjian pendahuluan antara dua belah pihak dan merupakan dasar dalam menyusun kontrak di masa mendatang yang didasarkan pada hasil permufakatan para pihak, baik secara tulisan maupun lisan [1] [2].

MoA adalah bentuk tertulis dari para pihak untuk sepakat (bukan hanya sepaham) dalam melakukan atau tidak melakukan sesuatu, MoA itu sendiri adalah bentuk lanjutan setelah adanya MoU. Disini tahapannya sudah sampai dalam ikatan saling menyepakati satu sama lain. Sehingga apabila kesepakatan dibatalkan secara sepihak maka terdapat sanksi denda maupun tuntutan pidana. Oleh karena itu dalam teknis penyusunan MoA berisi hal-hal secara terperinci yaitu objek perjanjian, harga, cara pembayaran, jangka waktu, sanksi-sanksi, domisili hukum dan lain sebagainya.

2.2. Kriptografi

Sistem Pendukung Keputusan merupakan suatu sistem yang dirancang dengan memanfaatkan komputer dalam proses pengambilan satu keputusan [3]. Menurut Raymond McLeod Jr, Sistem Pendukung Keputusan merupakan sistem informasi yang dirancang dengan tujuan untuk membantu manajemen dalam pemecahan masalah yang sedang dihadapi [4].

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Menurut Rinaldi Munir [5], kriptografi di definisikan sebagai teknik matematika yang berhubungan dengan aspek-aspek pada keamanan informasi, misalnya kerahasiaan, integritas data, otentikasi pengirim/penerima data dan otentikasi data.

2.3. Proses Enkripsi dan Dekripsi RSA

Dalam proses enkripsi dan dekripsi ini, RSA memiliki besaran-besaran yang umum digunakan. Besaran-besaran tersebut sebagai berikut:

p dan q bilangan prima	(rahasia)
$n = p \cdot q$	(tidak rahasia)
$\phi(n) = (p-1) \times (q-1)$	(rahasia)
e (kunci enkripsi)	(tidak rahasia)
d (kunci dekripsi)	(rahasia)
m (plainteks) atau m_{ij} (blok plainteks)	(rahasia)
c (cipherteks) atau c_{ij} (blok cipherteks)	(tidak rahasia)

Berikut merupakan langkah-langkah pembangkitan kunci algoritma RSA :

1. Pilih dua bilangan prima sembarang, p dan q .
2. Hitung $n = p \cdot q$ (sebaiknya $p \neq q$, sebab jika $p = q$, maka $n = p^2$ sehingga p dapat diperoleh dengan menarik akar pangkat dua dari n).
3. Hitung $\phi(n) = (p-1)(q-1)$.
4. Pilih sebuah bilangan bulat acak untuk kunci publik, sebut namanya e , yang relatif prima terhadap $\phi(n)$ atau ($\text{gcd}(e, \phi(n)) = 1$).
5. Bangkitkan kunci privat dengan menggunakan persamaan:

$$e \cdot d = 1 \pmod{\phi(n)}$$
yang ekuivalen dengan

$$d = \frac{1 \pmod{\phi(n)}}{e}$$
atau dapat juga ditulis dalam bentuk kesamaan:

$$d = \frac{1 + k \cdot \phi(n)}{e}$$

Hasil dari algoritma diatas adalah:

1. Kunci *public* atau enkripsi adalah pasangan (e, n)
2. Kunci *private* atau dekripsi adalah pasangan (d, n)

Proses enkripsi dilakukan dari persamaan yang telah di dapatkan :

$$c_{ij} = m_{ij}^e \text{ mod } n$$

Proses dekripsi dilakukan sebagai berikut :

$$m_{ij} = c_{ij}^d \text{ mod } n$$

3. METODOLOGI PENELITIAN

3.1. Teknik Pengumpulan Data (*Data Collecting*)

Beberapa teknik yang dilakukan dalam penelitian ini adalah sebagai berikut:

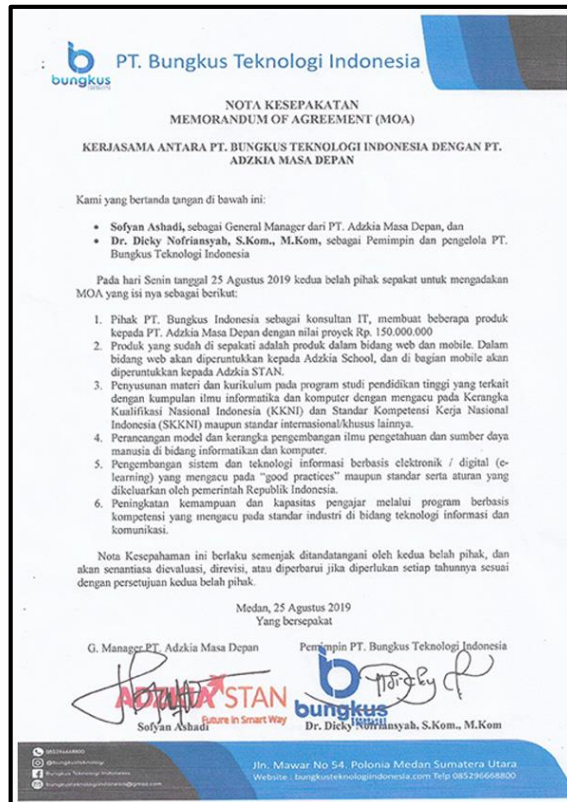
1. Observasi

Studi observasi merupakan teknik pengumpulan data secara langsung di tempat kejadian secara sistematis kejadian-kejadian, perilaku, objek-objek yang dilihat, dan hal-hal lain yang diperlukan dalam mendukung penelitian yang sedang berlangsung. Dalam penelitian ini, objek yang diamati adalah keamanan data pada dokumen MoA.

2. Wawancara

Teknik wawancara ini dilakukan untuk mendapatkan dan menggali informasi tambahan dari pihak-pihak yang memiliki wewenang dan berinteraksi langsung dengan sistem yang akan dirancang sebagai sumber data.

3.2. Dekripsi Data Dari Penelitian



Gambar 3.1 Data digital MoA

Gambar diatas merupakan data atau citra yang akan di amankan. Citra ini mempunyai format *.JPG dan *.JPEG, dengan ukuran 595 x 842 pixel. Dalam dunia komputasi citra terdiri dari piksel-piksel dimana nilai piksel menunjukkan warna citra. Citra digital tersusun dari sejumlah nilai tingkat keabuan yaitu piksel

pada posisi tertentu. Piksel adalah elemen terkecil dari sebuah citra digital. Warna adalah intensitas cahaya yang dipantulkan oleh obyek.

3.3. Penyelesaian Masalah Dengan Menggunakan Metode RSA

Sesuai dengan referensi yang telah dipaparkan pada bab sebelumnya, berikut ini adalah langkah-langkah penyelesaiannya yaitu:

1. Proses Pembangkitan Kunci

Proses pembangkitan kunci RSA dilakukan dengan langkah-langkah berikut.

Langkah 1 : Untuk proses pembangkitan kunci terlebih dahulu ditentukan bilangan acak prima p dan q , dimana $p = 1583$ dan $q = 1863$.

Langkah 2 : $n = p * q$
 $n = 1583 * 1861$
 $n = 2945963$

Langkah 3 : $\phi(n) = (p - 1) \times (q - 1)$
 $\phi(2945963) = (1583 - 1) \times (1861 - 1)$
 $\phi(2945963) = 1582 \times 1860$
 $\phi(2945963) = 2942520$

Langkah 4 : Memilih kunci $e = 11$, karena 11 relatif prima dengan 2945963.

Langkah 5 : Menghitung kunci d dari rumus $d = (1 + k \cdot \phi(n)) / e$; $k = 1, 2, 3, \dots$

$k=1$; $d = (1 + 1 \cdot 2942520) / 11 = 267501,91$ tidak bulat

$k=2$; $d = (1 + 2 \cdot 2942520) / 11 = 535003,73$ tidak bulat

$k=3$; $d = (1 + 3 \cdot 2942520) / 11 = 802505,55$ tidak bulat

$k=4$; $d = (1 + 4 \cdot 2942520) / 11 = 1070007,36$ tidak bulat

$k=5$; $d = (1 + 5 \cdot 2942520) / 11 = 1337509,18$ tidak bulat

$k=6$; $d = (1 + 6 \cdot 2942520) / 11 = 1605011,00$ bulat

Nilai $d = 1605011$.

Jadi perhitungan ini menghasilkan pasangan kunci *private* dan kunci *public*:

Kunci *public* : ($e = 11, n = 2945963$)

Kunci *private* : ($d = 1605011$)

2. Proses Enkripsi

Input yang dimasukkan berupa citra RGB, lalu direpresentasikan dalam bentuk matriks sesuai dengan ukuran piksel dari citra tersebut. Matriks nilai piksel dari citra diatas adalah sebagai berikut :

$$m = \begin{pmatrix} 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \end{pmatrix}$$

Matriks m diatas merupakan matriks dari citra RGB yang dikurangi elemennya. Plainteks asli berukuran 595 x 842. Setelah itu, nilai dari RGB nya akan di pecah sesuai dengan nilai masing mR , mG , dan mB . Setelah mendapatkan nilai dari masing-masing mR , mG , dan mB , maka akan di pecah lagi menjadi blok-blok yang lebih kecil, blok tersebut akan mempunyai panjang 6 digit angka.

$$\begin{array}{llll}
 mR_{11} = 250250; & mR_{12} = 250250; & mR_{13} = 250250; & mR_{14} = 250250; \\
 mR_{21} = 250250; & mR_{22} = 250250; & mR_{23} = 250250; & mR_{24} = 250250; \\
 mR_{31} = 250250; & mR_{32} = 250250; & mR_{33} = 250250; & mR_{34} = 250250; \\
 mR_{41} = 250250; & mR_{42} = 250250; & mR_{43} = 250250; & mR_{44} = 250250; \\
 mR_{51} = 250250; & mR_{52} = 250250; & mR_{53} = 250250; & mR_{54} = 250250; \\
 mG_{11} = 251251; & mG_{12} = 251251; & mG_{13} = 251251; & mG_{14} = 251251; \\
 mG_{21} = 251251; & mG_{22} = 251251; & mG_{23} = 251251; & mG_{24} = 251251; \\
 mG_{31} = 251251; & mG_{32} = 251251; & mG_{33} = 251251; & mG_{34} = 251251; \\
 mG_{41} = 251251; & mG_{42} = 251251; & mG_{43} = 251251; & mG_{44} = 251251; \\
 mG_{51} = 251251; & mG_{52} = 251251; & mG_{53} = 251251; & mG_{54} = 251251; \\
 mB_{11} = 253253; & mB_{12} = 253253; & mB_{13} = 253253; & mB_{14} = 253253; \\
 mB_{21} = 253253; & mB_{22} = 253253; & mB_{23} = 253253; & mB_{24} = 253253; \\
 mB_{31} = 253253; & mB_{32} = 253253; & mB_{33} = 253253; & mB_{34} = 253253; \\
 mB_{41} = 253253; & mB_{42} = 253253; & mB_{43} = 253253; & mB_{44} = 253253; \\
 mB_{51} = 253253; & mB_{52} = 253253; & mB_{53} = 253253; & mB_{54} = 253253;
 \end{array}$$

Nilai-nilai blok dari setiap mR , mG , dan mB masih terletak di dalam selang $[0, 2945963 - 1]$ agar transformasi menjadi satu-ke-satu.

Setelah itu melakukan proses enkripsi setiap blok mR , mG , dan mB dengan rumus $c_{ij} = m_{ij}^e \bmod n$.

$$\begin{array}{l}
 cR_{11} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{12} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{13} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{14} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{21} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{22} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{23} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{24} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{31} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{32} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{33} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{34} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{41} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{42} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{43} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{44} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{51} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{52} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{53} = 250250^{11} \bmod 2945963 = 78313; \\
 cR_{54} = 250250^{11} \bmod 2945963 = 78313; \\
 cG_{11} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{12} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{13} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{14} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{21} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{22} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{23} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{24} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{31} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{32} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{33} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{34} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{41} = 251251^{11} \bmod 2945963 = 2167563; \\
 cG_{42} = 251251^{11} \bmod 2945963 = 2167563;
 \end{array}$$

$mR_{43} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mR_{44} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mR_{51} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mR_{52} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mR_{53} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mR_{54} = 0078313^{1605011} \bmod 2945963 = 250250$
 $mG_{11} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{12} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{13} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{14} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{11} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{22} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{23} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{24} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{31} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{32} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{33} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{34} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{41} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{42} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{43} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{44} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{51} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{52} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{53} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mG_{54} = 2167563^{1605011} \bmod 2945963 = 251251$
 $mB_{11} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{12} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{13} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{14} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{21} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{22} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{23} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{24} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{31} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{31} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{31} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{31} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{41} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{42} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{43} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{44} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{51} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{52} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{53} = 1226304^{1605011} \bmod 2945963 = 253253$
 $mB_{54} = 1226304^{1605011} \bmod 2945963 = 253253$

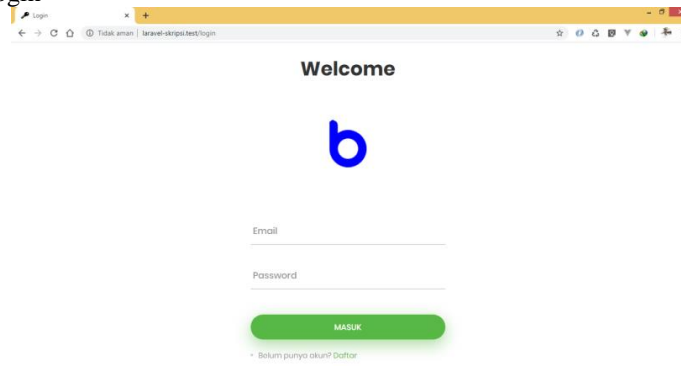
Setelah proses dekripsi berhasil, maka plainteks akan dipecah menjadi blok sepanjang 3 digit angka.

$$m = \begin{pmatrix} 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\ \\ 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\ 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\ 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \end{pmatrix}$$

4. IMPLEMENTASI

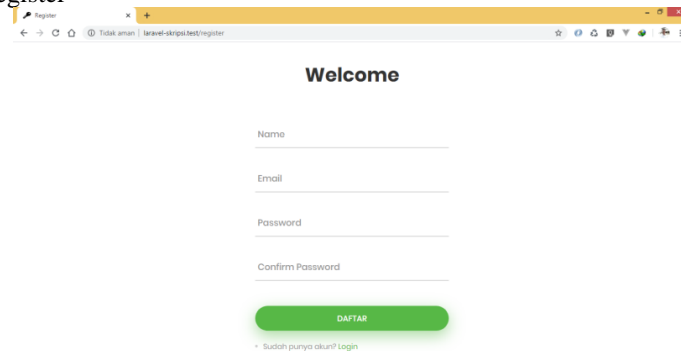
berikut adalah tampilan form dari sistem security untuk mengamankan data MoA yang telah dibangun:

Tampilan Halaman Login



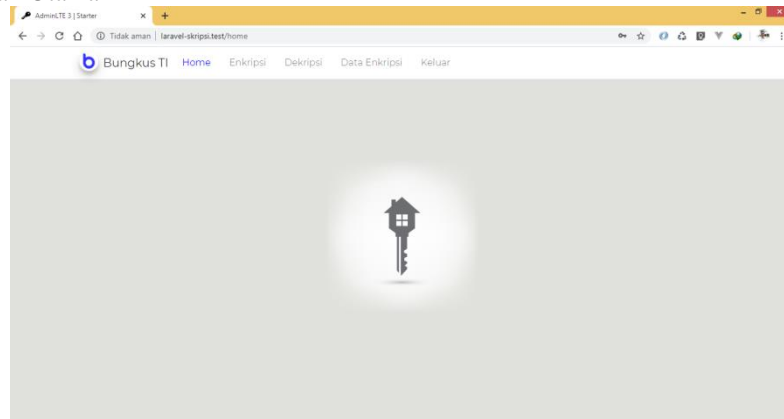
Gambar 4.1 Tampilan Halaman *Login*

Tampilan Halaman Register



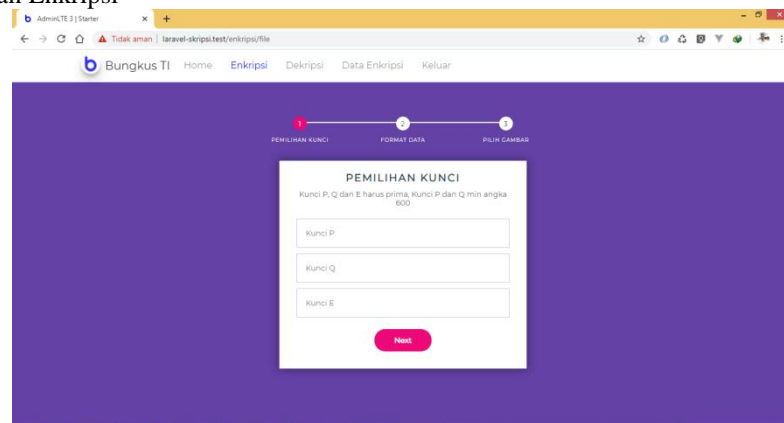
Gambar 4.2 Tampilan Halaman *Register*

Tampilan Halaman Utama



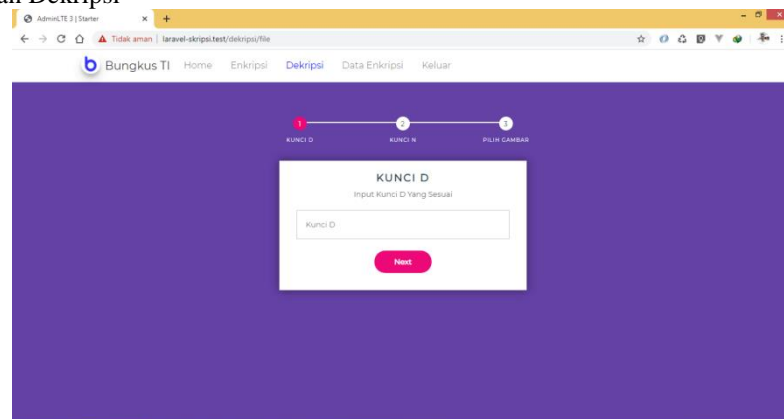
Gambar 4.3 Tampilan Halaman Utama

Tampilan Halaman Enkripsi



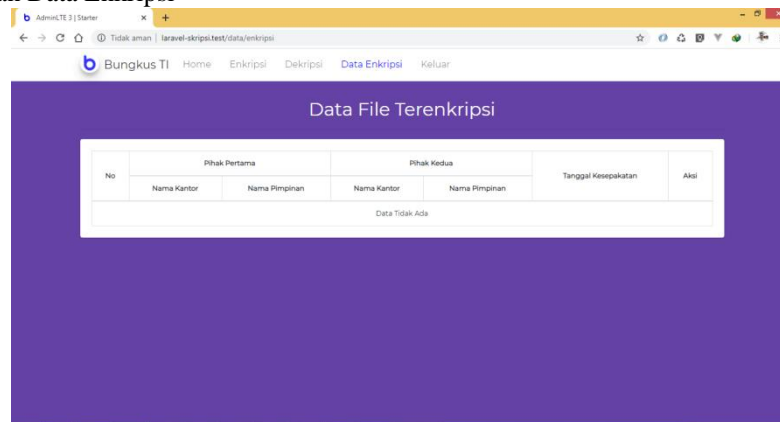
Gambar 4.4 Tampilan Halaman Enkripsi

Tampilan Halaman Dekripsi



Gambar 4.5 Tampilan Halaman Dekripsi

Tampilan Halaman Data Enkripsi



4. KESIMPULAN

Berdasarkan pengujian dan implementasi, pengaruh penerapan sistem keamanan data terhadap penyelesaian masalah pada PT. Bungkus Teknologi Indonesia dalam mengamankan data MoA terlihat sangat baik, hal ini di tandai dengan kemudahan dalam melakukan proses pengaman data tersebut.

Dengan algoritma RSA pemecahan masalah dalam mengamankan data MoA berhasil diterapkan. Beberapa masalah dalam mengamankan data MoA sebelum menggunakan sistem berhasil dipecahkan setelah dibangunnya sistem keamanan data ini, salah satunya adalah waktu yang cepat, hasil yang cukup akurat, proses yang lebih singkat.

UCAPAN TERIMA KASIH

Pada kesempatan ini penulis mengucapkan banyak terimakasih kepada Kedua Orang Tua yang telah banyak memberikan dukungan moril dan materil, tidak terkecuali doa yang senantiasa dipanjatkan sehingga penulis dapat menyelesaikan penelitian ini.

Penyusunan skripsi ini juga tidak terlepas dari bantuan berbagai pihak. Oleh karena itu dengan segala kerendahan hati, diucapkan terimakasih yang sebesar-besarnya kepada; Bapak Azanuddin, S.Kom., M.Kom selaku Dosen Pembimbing I. Kepada Ibu Ita Mariami, SE., Msi selaku Dosen Pembimbing II yang telah banyak membantu dalam memberikan arahan dan bimbingan.

REFERENSI

- [1] A. Society, I. Law, A. Society, I. Law, T. A. Journal, And I. Law, "International Agreements : Recent U . S . -Uk Practice Concerning The Memorandum Of Understanding Author (S): John H . Mcneill Source : The American Journal Of International Law , Vol . 88 , No . 4 (Oct . , 1994), Pp . 821-826," Vol. 88, No. 4, Pp. 821–826, 2015.
- [2] G. N. Pratama, "Kekuatan Hukum Memorandum Of Understanding (Mou) Dalam Hukum Perjanjian Di Indonesia," Vol. 2, Pp. 424–441.
- [3] A. Shofian And M. Anif, "Aplikasi Kriptografi Video Menggunakan Algoritma C-54," Vol. 7, Pp. 53–58, 2015.
- [4] D. P. Pahrizal, "Implementasi Algoritma," Vol. Iii, Pp. 44–49, 2016.
- [5] R. Munir, *Kriptografi*, 2nd Ed. Informatika Bandung, 2019.

BILIOGRAFI PENULIS

	<p>Rianto Pangihutan Pangaribuan, Laki-laki kelahiran, Medan 10 Maret 1997. Anak ke pertama dari 3 bersaudara, dan merupakan seorang mahasiswa STMIK Triguna Dharma, Medan. Saat ini sedang dalam proses menyelesaikan skripsi.</p>
	<p>Azanuddin, S.Kom., M.Kom, Dosen tetap di STMIK Triguna Dharma program studi Sisten Informasi.</p>
	<p>Ita Mariami, SE., Msi, Dosen tetap di STMIK Triguna Dharma program studi Sisten Informasi.</p>