

## Implementasi Algoritma Rivest Shamir Adleman Untuk Pengamanan Akta Pendirian Perusahaan

Rahmat Hassuna \*, Nurcahyo Budi Nugroho \*\*, Rico Imanta Ginting\*\*

\*Program Studi Mahasiswa, STMIK Triguna Dharma

\*\*Program Studi Dosen Pembimbing, STMIK Triguna Dharma

---

### Article Info

#### Article history:

Received Mei 12<sup>th</sup>, 2018

Revised Mei 20<sup>th</sup>, 2018

Accepted Mei 26<sup>th</sup>, 2018

---

#### Keyword:

Pengamanan,  
Kriptografi,  
Algoritma Rivest Shamir  
Adleman

---

### ABSTRACT

PT. Bungkus Teknologi Indonesia menyimpan dokumen penting, seperti akta pendirian perusahaan, 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. 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. Perancangan sistem Pengamanan Akta Pendirian Perusahaan PT. Bungkus Teknologi dan bentuk pengamannya dengan menggunakan algoritma Rivest Shamir Adleman.

Copyright © 2018 STMIK Triguna Dharma.  
All rights reserved.

---

#### First Author

Nama : Rahmat Hassuna  
Kampus : STMIK Triguna Dharma  
Program Studi : Sistem Informasi  
E-Mail : rahmathassuna@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. PT. Bungkus Teknologi Indonesia menyimpan dokumen penting, seperti akta pendirian perusahaan, menjadi arsip elektronik atau disebut juga dengan dokumen digital. Dokumen digital ini bersifat rahasia dan hanyadapat 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. Salah satu teknik pengamanan yang digunakan adalah kriptografi, yakni dengan menyandikan data, dalam hal ini dokumen digital, dengan menggunakan algoritma tertentu agar kemudian data tersebut berubah menjadi kode – kode yang tidak dapat dimengerti sehingga menjadi sulit dibaca jika tidak memiliki kunci untuk mendekripsinya.

Perkembangan dunia bisnis saat ini semakin hari semakin berkembang pesat. Tak pelak para pengusaha membutuhkan suatu wadah agar dapat bertindak terlebih dalam hal transaksi bisnis. Namun begitu, seyogyanya para pengusaha tetaplah mematuhi peraturan hukum. Saat seorang pengusaha ingin memulai sebuah bisnis, pengusaha tersebut pastinya harus memiliki sebuah izin atas pendirian sebuah usaha bisnis, terlebih jika yang dibangun adalah perusahaan yang besar. Akta pendirian perusahaan merupakan satu bukti yang sah di mata hukum dalam hal pengesahan perusahaan dan juga merupakan sebuah bukti lembaran tertulis berisikan keterangan terkait pendirian sebuah perusahaan dan lain sebagainya yang kemudian ditandatangani oleh pejabat terkait untuk mengesahkannya[1].

Salah satu dari algoritma kriptografi yang digunakan adalah RSA (Rivest Shamir Adleman). Algoritma ini dirancang oleh Ron Rivest, Adi Shamir, dan Len Adleman pada tahun 1977. Algoritma RSA termasuk algoritma kriptografi asimetris dimana algoritma ini menggunakan dua kunci, yaitu kunci publik dan kunci privat yang

masing-masing kunci tersebut digunakan untuk mengenkripsi data dan mendekripsi data yang telah dienkripsi[2] [3] [4].

Berdasarkan latar belakang permasalahan di atas, maka dari itu diangkat judul “Implementasi Algoritma Rivest Shamir Adleman Untuk Pengamanan Akta Pendirian Perusahaan Pada PT. Bungkus Teknologi Indonesia”. Sehingga data akta pendirian perusahaan yang bersifat rahasia tersebut dapat diamankan dan tidak takut dalam penyalahgunaan.

## 2. KAJIAN PUSTAKA

### 2.1 Akta Pendirian Perusahaan

Akta pendirian perusahaan adalah bukti otentik yang mengesahkan sebuah perusahaan di mata hukum Indonesia. Hal ini penting dimiliki oleh setiap badan usaha terutama yang berskala besar, seperti PT (Perseroan Terbatas). Dokumen tersebut berisikan identitas para pendiri lengkap dengan foto dan alamat, kesepakatan yang terjadi ketika mendirikan perusahaan tersebut, serta anggaran dasar yang dipakai sebagai modal awal.

Tujuan ke depan perusahaan yang harus dicapai juga diikutsertakan dalam akta pendirian. Agar, ketika ada satu masalah menghadang atau tujuan sudah melenceng jauh dari niat awal didirikannya usaha tersebut, maka para pendiri bisa melihat kembali akta untuk fokus pada tujuan awal. Semua yang tercatat dalam akta harus disahkan oleh Kementerian Hukum dan HAM agar memperoleh status badan hukum. Sehingga dapat dipakai untuk melakukan transaksi dengan semua pihak nantinya. Baik lembaga pemerintahan maupun lembaga swasta berskala besar yang memiliki badan hukum sah[1].

### 2.2 Kriptografi

Dalam bahasa Yunani kriptografi terdiri dari dua suku kata, yaitu *cryptos* yang artinya rahasia atau tersembunyi, dan *graphein* yang artinya tulisan[5]. Yang dapat diartikan secara harafiah sebagai tulisan yang bersifat rahasia. Secara umum juga kriptografi dapat diartikan sebagai seni dan ilmu di dalam proses pengamanan pesan atau data.

Menurut terminologinya, kriptografi adalah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat yang lain. Menurut Rinaldi Munir[6], 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.

Dalam perkembangannya, ilmu kriptografi terbagi ke dalam dua periode, yaitu periode kriptografi klasik dan periode kriptografi modern. Pada periode kriptografi klasik, Julius Caesar sudah menggunakan teknik sederhana di dalam perang *Galic*. Teknik lainnya pada periode ini diantara lain *Polybius square*. Pada periode kriptografi modern hanya dipergunakan oleh pemerintahan untuk keperluan militer.[7]

### 2.3 Citra JPEG

JPG atau JPEG yang merupakan kepanjangan dari *Joint Photographic Experts Group* adalah metode standar yang digunakan dalam pengkompresian untuk *photographic images*. Format *file* ini mampu mengompres objek dengan tingkat kualitas sesuai dengan pilihan yang disediakan. Format *file* ini sering dimanfaatkan untuk menyimpan gambar yang akan digunakan untuk keperluan halaman *web*, multimedia, dan publikasi elektronik lainnya. Format *file* ini mampu menyimpan gambar dengan mode warna RGB, CMYK, dan Grayscale. Pada citra 256 warna setiap piksel panjangnya 8 bit, tetapi komponen warna RGB-nya disimpan di dalam tabel RGB yang disebut *pallette*. Setiap komponen panjangnya 8 bit, jadi ada 256 nilai keabuan untuk warna merah, 256 nilai keabuan untuk warna hijau, 256 nilai keabuan untuk warna biru.

### 2.4 Algoritma Rivest Shamir Adleman

Algoritma RSA adalah algoritma kriptografi asimetris yang paling populer hingga saat ini. Algoritma ini memiliki dua kunci yang berbeda, yaitu kunci *public* untuk melakukan proses enkripsi dan kunci *private* untuk melakukan proses dekripsi. Kunci *public* dalam proses enkripsi dapat diketahui oleh siapa saja (bersifat tidak rahasia), berbeda dengan kunci *private* yang sifatnya sangat rahasia. Kerja algoritma RSA didasarkan oleh konsep bilangan prima dan aritmatika modulo.

#### 2.4.1 Proses Enkripsi dan Dekripsi RSA

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

1.  $p$  dan  $q$  bilangan prima (rahasia)
2.  $n = p \cdot q$  (tidak rahasia)
3.  $\phi(n) = (p-1) \times (q-1)$  (rahasia)
4.  $e$  (kunci enkripsi) (tidak rahasia)

- |    |  |                 |
|----|--|-----------------|
| 5. | $d$ (kunci dekripsi)                             | (rahasia)       |
| 6. | $m$ (plainteks) atau $m_{ij}$ (blok plainteks)   | (rahasia)       |
| 7. | $c$ (cipherteks) atau $c_{ij}$ (blok cipherteks) | (tidak rahasia) |

Berikut merupakan langkah-langkah pembangkitan kunci algoritma RSA :

- Pilih dua bilangan prima sembarang,  $p$  dan  $q$ .
- 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  $n$ ).
- Hitung  $\phi(n) = (p-1)(q-1)$ .
- Pilih sebuah bilangan bulat acak untuk kunci publik, sebut namanya  $e$ , yang relatif prima terhadap  $\phi(n)$  atau ( $\text{gcd}(e, \phi(n)) = 1$ ).
- 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:

- Kunci *public* atau enkripsi adalah pasangan ( $e, n$ )
- Kunci *private* atau dekripsi adalah pasangan ( $d, n$ )

Proses enkripsi dilakukan dari persamaan yang telah di dapatkan :

$$c_{ij} = m_{ij}^e \pmod{n}$$

Proses dekripsi dilakukan sebagai berikut :

$$m_{ij} = c_{ij}^d \pmod{n}$$

### 3. METODOLOGI PENELITIAN

#### 3.1 Teknik Pengumpulan Data (Data Collecting)

Beberapa teknik yang dilakukan dalam penelitian ini adalah sebagai berikut :

- 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 Akta Pendirian Perusahaan.
- 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.

Berikut ini adalah penerapan algoritma RSA (Rivest Shamir Adleman) untuk pengamanan Akta Pendirian Perusahaan pada PT. Bungkus Teknologi Indonesia dengan perhitungan dapat dilihat pada contoh dibawah ini :

- 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  $q = 1861$ .  
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  $m_R$ ,  $m_G$ , dan  $m_B$ .

$$m_R = \begin{pmatrix}
 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\
 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\
 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\
 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250 \\
 250 & 250 & 250 & 250 & 250 & 250 & 250 & 250
 \end{pmatrix}$$

$$m_G = \begin{pmatrix}
 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\
 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\
 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\
 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251 \\
 251 & 251 & 251 & 251 & 251 & 251 & 251 & 251
 \end{pmatrix}$$

$$m_B = \begin{pmatrix}
 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\
 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\
 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\
 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253 \\
 253 & 253 & 253 & 253 & 253 & 253 & 253 & 253
 \end{pmatrix}$$

Setelah mendapatkan nilai dari masing-masing  $m_R$ ,  $m_G$ , dan  $m_B$ , maka akan di pecah lagi menjadi blok-blok yang lebih kecil, blok tersebut akan mempunyai panjang 6 digit angka.

$mR_{11} = 250250; mR_{12} = 250250; mR_{13} = 250250; mR_{14} = 250250;$   
 $mR_{21} = 250250; mR_{22} = 250250; mR_{23} = 250250; mR_{24} = 250250;$   
 $mR_{31} = 250250; mR_{32} = 250250; mR_{33} = 250250; mR_{34} = 250250;$

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

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

$$c_{ij} = m_{ij}^e \bmod n$$

$cR_{11} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{12} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{13} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{14} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{21} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{22} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{23} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{24} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{31} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{32} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{33} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{34} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{41} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{42} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{43} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{44} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{51} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{52} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{53} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cR_{54} = 250250^{11} \bmod 2945963 = 78313$ ;  
 $cG_{11} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{12} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{13} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{14} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{21} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{22} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{23} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{24} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{31} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{32} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{33} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{34} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{41} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{42} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{43} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{44} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{51} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{52} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{53} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cG_{54} = 251251^{11} \bmod 2945963 = 2167563$ ;  
 $cB_{11} = 253253^{11} \bmod 2945963 = 1226304$ ;

$$\begin{aligned}
cB_{12} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{13} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{14} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{21} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{22} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{23} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{24} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{31} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{32} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{33} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{34} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{41} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{42} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{43} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{44} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{51} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{52} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{53} &= 253253^{11} \bmod 2945963 = 1226304; \\
cB_{54} &= 253253^{11} \bmod 2945963 = 1226304;
\end{aligned}$$

Setelah semua proses perhitungan selesai, maka blok cipherteks di satukan kembali sesuai dengan R, G dan B sehingga menghasilkan:

$$C = \begin{pmatrix}
78313 & 78313 & 78313 & 78313 \\
78313 & 78313 & 78313 & 78313 \\
78313 & 78313 & 78313 & 78313 \\
78313 & 78313 & 78313 & 78313 \\
78313 & 78313 & 78313 & 78313 \\
2167563 & 2167563 & 2167563 & 2167563 \\
2167563 & 2167563 & 2167563 & 2167563 \\
2167563 & 2167563 & 2167563 & 2167563 \\
2167563 & 2167563 & 2167563 & 2167563 \\
2167563 & 2167563 & 2167563 & 2167563 \\
1226304 & 1226304 & 1226304 & 1226304 \\
1226304 & 1226304 & 1226304 & 1226304 \\
1226304 & 1226304 & 1226304 & 1226304 \\
1226304 & 1226304 & 1226304 & 1226304 \\
1226304 & 1226304 & 1226304 & 1226304
\end{pmatrix}$$

### 3. Proses Dekripsi

Untuk melakukan proses dekripsi dibutuhkan kunci  $d$ , dan  $n$ . Dimana kunci  $d = 1605011$  dan kunci  $n = 2945963$  di dapat dari proses pembangkit kunci. Rumus untuk melakukan proses dekripsi adalah  $m_{ij} = c_{ij}^d \bmod n$ .

$$\begin{aligned}
mR_{11} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{12} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{13} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{14} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{21} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{22} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{23} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{24} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{31} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{32} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{33} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{34} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{41} &= 78313^{1605011} \bmod 2945963 = 250250 \\
mR_{42} &= 78313^{1605011} \bmod 2945963 = 250250
\end{aligned}$$

$$\begin{aligned} mR_{43} &= 78313^{1605011} \bmod 2945963 = 250250 \\ mR_{44} &= 78313^{1605011} \bmod 2945963 = 250250 \\ mR_{51} &= 78313^{1605011} \bmod 2945963 = 250250 \\ mR_{52} &= 78313^{1605011} \bmod 2945963 = 250250 \\ mR_{53} &= 78313^{1605011} \bmod 2945963 = 250250 \\ mR_{54} &= 78313^{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 \end{aligned}$$

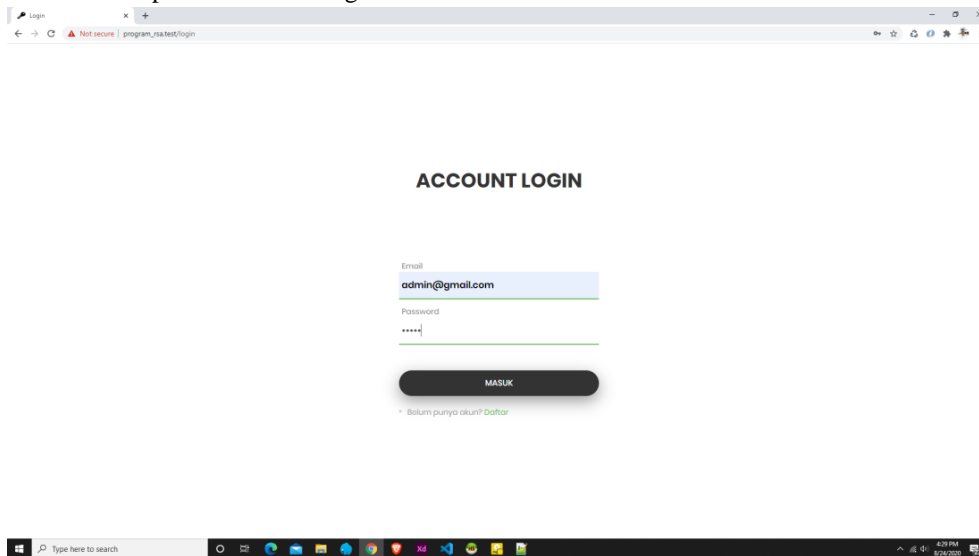
Setelah proses dekripsi berhasil, maka plainteks akan dipecah menjadi blok sepanjang 3 digit angka.

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

### 3.2 Hasil

#### 1. Tampilan Halaman Login

Sebelum masuk ke Menu Utama, pengguna diwajibkan untuk login terlebih dahulu pada halaman Login. Berikut adalah tampilan Halaman Login.



Gambar 1 Tampilan Halaman Login

#### 2. Tampilan Halaman Menu Utama

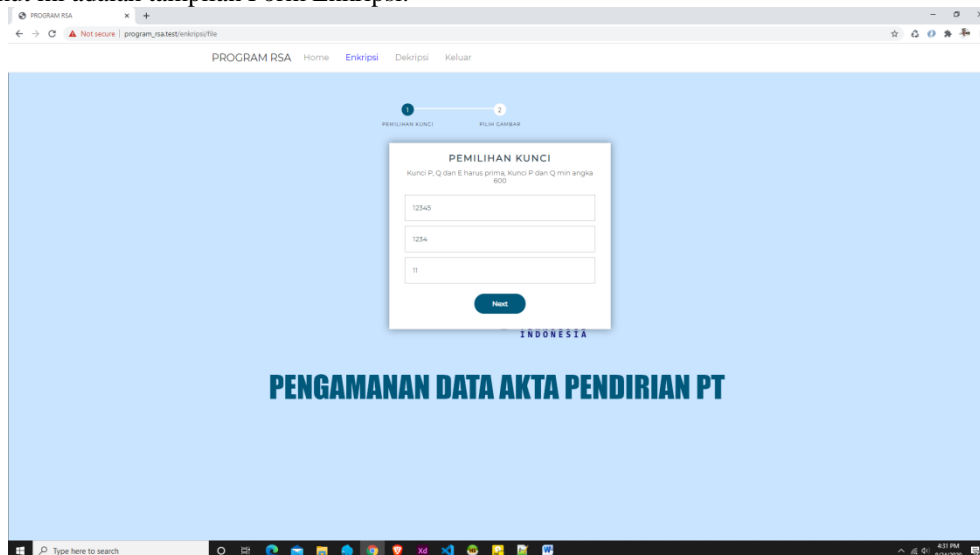
Berikut ini adalah tampilan Halaman Menu Utama.





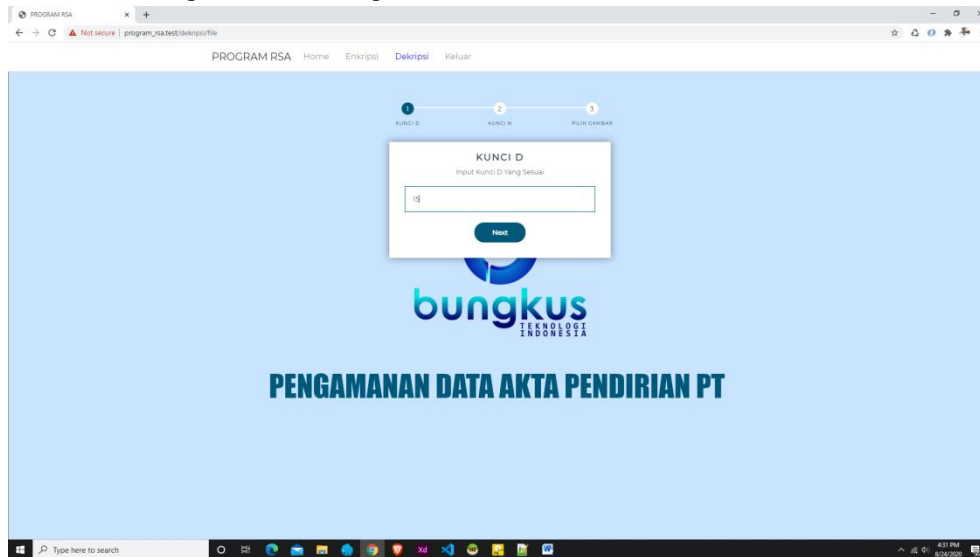
*Gambar 2 Tampilan Halaman Utama*

3. Tampilan Form Enkripsi  
Berikut ini adalah tampilan Form Enkripsi.



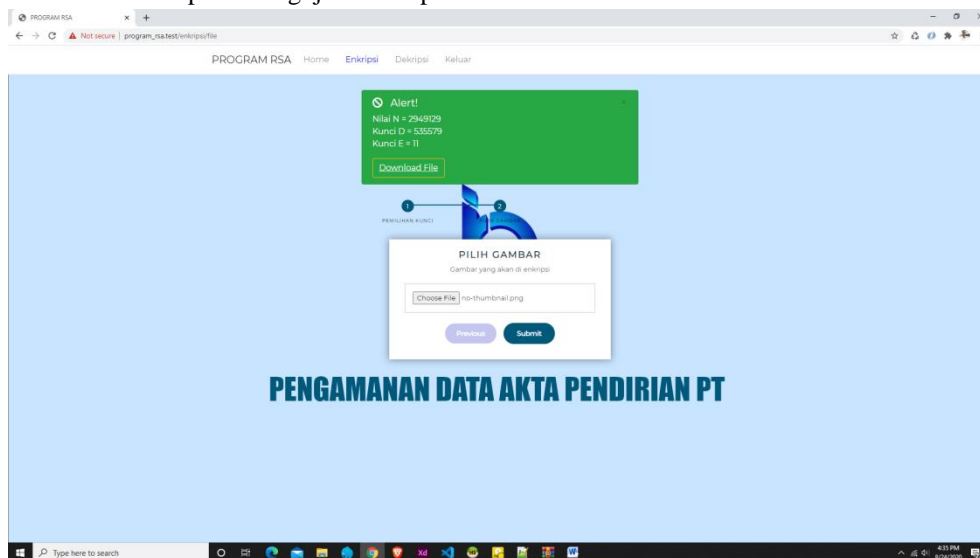
*Gambar 3 Tampilan Form Enkripsi*

4. Tampilan Form Dekripsi  
Berikut ini adalah tampilan Form Dekripsi.

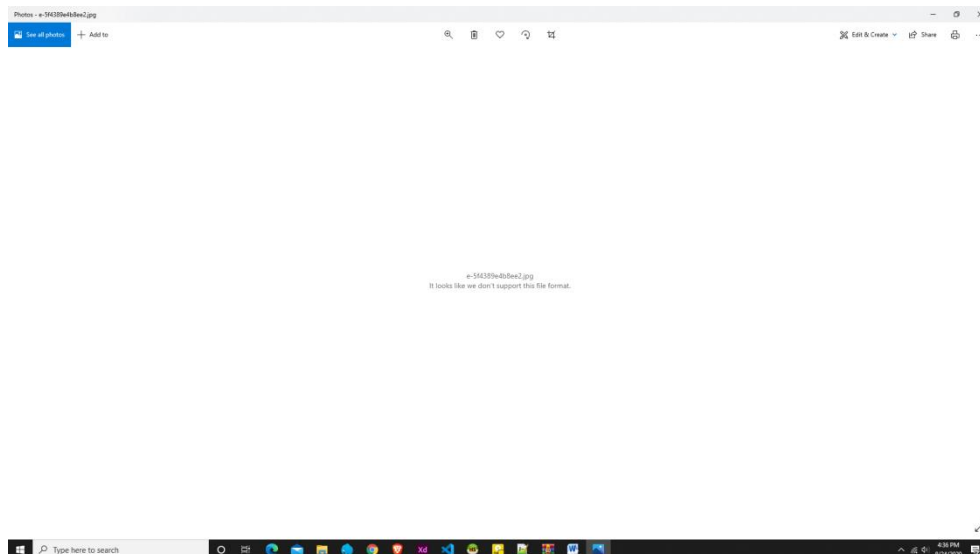


Gambar 4 Tampilan Form Dekripsi

5. Tampilan Pengujian Enkripsi  
Berikut ini adalah tampilan Pengujian Enkripsi



Gambar 5 Tampilan Pengujian Enkripsi



Gambar 6 Tampilan Pengujian Enkripsi

#### 4. KESIMPULAN

Jadi kesimpulan yang dapat disampaikan dari hasil pengamanan Akta Pendirian Perusahaan adalah sebagai berikut :

1. Berdasarkan hasil analisa, masalah yang terjadi pada PT. Bungkus Teknologi Indonesia dapat diselesaikan dengan metode RSA.
2. Berdasarkan hasil penelitian, algoritma RSA dapat diimplementasikan untuk melakukan pengamanan data, terutama Akta Pendirian Perusahaan.
3. Berdasarkan hasil penelitian, pengujian CTO pada PT. Bungkus Teknologi Indonesia menyatakan sistem ini layak digunakan dan diadopsi oleh perusahaan.




#### UCAPAN TERIMA KASIH

Saya ucapkan terima kasih kepada Ketua Yayasan STMIK Triguna Dharma, kepada Bapak Nurcahyo Budi Nugroho, S.Kom., M.Kom, selaku dosen pembimbing 1, kepada Bapak Rico Imanta Ginting, S.Kom., M.Kom, selaku dosen pembimbing 2, kepada kedua orang tua saya yang selalu memberikan dukungan dan doa kepada saya dan tidak lupa kepada teman-teman seperjuangan saya.

#### REFERENSI

- [1] "Implementasi undang-undang nomor 2 tahun 2014 tentang •," vol. 12, pp. 61–68, 2019.
- [2] M. A. Zainuddin and D. I. Mulyana, "PENERAPAN ALGORITMA RSA UNTUK KEAMANAN PESAN INSTAN PADA PERANGKAT ANDROID," vol. 9, no. 2, pp. 105–114, 2016.
- [3] F. Nuraeni, Y. H. Agustin, and I. M. Muharam, "Implementasi Tanda Tangan Digital Menggunakan RSA dan SHA-512 Pada Proses Legalisasi Ijazah," pp. 8–9, 2018.
- [4] D. Apdilah and H. Swanda, "Penerapan Kriptografi RSA Dalam Mengamankan File Teks Berbasis PHP," *J. Teknol. Inf.*, vol. 2, no. 1, p. 45, 2018, doi: 10.36294/jurti.v2i1.407.
- [5] D. Wulansari, F. A. Setyawan, and H. Susanto, "Mengukur Kecepatan Enkripsi dan Dekripsi Algoritma RSA pada Pengembangan Sistem Informasi Text Security," no. Snik, pp. 85–91, 2016.
- [6] R. Munir, *Kriptografi*, 2nd ed. Informatika Bandung, 2019.
- [7] B. Setiaji, "Analisis Dan Implementasi Algoritma Kriptografi Kunci Publik Rsa Dan Luc Untuk Penyandian Data," *Data Manaj. dan Teknol. Inf.*, vol. 16, no. 3, p. 27, 2015.
- [8] F. Aldiansyah, K. Nasution, and O. K. Sulaiman, "Trithemius Dalam Pengamanan Kompresi Teks," 2018.
- [9] S. S. Wicida, "Enkripsi Data Audio Menggunakan Metode Kriptografi Rsa," pp. 6–10, 2008.
- [10] M. Y. Simargolang, "IMPLEMENTASI KRIPTOGRAFI RSA DENGAN PHP," vol. 1, pp. 1–10, 2017.
- [11] R. Nuraini, "Desain Algorithma Operasi Perkalian Matriks Menggunakan Metode Flowchart," *J. Tek. Komput. Amik Bsi*, vol. 1, no. 1, p. 146, 2015.
- [12] F. Wongso, "Perancangan Sistem Informasi Penjualan Berbasis Java Studi Kasus Pada Toko Karya Gemilang Pekanbaru," *J. Ilm. Ekon. dan Bisnis*, vol. 12, no. 1, pp. 46–60, 2015.
- [13] M. Shalahuddin and A. . Rosa, *REKAYASA PERANGKAT LUNAK TERSTRUKTUR DAN BERORIENTASI OBJEK*. Bandung: Informatika Bandung, 2018.
- [14] Munawar, *ANALISIS PERANCANGAN SISTEM BERORIENTASI OBJEK DENGAN UML*. Bandung: Informatika Bandung, 2018.

**BIOGRAFI PENULIS**

|   |   |
|---|---|
|    | <p><b>Rahmat Hassuna</b>, kelahiran Medan, 28 Februari 1996 anak pertama dari tiga bersaudara. Anak dari Bapak Muhammad Nuh dan Ibu Yustina Wati.</p>                     |
|   | <p><b>Nurcahyo Budi Nugroho, S.Kom., M.Kom</b>, beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.</p> |
|  | <p><b>Rico Imanta Ginting, S.Kom., M.Kom</b>, beliau merupakan dosen tetap STMIK Triguna Dharma Medan dan aktif sebagai pengajar pada bidang ilmu Sistem Informasi.</p>   |