

# Pengamanan Pesan Teks Menggunakan Algoritma FEAL dan RSA Pada Aplikasi Android

Sri Nofrida Siregar

Program Studi Teknik Informatika, Universitas Budi Darma, Medan, Indonesia

Email: srinofrida40@gmail.com

Submitted: 28/06/2020; Accepted: 20/08/2020; Published: 21/08/2020

**Abstrak**—Pesan teks sangat rentan terhadap penyandapan maupun pencurian informasi oleh pihak-pihak yang tidak bertanggung jawab. Demi menjaga keamanan pesan teks dapat dilakukan dengan pemanfaatan teknik kriptografi. Teknik kriptografi dapat menyandikan pesan teks dengan mengenkripsikannya ke dalam bentuk sandi-sandi yang tidak dipahami. Algoritma FEAL adalah algoritma enkripsi tipe simetris block chipper, yang panjang blok 64 bit, panjang kunci 64 bit, dan memiliki iterasi sebanyak 8 ronde. Algoritma RSA adalah salah satu algoritma yang dapat diandalkan dalam mewujudkan teknik kriptografi. Algoritma asimetri ini akan menghasilkan tingkat keamanan yang lebih tinggi terhadap pesan teks karena prosesnya yang cukup rumit dengan pembangkitan dan menggunakan kunci yang berbeda sehingga akan mempersulit kriptanalisis untuk mengakses pesan teks tersebut. Penelitian ini akan menggunakan Algoritma FEAL dan RSA untuk proses enkripsi dan dekripsinya, sehingga dalam prosesnya perlu melalui beberapa tahap yang panjang agar dapat menghasilkan cipher akhirnya. Penelitian ini menguraikan proses pengamanan pesan teks dengan menyandikannya berdasarkan algoritma FEAL dan RSA, dalam bentuk sandi yang sulit dipahami dan dimengerti oleh orang lain. Hal ini dilakukan sebagai upaya untuk meminimalisir tindakan-tindakan dari pihak-pihak yang tidak bertanggung jawab.

**Kata Kunci:** Kriptografi, Pesan Teks, FEAL, RSA

**Abstract**—Text messages are very vulnerable to the encoding or theft of information by irresponsible parties. In order to maintain the security of text messages, it can be done by using cryptographic techniques. Cryptographic techniques can encode text messages by encrypting them in the form of passwords that are not understood. The FEAL algorithm is a symmetrical block chipper type encryption algorithm, which has a block length of 64 bits, a length of 64 bits, and has an iteration of 8 rounds. The RSA algorithm is one algorithm that can be relied upon in realizing cryptographic techniques. This asymmetry algorithm will produce a higher level of security against text messages because the process is quite complicated with generation and uses different keys so that it will be difficult for cryptanalysts to access the text messages. This research will use FEAL and RSA Algorithm for the encryption and decryption process, so that in the process it is necessary to go through several long steps in order to produce the final cipher. This study describes the process of securing text messages by encoding them based on the FEAL and RSA algorithms, in the form of a password that is difficult for others to understand and understand. This is done as an effort to minimize the actions of irresponsible parties.

**Keywords:** Cryptography, Text Messaging, FEAL, RSA

## 1. PENDAHULUAN

Pesan teks merupakan salah satu cara komunikasi baik yang formal maupun tidak formal yang dikirim oleh satu orang ke orang lain. Pesan adalah inti dari prosesnya komunikasi yang terjalin, pesan teks biasanya disampaikan melalui perangkat komunikasi yang saat ini dikenal dengan telepon genggam (*handphone*).

Keamanan merupakan salah satu aspek penting dalam pengiriman data maupun komunikasi melalui jaringan. Keamanan digunakan untuk menjaga kerahasiaan pesan teks agar pesan teks tetap terjaga hingga pada penerima. Oleh sebab itu keamanan sangat penting untuk melindungi pesan dari segala aspek-aspek yang dapat merugikan. Pesan-pesan yang dikirim dengan memakai keamanan merupakan pesan yang sangat penting dan rahasia agar pada saat pesan sampai kepada penerimanya pesan masih tetap utuh dengan proses enkripsi dan dekripsi.

Masalah keamanan merupakan salah satu aspek penting dalam pengiriman pesan teks rahasia melalui jaringan. Hal ini disebabkan oleh kemajuan jaringan komputer dengan konsep *open system*-nya sehingga sangat mudah untuk seseorang masuk ke dalam jaringan tersebut. Hal ini dapat mengakibatkan proses pengiriman pesan teks menjadi tidak aman karena adanya pihak-pihak yang tidak bertanggung jawab pada saat pesan teks dikirim. Oleh karena itu dibutuhkan sistem keamanan yang dapat menjaga kerahasiaan pesan teks, maka demi menghindari masalah tersebut peneliti memberikan suatu solusi untuk pengamanan pesan teks menggunakan algoritma FEAL dan RSA pada aplikasi android *client server*.

Algoritma FEAL merupakan suatu algoritma simetrik yang mempunyai nilai kunci enkripsi dan dekripsi yang sama. Kunci pada algoritma simetrik diasumsikan dengan sifat rahasia karena pihak enkripsi dan dekripsi yang dapat melakukan dan mengetahui nilainya. Sedangkan algoritma RSA merupakan algoritma asimetrik atau sering disebut dengan kunci publik karena nilai kunci enkripsi dan dekripsinya tidak sama. Nilai kunci enkripsi disebut dengan kunci publik yang bersifat terbuka dan nilai kunci dekripsi disebut dengan kunci privat yang bersifat rahasia.

Berdasarkan penelitian sebelumnya yang dilakukan oleh Semuil Tjiharjadi, dan Marvin Chandra Wijaya pada tanggal 20 Juni 2009 di Yogyakarta dengan judul “Pengamanan Data Menggunakan Metoda Enkripsi Simetri Dengan Algoritma Feal” yang membahas isi bagaimana cara mengamankan sebuah data agar tidak diambil oleh

pihak lain yang tidak bertanggung jawab, pada saat data dikirimkan, sehingga data benar-benar aman pada saat sampai ditujuan [1].

Penelitian kedua dilakukan oleh Andi Riski Alvianto dan Darmaji pada Volume 4 No 1 tahun 2015 di Surabaya dengan judul “Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android” yang membahas tentang pengamanan pesan via SMS berbasis android menggunakan algoritma RSA. Dengan membuat sebuah aplikasi pada smartphone berbasis Android untuk memodifikasi pesan SMS menjadi ciphertext agar isi informasi dari SMS tersebut tidak diketahui oleh orang lain. Pada saat pengiriman pesan telah menjadi *ciphertext* kemudian dikirimkan kepada penerima agar didekripsi [2].

## 2. METODOLOGI PENELITIAN

### 2.1 Kriptografi

Kriptografi (*cryptography*) berasal dari bahasa Yunani, terdiri dari dua suku kata yaitu *kripto* dan *graphia*. *Kripto* artinya menyembunyikan, sedangkan *graphia* artinya tulisan. Sehingga Kriptografi dapat diartikan sebagai ilmu yang mempelajari tentang penyembunyian huruf atau tulisan sehingga membuat tulisan tersebut tidak dapat dibaca oleh orang yang tidak berkepentingan. Algoritma atau hitungan kriptografi dapat disebut juga *chipper* yaitu hitungan matematik yang digunakan untuk membuat suatu enkripsi maupun dekripsinya. Sebuah data yang tidak dienkripsi disebut *plaintext* [3][4].

### 2.2 Algoritma FEAL

Akihiro Shimizu dan Shoji Miyaguchi dari NTT Jepang (1435). FEAL singkatan dari *Fast Encryption Algorithm*. FEAL merupakan enkripsi tipe simetris *block chippers*. FEAL mempunyai panjang blok 64 bit, panjang kunci 64 bit, dan memiliki iterasi sebanyak 8 ronde [1]

Untuk proses enkripsi, pertama kali program akan memeriksa terlebih dahulu ada atau tidaknya teks pada kotak *plaintext* sebagai teks input proses enkripsi, jika teks belum dimasukkan maka akan ditampilkan pesan peringatan dan program akan dihentikan. Pada fungsi enkripsi, kemudian akan dicek jumlah karakter dari *plaintext*-nya. Jika *plaintext* bukan kelipatan dari blok yang panjangnya 64 bit, maka akan ditambahkan angka “0” sebanyak jumlah karakter yang perlu ditambahkan agar jumlahnya merupakan kelipatan 64 bit dikurangi satu, dan karakter terakhir yang ditambahkan adalah nilai dari banyaknya karakter yang ditambahkan [1].

Proses dekripsi algoritma FEAL sama dengan proses enkripsi, hanya pada proses dekripsi input yang digunakan berupa ciphertext dan proses kerjanya kebalikan dari proses enkripsi. Pada proses dekripsi urutan kunci yang digunakan merupakan kebalikan dari urutan kunci yang digunakan pada proses enkripsinya [1].

### 2.3 Algoritma RSA

Enkripsi merupakan proses yang dilakukan untuk mengubah pesan asli (*plaintext*) menjadi sebuah pesan acak (*ciphertext*) yang tidak dapat diterjemahkan secara langsung oleh penerima, agar tidak dapat diketahui oleh orang lain [5].

Berikut ini merupakan proses dari enkripsi RSA. Dilakukan oleh pihak pengirim (*Sender*). Seluruh perhitungan pada pemangkatan bilangan modulo dilakukan menggunakan metode *fast exponentiation* [4].

Langkah-langkah proses enkripsi algoritma RSA antara lain yaitu :

1. Ambil kunci publik ( $n, e$ ).
2. Pilih plainteks  $m$ , dengan  $0 \leq m \leq n - 1$ .
3. Hitung  $c = me \text{ mod } n$ .
4. Diperoleh cipherteks  $c$

Dekripsi merupakan proses untuk mengolah pesan acak (*ciphertext*) menjadi data awal (*plaintext*), sehingga dapat dibaca atau dimengerti kembali [5].

Berikut ini merupakan proses dari dekripsi RSA. Dilakukan oleh pihak penerima yang telah menerima cipherteks [4].

Langkah-langkah proses dekripsi algoritma RSA antara lain yaitu :

1. Ambil kunci publik ( $n, e$ ) dan kunci rahasia ( $n, d$ ).
2. Hitung  $m = cd \text{ mod } n$ .
3. Diperoleh plainteks  $m$ .

## 3. HASIL DAN PEMBAHASAN

### 3.1 Analisa Masalah

Analisa yang dilakukan adalah kegiatan yang utama dalam skripsi ini untuk proses penguraian dari suatu aplikasi yang akan dirancang secara utuh ke dalam bagian-bagian komponennya dengan maksud untuk mengidentifikasi dan mengevaluasi permasalahan enkripsi data teks dan dekripsi data teks ke bentuk semula. Adapun tujuan dilakukannya analisis terhadap suatu sistem adalah untuk mengetahui alasan mengapa sistem

tersebut diperlukan, yaitu dengan merumuskan kebutuhan-kebutuhan dari sistem tersebut untuk meminimalisir sumber daya yang berlebih serta membantu merencanakan penjadwalan pembentukan sistem, meminimalkan distorasi-distorasi yang mungkin terdapat di dalam sistem tersebut sehingga dapat bekerja secara optimal.

### 3.2 Penerapan Algoritma FEAL dan RSA

Untuk mengenkripsi suatu pesan teks menggunakan algoritma FEAL dan RSA pesan yang akan dienkripsi hanya berupa sampel untuk keperluan hitungan manual. Berikut diuraikan penerapan algoritma FEAL DAN RSA dalam mengenkripsi pesan teks yang berisi karakter huruf sebagai berikut :

Plainteks : AYOCEPATPERGI

Kunci : 5

#### Enkripsi FEAL

$$\begin{aligned}C1 &= (P1 + 5) \text{ mod } 256 \\ &= (65 + 5) \text{ mod } 256 \\ &= 70 \text{ mod } 256 \\ &= 70 \\ &= F\end{aligned}$$

$$\begin{aligned}C2 &= (P2 + 5) \text{ mod } 256 \\ &= (89 + 5) \text{ mod } 256 \\ &= 94 \text{ mod } 256 \\ &= 94 \\ &= ^\end{aligned}$$

$$\begin{aligned}C3 &= (P3 + 5) \text{ mod } 256 \\ &= (79 + 5) \text{ mod } 256 \\ &= 84 \text{ mod } 256 \\ &= 84 \\ &= T\end{aligned}$$

$$\begin{aligned}C4 &= (P4 + 5) \text{ mod } 256 \\ &= (67 + 5) \text{ mod } 256 \\ &= 72 \text{ mod } 256 \\ &= 72 \\ &= H\end{aligned}$$

$$\begin{aligned}C5 &= (P5 + 5) \text{ mod } 256 \\ &= (69 + 5) \text{ mod } 256 \\ &= 74 \text{ mod } 256 \\ &= 74 \\ &= J\end{aligned}$$

$$\begin{aligned}C6 &= (P6 + 5) \text{ mod } 256 \\ &= (80 + 5) \text{ mod } 256 \\ &= 85 \text{ mod } 256 \\ &= 85 \\ &= U\end{aligned}$$

$$\begin{aligned}C7 &= (P7 + 5) \text{ mod } 256 \\ &= (65 + 5) \text{ mod } 256 \\ &= 70 \text{ mod } 256 \\ &= 70 \\ &= F\end{aligned}$$

$$\begin{aligned}C8 &= (P8 + 5) \text{ mod } 256 \\ &= (84 + 5) \text{ mod } 256 \\ &= 89 \text{ mod } 256 \\ &= 89 \\ &= Y\end{aligned}$$

$$\begin{aligned}C9 &= (P9 + 5) \text{ mod } 256 \\ &= (80 + 5) \text{ mod } 256 \\ &= 85 \text{ mod } 256 \\ &= 85 \\ &= U\end{aligned}$$

$$\begin{aligned}C10 &= (P10 + 5) \text{ mod } 256 \\ &= (69 + 5) \text{ mod } 256 \\ &= 74 \text{ mod } 256 \\ &= 74\end{aligned}$$

$$\begin{aligned} &= J \\ C_{11} &= (P_{11} + 5) \bmod 256 \\ &= (82 + 5) \bmod 256 \\ &= 87 \bmod 256 \\ &= 87 \\ &= W \\ C_{12} &= (P_{12} + 5) \bmod 256 \\ &= (71 + 5) \bmod 256 \\ &= 76 \bmod 256 \\ &= 76 \\ &= L \\ C_{13} &= (P_{13} + 5) \bmod 256 \\ &= (73 + 5) \bmod 256 \\ &= 78 \bmod 256 \\ &= 78 \\ &= N \end{aligned}$$

Sehingga Ciphertext adalah : F<sup>^</sup>THJUFYUJWLN

### Enkripsi RSA

Plaintext : F<sup>^</sup>THJUFYUJWLN → 70 94 84 72 74 85 70 89 85 74 87 76 78

e = 5

n = p x q

$$\begin{aligned} n &= 113 \times 157 \\ &= 17741 \end{aligned}$$

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

$$C_1 = P^5 \bmod 17741$$

$$\begin{aligned} C_1 &= 70^5 \bmod 17741 \\ &= 6365 \end{aligned}$$

$$C_2 = P^5 \bmod 17741$$

$$\begin{aligned} C_2 &= 94^5 \bmod 17741 \\ &= 14308 \end{aligned}$$

$$C_3 = P^5 \bmod 17741$$

$$\begin{aligned} C_3 &= 84^5 \bmod 17741 \\ &= 15753 \end{aligned}$$

$$C_4 = P^5 \bmod 17741$$

$$\begin{aligned} C_4 &= 72^5 \bmod 17741 \\ &= 13208 \end{aligned}$$

$$C_5 = P^5 \bmod 17741$$

$$\begin{aligned} C_5 &= 74^5 \bmod 17741 \\ &= 15567 \end{aligned}$$

$$C_6 = P^5 \bmod 17741$$

$$\begin{aligned} C_6 &= 85^5 \bmod 17741 \\ &= 11284 \end{aligned}$$

$$C_7 = P^5 \bmod 17741$$

$$\begin{aligned} C_7 &= 70^5 \bmod 17741 \\ &= 6365 \end{aligned}$$

$$C_8 = P^5 \bmod 17741$$

$$\begin{aligned} C_8 &= 89^5 \bmod 17741 \\ &= 8735 \end{aligned}$$

$$C_9 = P^5 \bmod 17741$$

$$\begin{aligned} C_9 &= 85^5 \bmod 17741 \\ &= 11284 \end{aligned}$$

$$C_{10} = P^5 \bmod 17741$$

$$\begin{aligned} C_{10} &= 74^5 \text{ mod } 17741 \\ &= 15567 \end{aligned}$$

$$\begin{aligned} C_{11} &= P^5 \text{ mod } 17741 \\ C_{11} &= 87^5 \text{ mod } 17741 \\ &= 17185 \end{aligned}$$

$$\begin{aligned} C_{12} &= P^5 \text{ mod } 17741 \\ C_{12} &= 76^5 \text{ mod } 17741 \\ &= 88102 \end{aligned}$$

$$\begin{aligned} C_{13} &= P^5 \text{ mod } 17741 \\ C_{13} &= 78^5 \text{ mod } 17741 \\ &= 4028 \end{aligned}$$

Sehingga Ciphertext adalah 6365 14308 15753 13208 15567 11284 6365 8735 11284 15567 17185 88102 4028

### Dekripsi RSA

$$e = 5$$

$$Q(n) = (113-1) \times (157-1) = 17472$$

Kunci dekripsi (d)  $\rightarrow$   $e = 5$  &  $Q(n) = 17472$

$$e * d = 1 \text{ mod } (Q(n))$$

$$5 * d = 1 \text{ mod } (17472)$$

Missalkan  $d = 6989$

$$5 * 6989 = 1 \text{ mod } 17472$$

$$34945 \text{ mod } 17472 = 1$$

Karena  $e * d = 1 \text{ mod } (Q(n))$ ,

Maka nilai  $d = 6989$  dapat digunakan.

$$P = C^d \text{ mod } n$$

$$\begin{aligned} P_1 &= 6365^{6989} \text{ mod } 17741 \\ &= 70 \end{aligned}$$

$$\begin{aligned} P_2 &= 14308^{6989} \text{ mod } 17741 \\ &= 94 \end{aligned}$$

$$\begin{aligned} P_3 &= 15753^{6989} \text{ mod } 17741 \\ &= 84 \end{aligned}$$

$$\begin{aligned} P_4 &= 13208^{6989} \text{ mod } 17741 \\ &= 72 \end{aligned}$$

$$\begin{aligned} P_5 &= 15567^{6989} \text{ mod } 17741 \\ &= 74 \end{aligned}$$

$$\begin{aligned} P_6 &= 11284^{6989} \text{ mod } 17741 \\ &= 85 \end{aligned}$$

$$\begin{aligned} P_7 &= 6365^{6989} \text{ mod } 17741 \\ &= 70 \end{aligned}$$

$$\begin{aligned} P_8 &= 8735^{6989} \text{ mod } 17741 \\ &= 89 \end{aligned}$$

$$\begin{aligned} P_9 &= 11284^{6989} \text{ mod } 17741 \\ &= 85 \end{aligned}$$

$$\begin{aligned} P_{10} &= 15567^{6989} \text{ mod } 17741 \\ &= 74 \end{aligned}$$

$$\begin{aligned} P_{11} &= 17185^{6989} \text{ mod } 17741 \\ &= 87 \end{aligned}$$

$$P_{12} = 88102^{6989} \text{ mod } 17741$$

$$= 76$$

$$P13 = 4028^{6989} \bmod 17741 \\ = 78$$

Sehingga plaintext adalah 70 94 84 72 74 85 70 89 85 74 87 76 78 → F<sup>A</sup>THJUFYUJWLN

### **Dekripsi FEAL**

Ciphertext : F<sup>A</sup>THJUFYUJWLN

Kunci : 5

$$P_i = (C_i - 5) \bmod 256$$

$$P1 = (C1 - 5) \bmod 256 \\ = (70 - 5) \bmod 256 \\ = 65 \\ = A$$

$$P2 = (C1 - 5) \bmod 256 \\ = (94 - 5) \bmod 256 \\ = 89 \\ = Y$$

$$P3 = (C1 - 5) \bmod 256 \\ = (84 - 5) \bmod 256 \\ = 79 \\ = O$$

$$P4 = (C1 - 5) \bmod 256 \\ = (72 - 5) \bmod 256 \\ = 67 \\ = C$$

$$P5 = (C1 - 5) \bmod 256 \\ = (74 - 5) \bmod 256 \\ = 69 \\ = E$$

$$P6 = (C1 - 5) \bmod 256 \\ = (85 - 5) \bmod 256 \\ = 80 \\ = P$$

$$P7 = (C1 - 5) \bmod 256 \\ = (70 - 5) \bmod 256 \\ = 65 \\ = A$$

$$P8 = (C1 - 5) \bmod 256 \\ = (89 - 5) \bmod 256 \\ = 84 \\ = T$$

$$P9 = (C1 - 5) \bmod 256 \\ = (85 - 5) \bmod 256 \\ = 80 \\ = P$$

$$P10 = (C1 - 5) \bmod 256 \\ = (74 - 5) \bmod 256 \\ = 69 \\ = E$$

$$P11 = (C1 - 5) \bmod 256 \\ = (87 - 5) \bmod 256$$

$$= 82$$

$$= R$$

$$P12 = (C1 - 5) \text{ mod } 256$$

$$= (76 - 5) \text{ mod } 256$$

$$= 71$$

$$= G$$

$$P13 = (C1 - 5) \text{ mod } 256$$

$$= (78 - 5) \text{ mod } 256$$

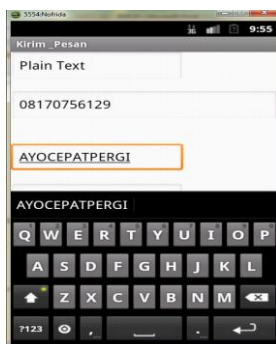
$$= 73$$

$$= I$$

Sehingga plaintext adalah “AYOCEPATPERGI”

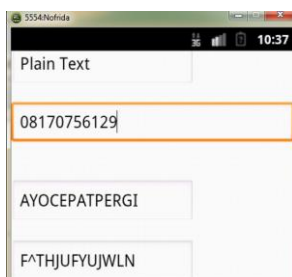
### 3.3 Kebutuhan Sistem

Pada tahap ini merupakan tahap untuk pesan teks yang akan dienkripsi atau pesan yang akan dikirim, dapat dilihat seperti pada gambar dibawah ini:



Gambar 1. Tampilan Tahap Plainteks

Proses enkripsi dilakukan sebanyak 2 kali proses yang telah digabungkan dalam satu tombol perintah. Proses enkripsi pertama kali dilakukan menggunakan algoritma FEAL dan hasil cipherteks langsung dijadikan sebagai plaintexts untuk algoritma RSA. Adapun proses enkripsi tersebut dapat dilihat pada gambar di bawah ini



Gambar 2. Tampilan Proses Enkripsi FEAL

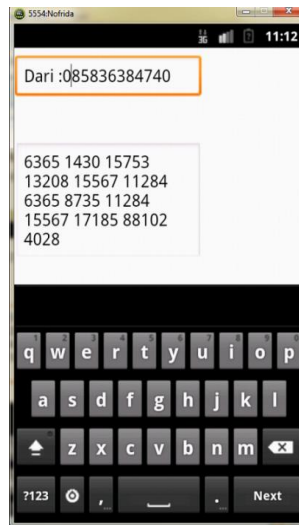
Berdasarkan pada gambar di atas, proses enkripsi berhasil menyandikan pesan teks *plaintexts* ke *cipherteks*. *Cipherteks* tersebut dapat *dicopy* dan di *paste* kan kembali kedalam *toolbox plaintexts* seperti gambar di bawah ini:



Gambar 3. tampilan proses Enkripsi RSA

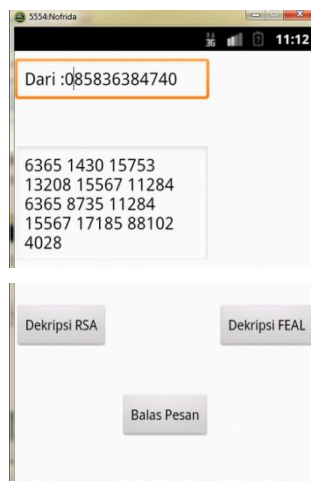
*Form* dekripsi pada aplikasi ini terdapat pada *form* pesan masuk yang terdapat di menu utama. Pada tahap ini ada 2 tahap yaitu tahap pertama yang dilakukan yaitu mendekripsi pesan teks algoritma RSA dan yang kedua

algoritma FEAL sehingga pesan asli akan diketahui. Adapun tampilan *form* dekripsi dapat dilihat pada gambar di bawah.



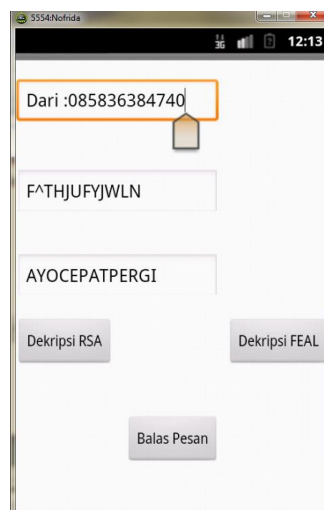
**Gambar 4.** Tampilan *Form* Dekripsi Pesan Masuk

Proses ini merupakan proses pertama untuk mengembalikan pesan teks yang asli. Adapun tampilannya dapat dilihat seperti gambar berikut ini :



**Gambar 5.** Tampilan Dekripsi RSA

Proses dekripsi algoritma FEAL merupakan proses kedua untuk mengembalikan pesan teks asli, sehingga dengan proses terakhir ini kita tahu apa sebenarnya makna/arti pesan teks kita terima, adapun tampilannya dapat dilihat seperti gambar berikut ini :



**Gambar 6.** Tampilan Dekripsi Algoritma FEAL

## 4. KESIMPULAN

Adapun kesimpulan yang diperoleh dari penulisan skripsi ini adalah sebagai berikut:

1. Pengamanan pesan teks berdasarkan algoritma FEAL dan RSA mampu mempersulit pihak-pihak untuk mengerti dan memahami isi dari pesan teks tersebut.
2. Tingkat keamanan yang dihasilkan sangat tinggi karena algoritma FEAL termasuk salah satu *cipher* blok dengan panjang blok 64 bit, dengan kunci 64 bit, serta memiliki iterasi 8 ronde.
3. Bahasa pemrograman Eclipse Juno digunakan untuk perancangan aplikasi penyandian pesan teks dengan algoritma FEAL dan RSA. Dalam perancangan untuk proses enkripsi dan dekripsi untuk masing-masing antarmuka menggunakan fungsi Eclipse Juno untuk string atau karakter ASCII.

## REFERENCES

- [1] S. Tjiharjadi, M.C. Wijaya, "Pengamanan Data Menggunakan Metoda Enkripsi Simetri Dengan Algoritma Feal", Seminar Nasional Aplikasi Teknologi Informasi 2009 (SNATI 2009), pp.1907-5022, 2009
- [2] A.R. Alvianto, Darmaji, "Pengaman Pengiriman Pesan Via SMS dengan Algoritma RSA Berbasis Android", Jurnal Sains Dan Seni Its, Vol. IV, pp.1, 2015
- [3] M. Arief, Fitriyani, N. Ikhsan, "Kriptografi Rsa Pada Aplikasi File Transfer Client- Server Based", Jurnal Ilmiah Teknolog informasi Terapan, Vol. I, pp.2407 – 3911, 2015
- [4] T. Firasyan, "Penggunaan Algoritma Rsa Untuk Keamanan Transaksi Online Berbasis Aplikasi Mobile", Jurusan Teknik Informatika, 2015
- [5] R.K. Hondro, "Aplikasi Enkripsi Dan Dekripsi Sms Dengan Algoritma Zig Zag Cipher Pada Mobile Phone Berbasis Android", Pelita Informatika Budi Darma, Vol. X, pp.122 – 127, 2015
- [6] B. Setiaji, "Analisis Dan Implementasi Algoritma Kriptografi Kunci Publik Rsa Dan Luc Untuk Penyandian Data", Jurnal Ilmiah DASI, Vol. XVI, pp.27 – 36, 2015
- [7] S.T.C. Kurniawan, Dedih, Supriyadi, "Implementasi Kriptografi Algoritma Rivest Shamir Adleman dengan Playfair Cipher pada Pesan Teks Berbasis Android", JOIN (Jurnal Online Informatika), Vol. II, pp.102-109, 2017
- [8] I. Alamsyah, E. Gunadhi, A.D. Supriatna, "Pengelolaan Keamanan Database Pada Data Kepegawaian ( Studi Kasus Di Pdam Tirta Intan Kabupaten Garut ), Jurnal Informatika, Vol. X, pp.1, 2013
- [9] A. Prayitno, N. Nurdin, "Analisa Dan Implementasi Kriptografi Pada Pesan Rahasia Menggunakan Algoritma Cipher Transposition", Jurnal Elektronik Sistem Informasi dan Komputer, Vol. III, pp.2477-5290, 2017
- [10] M. Syafrizal, Pengantar Jaringan Komputer, Jakarta: PT Elex Media Komputindo. 2005
- [11] S. Dian, (2017, April,27). Simbol Flowchart : Pengertian, Jenis, Fungsi Dan Contohnya [online]. Available: <https://salamadian.com/simbol-simbol-flowchart/>
- [12] Rosa A.S, and M. Shalahuddin, Rekayasa Perangkat Lunak (Terstruktur dan Berorientasi Objek), Bandung: Informatika Bandung. 2016