**JOIN (Jurnal Online Informatika)**
Volume 2 No. 2 | Desember 2017 : 102-109
DOI: 10.15575/join.v2i2.113

# Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android

Satriya Tri Cahya Kurniawan[1], Dedih [2], Supriyadi [3]
[1, 3]Teknik Informatika, STMIK Kharisma Karawang
[2]Sistem Informasi, STMIK Kharisma karawang
[1]13tisatriya@gmail.com
[2]dedih@stmik-kharisma.ac.id
[3]fnfcreator@stmik-kharisma.ac.id

***Abstract - Cryptography is a technique of hiding messages where the message can only be known by a particular person where the message was often referred to by this enkripsi.saat encryption has been developed one of which is a method of Rivest Shamir Adleman (RSA) that uses two keys of a public key and a private key, where the lock can be set up where the longer bits key establishment it is increasingly difficult to solved because the difficulty of factoring the two a very large number and it is considered safe although never proven safe or not, and therefore in this study will be made better security again to combine them with methods Playfair cipher in which the public key that is set is first converted or encrypted with the Playfair cipher can only be solved back with algorithms Rivest Shamir Adleman (RSA)***

***Keywords: cryptography, encryption, Rivest Shamir Adlemen (RSA), Playfair Chiper***

**Abstrak - Kriptografi merupakan suatu teknik penyembunyian pesan dimana pesan tersebut hanya dapat diketahui oleh orang tertentu dimana pesan itu sering disebut dengan enkripsi.saat ini enkripsi sudah banyak dikembangkan salah satunya adalah metode *Rivest Shamir Adleman* (RSA) yang menggunakan dua kunci yaitu kunci publik dan kunci pribadi, dimana kunci tersebut dapat diatur dimana semakin panjang bit pembentukan kunci maka semakin sukar untuk dipecahkan karena sulitnya memfaktorkan dua bilangan yang sangat besar dan itu dianggap aman meskipun tidak pernah dibuktikan aman tidaknya, maka dari itu dalam penelitian ini akan dibuat keamanan yang lebih baik lagi dengan memadukannya dengan metode *playfair chiper* dimana pada kunci publik yang diatur diubah terlebih dahulu atau di enkripsi dengan *playfair chiper* baru bisa dipecahkan kembali dengan algoritma *Rivest Shamir Adleman* (RSA).**

**Kata kunci : Kriptografi, Enkripsi, *Rivest Shamir Adlemen (RSA), Playfair Chiper***

## I. PENDAHULUAN

### A. Latar Belakang Masalah

Keamanan dan kerahasiaan data merupakan salah satu aspek yang sangat penting dalam sistem informasi pada saat ini. Salah satu usaha untuk mengamankan data diantaranya dengan menggunakan kriptografi. Berbagai macam algoritma kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data[1]. Ada beberapa teknik keamanan untuk melindungi pesan yang disimpan maupun dikirim, di antaranya adalah teknik kriptografi dan teknik steganografi. Secara umum, kriptografi merupakan teknik suatu metode dengan suatu kunci tertentu menggunakan mengolah informasi awal (*plain text*) yang tidak dapat dibaca baru *(cipher text*) suatu informasi menghasilkan enkripsi tertentu sehingga menjadi informasi awal *(plain text*) melalui tersebut dapat dikembalikan *cipher text* secara langsung sehingga orang lain tidak dapat mengenali data tersebut[2]. Adapun proses penamaannya disebut proses enkripsi. Data atau pesan yang asli sering disebut sebagai plaintext dan data yang telah dienkripsi disebut yang lebih tepat encipher[3]. Berbagai macam algoritma kriptografi dapat diimplementasikan untuk mewujudkan sistem keamanan data. Diantaranya yaitu algoritma kriptografi *Rivest Shamir Adleman* (RSA) dan *playfair chiper.*

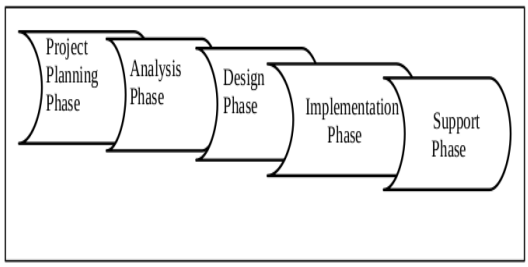
RSA adalah algoritma kriptografi asimetris. diperkenalkan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman. penamaan RSA merupakan inisial nama depan ketiga penemunya[4]. Sebagai algoritma kunci publik, RSA mempunyai dua kunci, yaitu kunci publik dan kunci pribadi. Kunci publik boleh diketahui oleh siapa saja, dan digunakan untuk proses enkripsi. Sedangkan kunci pribadi hanya pihak-pihak tertentu saja yang boleh mengetahuinya, dan digunakan untuk proses dekripsi. Tetapi agar lebih terjaga keamanannya kriptografi ini dikombinasikan dengan playfair cheper yaitu menggunakan tabel 5x5. “Semua alfabet kecuali J diletakkan ke dalam tabel. Huruf J dianggap sama dengan huruf I, sebab huruf J mempunyai frekuensi kemunculan yang paling kecil. Kunci yang digunakan berupa kata dan tidak ada huruf sama yang

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

berulang" [2]. .Maka dengan dua algoritma yang ada diharapkan dapat lebih menjaga kemaanan pesan yang dikirim maupun diterima dengan mengubah terlebih dahulu kunci publik aslinya menggunakan playfair chiper setelah itu dipecahkan kembali menggunakan algoritma *Rivest Shamir Adleman* (RSA) sehingga menjadi pesan asli.

## II. METODE PENELITIAN

Adapun metode pengembangan sistem yang digunakan adalah adalah metode SDLC *Waterfall* [5].




Gambar 1. SDLC *Waterfall* [5]

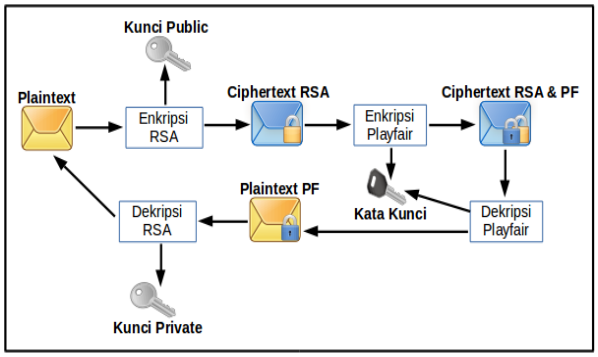
A. *Project Planning Phase*

Tahap ini dilakukan penelitian terlebih dahulu untuk mendapatkan data serta informasi yang terkait penelitian steganografi dan kriptografi. Tahap ini meliputi identifikasi masalah steganografi dan kriptografi, pengumpulan data penunjang penelitian, analisis teori, pembuatan jadwal, menentukan solusi, dan menganalisis kebutuhan sistem *(software dan hardware)*.

B. *Analysis Phase*

1. Analisis Proses

Di dalam tahapan analisis proses kriptografi digambarkan dalam bentuk skema berikut :




Gambar 2. Proses Enkripsi dan Dekripsi

2. Analisis Sistem

Tahap analisis sistem yang digunakan adalah analisis berbasis objek, yaitu:

1. Aktivitas sistem (deskripsi aktor and deskripsi use case, diagram use case, use case skenario).
2. Diagram class (definisi class, relasi class).
3. Interaksi objek ( diagram sekuen).
4. Perilaku objek (diagram aktivitas).

C. *Design Phase*

Pada fase desain menggunakan *desain berorientasi objek*, seperti :

1. Desain Proses.
2. Desain Antarmuka

D. *Implementation Phase*

Pada Tahapan implementasi melakukan langkah-langkah berikut ini :

1. Instalasi Sistem
   Melaksanakan proses instalasi aplikasi.
2. Pelatihan Prosedural
   Memberikan penjelasan bagaimana cara menggunakan aplikasi kepada pemakai.
3. Pengujian Terhadap Sistem
   a. Pengujian *white box*
   b. Pengujian *black box*

## III. HASIL DAN PEMBAHASAN

Dalam penelitian kriptografi dengan algoritme RSA dengan *playfair cipher*. Pesan teks *(Plain text)* akan dienkripsi dengan algoritme RSA menghasilkan *cipher text* dan akan dienkripsi lagi menggunakan kriptografi *playfair cipher.*

A. Hasil *Project Planning Phase*

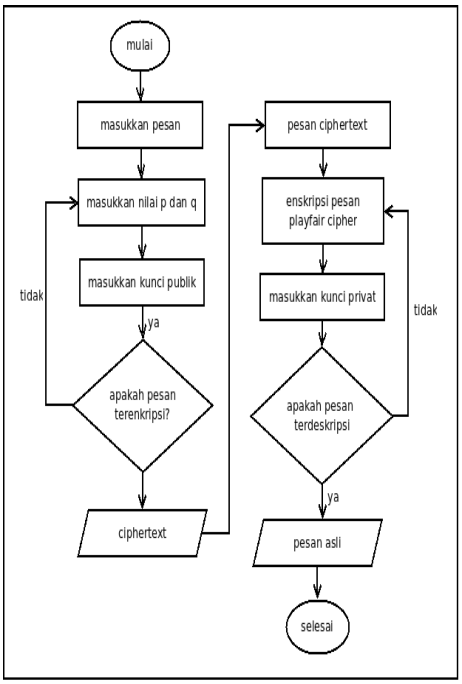
Tabel 1. Hasil *Project Planning Phase*

| No | Tahapan | Hasil |
|---|---|---|
| 1 | Identifikasi Masalah | Hasil penelitian dari identifikasi masalah yang ada sebagai berikut :<br>1.Mengubah pesan yang dikirim dan diterima dengan menggunakan kriptografi.<br>2.Dengan membuat aplikasi kriptografi sebagai pengamanan dan kerahasiaan pesan yang dikirim maupun diterima. |
| 2 | Pengumpulan Data | Diperoleh data dari jurnal penelitian terkait yaitu Teknik kriptografi menggunakan algoritme RSA dengan menggabungkan dengan *playfair chiper* yang akan menambah keamanan pesan yang dikirim maupun diterima. |

| No | Tahapan | Hasil |
|---|---|---|
| 3 | Menganalisis Teori | Dari jurnal penelitian terkait dan buku pemrograman diperoleh teori :<br>1.Aplikasi android.<br>2.Teknik kriptografi RSA dan *playfair cipher*<br>3.Dari *ebook* tentang pendekatan sistem SDLC *waterfall* diperoleh tahapan teori pengembangan sistem dari *Project planing phase, Analysis phase, Desain phase, Implementasi phase* dan *Support phase.* |
| 4 | Pembuatan Jadwal | Penelitian ini dimulai pada bulan Febuari 2017 selesai pada bulan Juni 2017 (± 5 Bulan) yang dijelaskan pada Gambar 1.1 Waktu penelitian. |
| 5 | Mencari Solusi | Aplikasi kriptografi dibangun agar dapat dapat menyamarkan pesan rahasia yang dikirim dan diterima dengan mengacak atau merubah pesan aslinya. |
| 6 | Mendefinisikan Kebutuhan | 1. Spesifikasi *hardware* yang digunakan adalah laptop dengan *harddisk* 500gb, RAM 2<br>2. Spesifikasi *software* yang digunakan yaitu sistem<br>3. operasi *open source* linux ubuntu 16.04.2 32 bit, eclipse, JDK 1.8, SDK 19, *libre office,* dia diagram dan *Genymotion*. |

*1. Analysis* Proses

Proses *flowchart* algoritme RSA dengan kriptografi *playfair cipher*.




Gambar 3. Proses Algoritma RSA dengan playfair cipher

2. Analisis Kriptografi

Sesuai dengan alur *flowchart* analisis untuk pengamanan pesan, maka pesan asli akan diacak (enkripsi) terlebih dulu menjadi pesan tersandi.

1. Proses enkripsi algoritma RSA

Dalam proses enkripsi algoritme RSA ada beberapa tahap yaitu sebagai berikut :

a. Untuk membangkitkan kunci public dan kunci privat maka menentukan nilai p dan q yaitu :

nilai p : 47
nilai q : 71

perhitungan untuk menentukan kunci *public* sebagai berikut :

$n = p * q$ dimana, n = kunci *public*
p = nilai p
q = nilai q

menentukan nilai pembangkit kunci *public*

Untuk n = p * q
= 47 * 71
= 3337

b. Menentukan *totient* dari kunci *public* (n)

untuk menghitung nilai totient sebagai berikut :

$Q = (p-1)(q-1)$ dimana, Q = *totient* dari kunci *public*
p = nilai p
q = nilai q

menentukan nilai *totient* dari kunci *public*

untuk Q(n) = (p - 1)(q – 1)
= (47-1)(71-1)
= 46 * 70
= 3220

c. Memilih kunci *public* e = 79, karena 79 relatif prima dengan 3220

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

d. Mengitung kunci deskripi / kunci *private* sebagai berikut :

$$d = (1 + ( k * Q(n))) /e$$

keterangan, d = kunci *private*
k = bilangan bulat
Q= nilai *totient*
e = kunci *public*
menentukan nilai dari kunci private
untuk d = (1 + ( k × Q(n))) /e
= (1 + ( 25 × 3220)) / 79
= 1019
Setelah kunci privat dan kunci publik terbentuk barulah bisa mengenkripsi pesan yang akan dikirim sebagai berikut :
pesan asli: Kharisma 2013
kunci : Yakin bisa 100%
mengubah pesan asli ke dalam kode ASCII Untuk *index* karakter pesan asli dapat dilihat pada tabel dibaawah ini *Index* karakter pesan asli berikut :

Tabel 2. *Index* Karakter Asli

| ***Index* ke-i** | **Kunci (K)** | **Desimal dalam ASCII 256 bit** |
|---|---|---|
| $P_1$ | K | 75 |
| $P_2$ | h | 104 |
| $P_3$ | a | 97 |
| $P_4$ | r | 114 |
| $P_5$ | i | 105 |
| $P_6$ | s | 115 |
| $P_7$ | m | 109 |
| $P_8$ | a | 97 |
| $P_9$ | (spasi) | 32 |
| $P_{10}$ | 2 | 50 |
| $P_{11}$ | 0 | 48 |
| $P_{12}$ | 1 | 49 |
| $P_{13}$ | 3 | 51 |

memecah P menjadi blok yang lebih kecil, misalnya P dipecah menjadi beberapa blok yang berukuran beberapa digit:
P = 751049711410511510997325048495 1
dipecah menjadi beberapa digit :
$P_1 = 751$ $P_4 = 410$ $P_7 = 997$ $P_{10} = 49$
$P_2 = 049$ $P_5 = 511$ $P_8 = 325$ $P_{11} = 51$
$P_3 = 711$ $P_6 = 510$ $P_9 = 048$
dalam menentukan nilai nilai P ini masih terletak di dalam selang [0, 3337 – 1] agar transformasi menjadi satu-ke-satu.

Setelah menentukan nilai setiap nilai m maka bisa menghitung *ciphertext* pesan yang akan dikirim dengan rumus sebagai berikut :

$$C = P^e \bmod n$$

keterangan :
C = *ciphertext*
p = *plantext*
*e* = kunci publik
n = pembangkit kunci publik
maka didapatkan ciphertext setiap P adalah :
$C_1 = 751^{79} \bmod 3337 = 3289$
$C_2 = 049^{79} \bmod 3337 = 789$
$C_3 = 711^{79} \bmod 3337 = 2415$
$C_4 = 410^{79} \bmod 3337 = 566$
$C_5 = 511^{79} \bmod 3337 = 1486$
$C_6 = 510^{79} \bmod 3337 = 1143$
$C_7 = 997^{79} \bmod 3337 = 1436$
$C_8 = 325^{79} \bmod 3337 = 93$
$C_9 = 048^{79} \bmod 3337 = 2304$
$C_{10} = 49^{79} \bmod 3337 = 789$
$C_{11} = 51^{79} \bmod 3337 = 523$
jadi ciphertext dari algoritma RSA adalah :
**“3289789241556614861143143693230478952 3”.**

2. Proses enkripsi *playfair cipher*

Setelah tahap pertama pengacakan pesan akan dilanjutkan dengan tahap kedua yaitu pengacakan menggunakan *playfair cipher*. Untuk *index* karakter kunci dapat dilihat pada tabel 3 *Index* karakter kunci berikut:

Tabel 3. *Index* Karakter Kunci

| ***Index* ke-i** | **Kunci (K)** | **Desimal dalam ASCII 256 bit** |
|---|---|---|
| $K_1$ | Y | 89 |
| $K_2$ | a | 97 |
| $K_3$ | k | 107 |
| $K_4$ | i | 105 |
| $K_5$ | n | 110 |
| $K_6$ | (spasi) | 32 |
| $K_7$ | b | 98 |
| $K_8$ | i | 105 |
| $K_9$ | s | 115 |
| $K_{10}$ | a | 97 |

Masukkan kunci kedalam tabel playfair 16x16 seperti beikut :

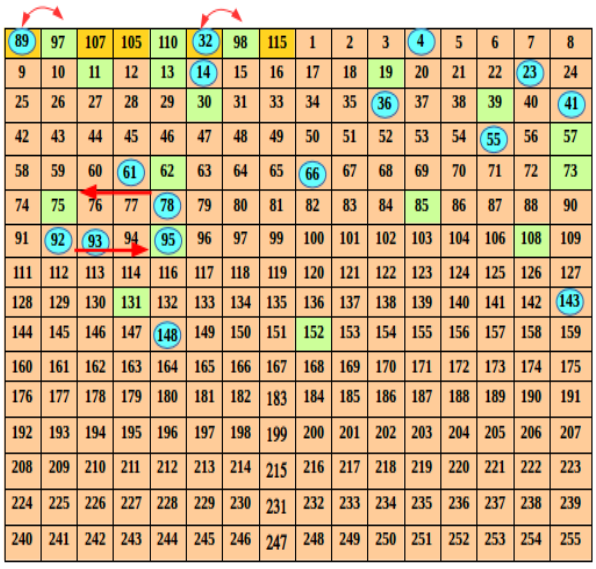
| | | | | | | | | | | | | | | | |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 89 | 97 | 107 | 105 | 110 | 32 | 98 | 115 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 |
| 9 | 10 | 11 | 12 | 13 | 14 | 15 | 16 | 17 | 18 | 19 | 20 | 21 | 22 | 23 | 24 |
| 25 | 26 | 27 | 28 | 29 | 30 | 31 | 33 | 34 | 35 | 36 | 37 | 38 | 39 | 40 | 41 |
| 42 | 43 | 44 | 45 | 46 | 47 | 48 | 49 | 50 | 51 | 52 | 53 | 54 | 55 | 56 | 57 |
| 58 | 59 | 60 | 61 | 62 | 63 | 64 | 65 | 66 | 67 | 68 | 69 | 70 | 71 | 72 | 73 |
| 74 | 75 | 76 | 77 | 78 | 79 | 80 | 81 | 82 | 83 | 84 | 85 | 86 | 87 | 88 | 90 |
| 91 | 92 | 93 | 94 | 95 | 96 | 97 | 99 | 100 | 101 | 102 | 103 | 104 | 106 | 108 | 109 |
| 111 | 112 | 113 | 114 | 116 | 117 | 118 | 119 | 120 | 121 | 122 | 123 | 124 | 125 | 126 | 127 |
| 128 | 129 | 130 | 131 | 132 | 133 | 134 | 135 | 136 | 137 | 138 | 139 | 140 | 141 | 142 | 143 |
| 144 | 145 | 146 | 147 | 148 | 149 | 150 | 151 | 152 | 153 | 154 | 155 | 156 | 157 | 158 | 159 |
| 160 | 161 | 162 | 163 | 164 | 165 | 166 | 167 | 168 | 169 | 170 | 171 | 172 | 173 | 174 | 175 |
| 176 | 177 | 178 | 179 | 180 | 181 | 182 | 183 | 184 | 185 | 186 | 187 | 188 | 189 | 190 | 191 |
| 192 | 193 | 194 | 195 | 196 | 197 | 198 | 199 | 200 | 201 | 202 | 203 | 204 | 205 | 206 | 207 |
| 208 | 209 | 210 | 211 | 212 | 213 | 214 | 215 | 216 | 217 | 218 | 219 | 220 | 221 | 222 | 223 |
| 224 | 225 | 226 | 227 | 228 | 229 | 230 | 231 | 232 | 233 | 234 | 235 | 236 | 237 | 238 | 239 |
| 240 | 241 | 242 | 243 | 244 | 245 | 246 | 247 | 248 | 249 | 250 | 251 | 252 | 253 | 254 | 255 |

Gambar 4. Tabel P*layfair Cipher* 1

Berdasarkan tabel 3.2 kunci diatas maka dapat dicari ciphertext ke 2 dari playfair dengan mengunakan ciphertext dari algortime RSA yang sudah diketahui seperti berikut :

***Ciphertext* ke 1 :**
**"32897892415566148611431436932304789523".**
**bigram : " 32 89 78 92 41 55 66 148 61 143 14 36 93 23 04 78 95 23 ".**

dari diagram diatas maka dapat dicari ciphertext dari tabel kunci playfair dari gambar berikut :



Gambar 5 Tabel P*layfair Cipher* 2

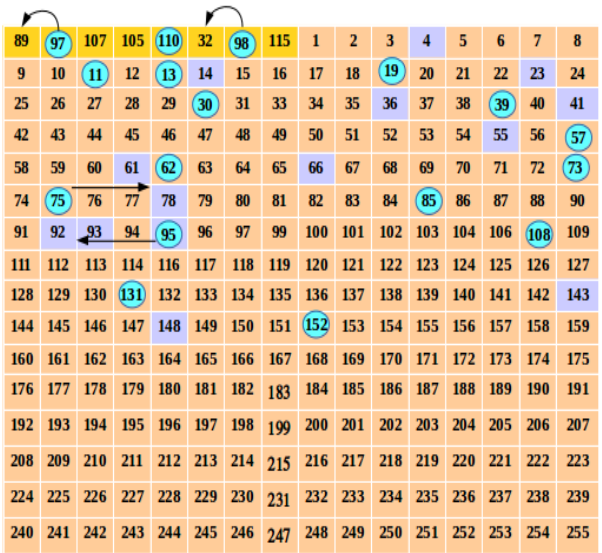
dari gambar tabel 5 maka didapatkan *ciphertext* ke 2 dengan langkah *playfair cipher* sebagai berikut :

1. Jika kedua angka tidak terletak pada baris dan kolom yang sama,maka angka pertama men-jadi angka yang sebaris dengan angka pertama dan sekolom dengan angka kedua. Angka ke-dua menjadi angka yang sebaris dengan angka kedua dan yang sekolom dengan angka pertama.
2. Jika kedua angka terletak pada baris yang sama maka angka pertama menjadi angka setelahnya dalam baris yang sama, demikian juga dengan angka kedua. Jika terletak pada baris kelima, maka menjadi baris pertama, dan sebaliknya. Arahnya tergantung dari posisi angka pertama dan kedua, pergeserannya ke arah angka kedua.
3. Jika kedua angka terletak pada kolom yang sama maka angka pertama menjadi angka setelahnya dalam kolom yang sama, demikian juga dengan angka kedua. Jika terletak pada kolom kelima, maka menjadi kolom pertama, dan sebaliknya. Arahnya tergantung dari posisi angka pertama dan kedua, pergeserannya ke arah angka kedua.
4. Jika kedua angka sama, maka letakkan sebuah angka di tengahnya (sesuai kesepakatan).

Diperolehlah ciphertext playfair :
**"97987595395762152731311930111081108513108".**

3. Proses dekripsi *playfair chiper*

Setelah pesan terkirim maka akan dilakukan pengembalian ke pesan asli oleh penerima dengan pendekripsian pesan dengan menggunakan tabel kunci *playfair* dari langkah enkripsi dengan cara kebalikannya seperti pada gambar berikut :



Gambar 6 tabel playfair cipher 3

**pesan ciphertext :**
**"97987595395762152731311930111081108513108"**
**bigram :"97 98 75 95 39 57 62 152 73 131 19 30 11 108 110 85 13 108"**
**hasil plaintext playfair:**
"**32897892415566148611431436932304789523**".

4. Proses dekripsi algoritme RSA

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

Pesan hasil dekripsi *playfair cipher* akan di dekripsikan kembali dengan algoritme RSA sehingga akan menghasilkan pesan aslinya. Pecah *ciphertext* dalam beberapa blok yang lebih kecil seperti berikut :

*Ciphertext* :

**"32897892415566148611431436932304789523"**

$C_1 = 3289$ $C_5 = 1486$ $C_9 = 2304$
$C_2 = 789$ $C_6 = 1143$ $C_{10} = 789$
$C_3 = 2415$ $C_7 = 1436$ $C_{11} = 523$
$C_4 = 566$ $C_8 = 93$

Setelah menentukan nilai setiap nilai C maka bisa menghitung dekripsi pesan yang akan diterima menjadi pesan asli dengan rumus sebagai berikut :

$$P = C^d \bmod n$$

keterangan,
P = *plaintext*
C = *ciphertext*
d = kunci deskripsi/kunci privat
n = pembangkit kunci publik

*Plaintext* dari setiap nilai C dengan kunci privat yang sudah dicari sebelumnya yaitu dengan d = 1019. Maka didapatkan nilai *plaintext* yaitu :

$P_1 = 3289^{1019} \bmod 3337 = 751$
$P_2 = 789^{1019} \bmod 3337 = 049$
$P_3 = 2415^{1019} \bmod 3337 = 711$
$P_4 = 566^{1019} \bmod 3337 = 410$
$P_5 = 1486^{1019} \bmod 3337 = 511$
$P_6 = 1143^{1019} \bmod 3337 = 510$
$P_7 = 1436^{1019} \bmod 3337 = 997$
$P_8 = 93^{1019} \bmod 3337 = 328$
$P_9 = 2304^{1019} \bmod 3337 = 048$
$P_{10} = 789^{1019} \bmod 3337 = 49$
$P_{11} = 523^{1019} \bmod 3337 = 51$

Maka diperoleh *plaintext* asli yang dikirimkan sebelumnya yaitu

***Plaintext* = "57 104 97 114 105 115 109 97 32 80 48 49 51".**

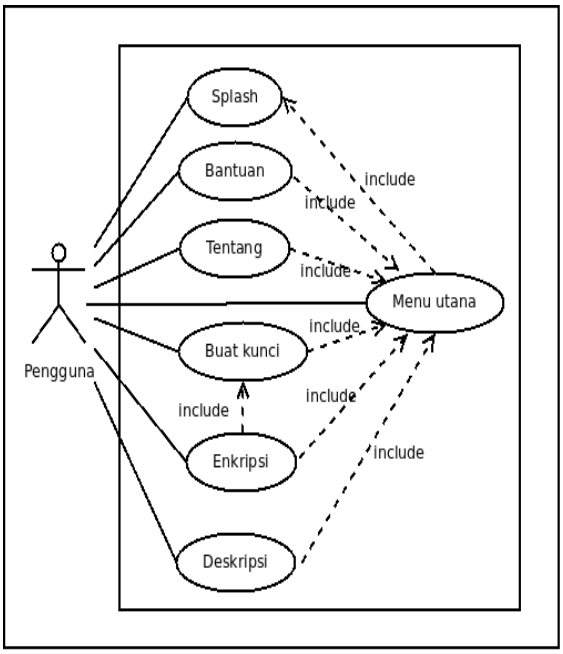
diubah dalam kode ASCII menjadi = **Kharisma 2013.**

B. Hasil Analisis Sistem

1. *Actor Description*

Aktor pada aplikasi ini adalah pengguna.

2. *Usecase diagram*

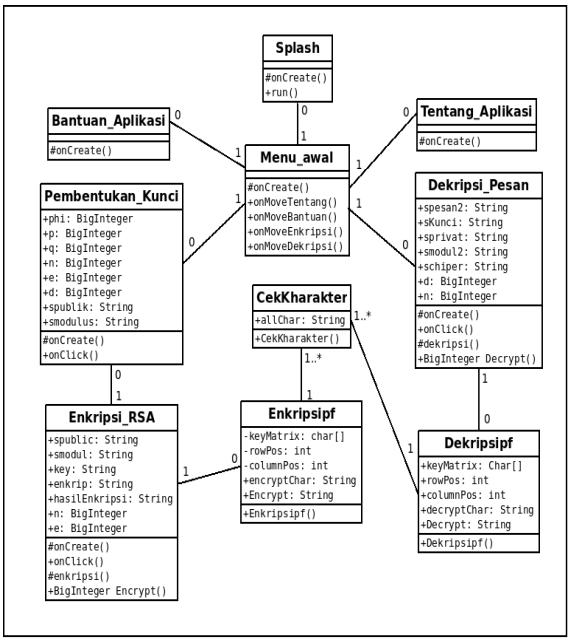



Gambar 7. *Use Case Diagram*

3. Skenario *Usecase*

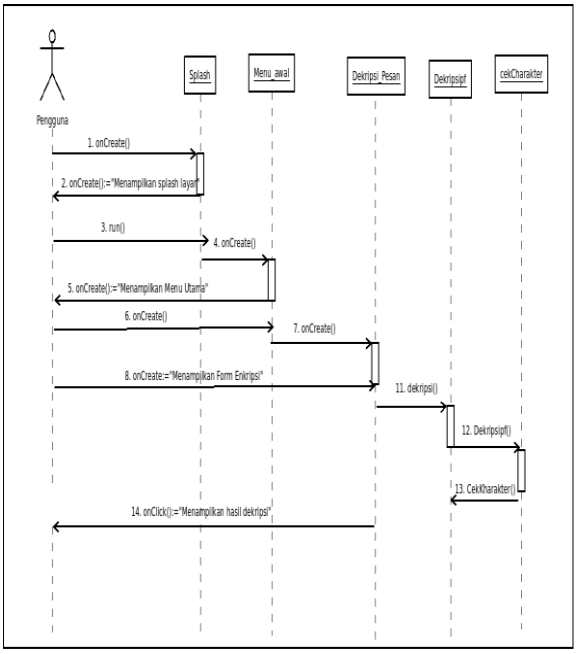
Terdiri dari 7 skenario yaitu s*plash, m*enu utama, bantuan, tentang, enkripsi, buat kunci dan dekripsi.

4. *Class diagram*



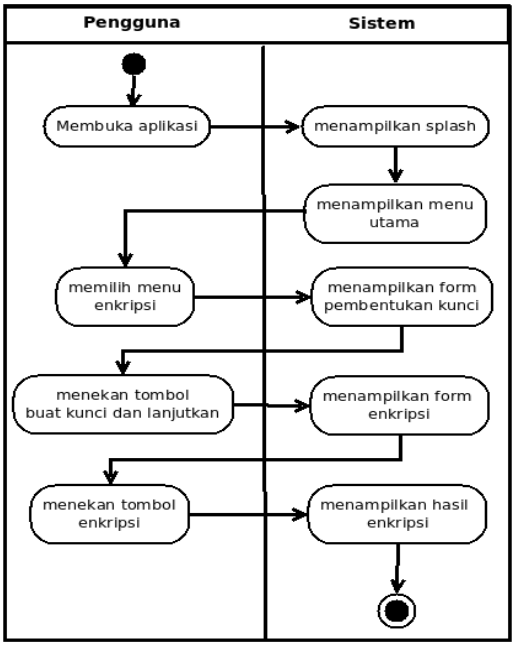

Gambar 8. *Class diagram*

5. Sequence diagram




Gambar 9. Sequence Diagram Enkripsi Pesan

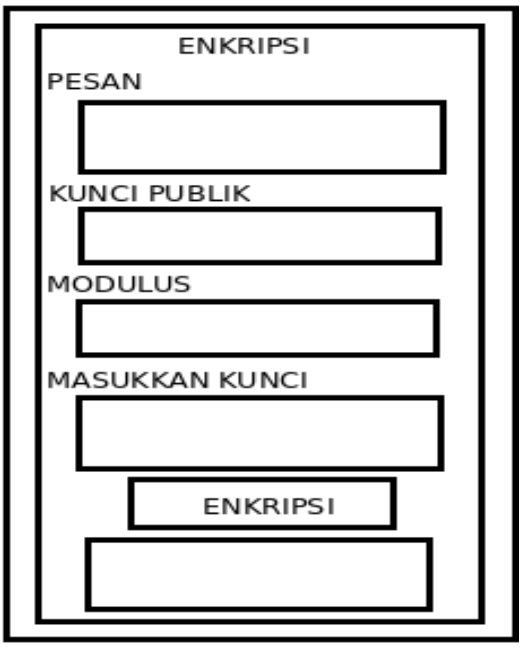
6. *Actitvity diagram*



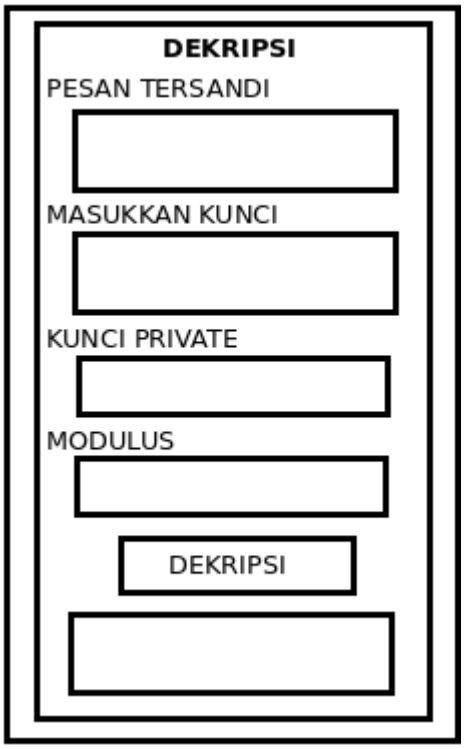

Gambar 10. *Activity Diagram* Enkripsi Pesan

*C. Desain phase*

1. Desain antar muka




Gambar 11. Desain Antarmuka Enkripsi Pesan

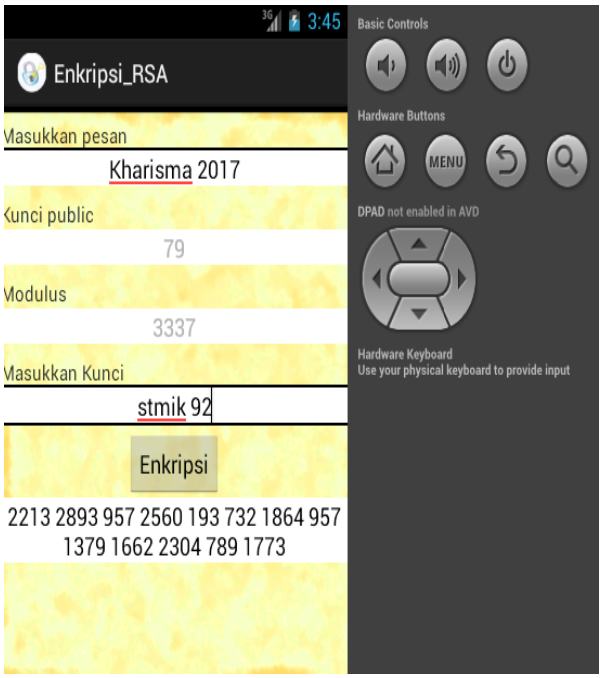



Gambar 12. Desain Antarmuka Dekripsi Pesan

ISSN 2527-1682 (Print)
ISSN 2527-9165 (Online)

*D. Implementation Phase*

1. Tampilan Aplikasi kriptografi




Gambar 13. Tampilan Halaman *Enkripsi*


Gambar 14 Tampilan Halaman *Dekripsi*

2. Instalasi Sistem

a. Instalasi perangkat keras s*martphone* dengan RAM 2 Gb dan internal *storage* minimal 4 Gb.

b. Instalasi Perangkat lunak dengan sistem operasi minimal *Gingerbird* 2.3.3.

## IV. PENUTUP

A. Kesimpulan

Dari penelitian ini dapat disimpulkan bahwa :

1. Dapat mengimplementasikan kriptografi algoritma *rivest shamir adleman* (RSA) yang dipadukan dengan playfair cipher berbasis android pada media file teks
2. Dapat mengimplementasikan ilmu kriptografi dalam bidang teknik informatika sebagai menyamarkan pesan aslinya untuk melindungi keamananya.

B. Saran

Berdasarkan kesimpulan diatas, aplikasi ini masih memiliki kekurangan dan perlu dikembangkan lagi seperti :

1. Dalam pengimplementasi algoritme *rivest shamir adleman* (RSA) dapat dipadukan dengan kriptografi lain tidak hanya dengan *playfair cipher* saja
2. Pesan yang diamankan dapat diperpanjang karakter teks pesan yang akan ditulis

## V. REFERENSI

[1] Puspita, Kori Carda. (2016). implementasi kriptografi dengan metode rsa menggunakan java.jurnal.Bandung.Teknik Informatika Fakultas Sains dan Teknologi , Universitas Islam Negeri Sunan Gunung Djati Bandung.

[2] Susanto, Ajib., Tritanto, Rico. (2011).Kombinasi Algoritma Rsa Dan Algoritma Gipher Transposisi Untuk

[3] Santi, Rina Chandra Noer. (2010). Implementasi Algoritma Enkripsi Playfair pada File Teks.jurnal. Program Studi Teknik Informatika Fakultas Teknologi Informasi, Universitas Stikubank.

[4] Kromodimoeljo, Sentot. (2009). Teori dan Aplikasi Kriptografi.SPK IT Consulting

[5] Satzinger, John W, Jackson, Robert B, dan Burd, Stephen D. (2010). System analysis and design in a changing world, fifth edition. Course Technology, Boston.