In Search

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

IMPLEMENTASI APLIKASI KRIPTOGRAFI BERBASIS ANDROID MENGGUNAKAN METODE SUBTITUSI DAN PERMUTASI

Deden Pradeka
Fakultas Teknologi dan Informatika, Universitas Informatika dan Bisnis Indonesia
Email : deden.pradeka@gmail.com

Abstrak

Saat ini pengiriman informasi menggunakan *smart phone* menjadi kebutuhan utama pada dunia teknologi dan informasi, tapi sedikit orang yang menyadari betapa pentingnya keamanan informasi tersebut. Banyak cara atau teknik untuk melindungi informasi atau pesan yang dikirim melalui *smart phone*, salah satunya kriptografi. Kriptografi adalah teknik atau seni untuk menyembunyikan pesan atau data, dengan cara mengubah pesan menjadi kode tertentu yang hanya dimengerti oleh pengirim dan penerima, sehingga orang yang tidak berkepentingan sulit dan membutuhkan waktu yang lama untuk memecahkan kode tersebut. Ada beberapa teknik dasar kriptografi dalam mengubah pesan menjadi kode tertentu, seperti *subtitution*, *blocking*, *permutation*, *ekspansion*, *compression,* dan yang lainnya.
Pada penelitian ini mengusulkan teknik *substitution* (subtitusi) dan *permutation* (permutasi) pada kriptografi dengan menggunakan media android, sehingga metode kriptografi ini diaplikasikan pada *smart phone.* Teknik subtitusi dan permutasi dipilih karena metodenya yang sederhana dan tingkat keamanannya kuat sehingga sangat memungkinkan di aplikasikan pada android smart phone, dimana smart phone memiliki kapasitas jauh lebih kecil dibandingkan komputer.

Kata Kunci: *Smart phone*, *subtitution*, *blocking*, *permutation*, *ekspansion*, *compression.*

Abstract

Currently sending information using smart phones is a major requirement in the world of technology and information, but few people realize the importance of information security. Many ways or techniques to protect information or messages sent via smart phones, one of which is cryptography. Cryptography is a technique or art to hide messages or data, by converting messages into certain codes that are only understood by senders and recipients, so that people who have no interest are difficult and need a long time to decode them. There are several basic cryptographic techniques in converting messages into certain codes, such as subtitution, blocking, permutation, expansion, compression, and others. In this study propose permutation (permutation) techniques on cryptography using android media, so this cryptographic method is applied to smart phones. Permutation technique was chosen because the method is simple and the security level is strong so it is very possible to apply it on an Android smart phone, where smart phones have a much smaller capacity than computers.

Keywords: *Smart phone*, *subtitution*, *blocking*, *permutation*, *ekspansion*, *compression.*

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

1.PENDAHULUAN

1.1 Latar Belakang

Informasi menjadi hal yang sangat penting untuk dilindungi. Dengan peran teknologi internet, informasi sangat mudah dikirim dan diterima antara dua orang atau lebih. Tapi sedikit orang yang peduli dengan pentingnya menjaga informasi yang sifatnya privasi.

Saat ini tukar menukar informasi sangat mudah dilakukan, seperti menggunakan telpon pintar (android). Pengembang aplikasi seluler berlomba-lomba membangun produk untuk melindungi data yang sensitive seperti kata sandi, pesan singkat, dan dokumen lainnya dengan memanfaatkan teknik kriptografi. Aplikasi tersebut biasanya tersedia di Google Play dan gratis untuk di unduh.

Berdasarkan hasil penelitian ternyata menunjukkan bahwa 87.8% aplikasi yang tersedia menyajikan beberapa jenis penyalahgunaan [1]. Dampaknya adalah informasi yang ingin dilindungi dapat dimanfaatkan orang yang tidak bertanggung jawab.

Kebutuhan untuk melindungi informasi yang bersifat privasi ini memaksa pemanfaatan kriptografi dalam membangun aplikasi yang mengelola data sensitive [2].

Kriptografi adalah seni dan ilmu matematika untuk mengubah informasi menjadi kode unik tertentu dan hanya bisa dibuka oleh pengirim dan penerima [3]. Ada berberapa teknik dasar yang digunakan dalam ilmu kriptografi, seperti subtitusi, block, permutasi, ekspansi, kompresi dan yang lainnya [4].

Subtitusi dan permutasi adalah teknik umum yang digunakan dalam kriptografi. Subtitusi merupakan teknik merubah karakter pesan menjadi kode atau symbol tertentu. Sedangkan permutasi merupakan teknik kriptografi yang mengatur ulang posisi pada pesan. Kedua teknik ini sangat sesuai diaplikasikan di dalam android, dimana android memiliki spesifikasi yang lebih kecil dibandingkan dengan komputer.

Pada penilitian ini diusulkan pengaplikasian kriptografi dengan menggunakan metode subtitusi dan permutasi pada android.

1.2 Identifikasi Masalah

Saat ini sangat sedikit aplikasi kriptografi berbasis android yang dapat dipercaya, beberapa aplikasi yang tersedia menyajikan beberapa jenis penyalahgunaan.

1.3 Rumusan Masalah

Perumusan masalah yang mendasari penelitian ini adalah bagaimana membuat aplikasi kriptografi berbasis android.

1.4 Batasan Masalah

Batasan masalah dari penelitian ini adalah aplikasi hanya dapat dijalankan pada sistem operasi seluler Android (minimal system operasi lollipop).

2.TINJAUAN PUSTAKA

2.1 Android

Android adalah system operasi seluler yang berbasis Linux [5]. Pada awalnya dikembangkan oleh startup Android.inc pada tahun 2005, kemudian Google membeli dan mengambil alih untuk dikembangkan, tujuannya Google ingin membuat gratis system pengembang Android tersebut, karena sebagian besar kode Android dirilis dibawah lisensi Apache open-source, yang berarti bahwa semua pengembang bebas mengunduh dan menggunakan sumber daya Android dengan lengkap.

Saat ini android telah rilis beberapa system operasi dari tahun 2009 sampai saat ini, dengan tampilan dan spesifikasi yang berbeda-beda, daftar bisa diliahat pada tabel 2.1.

Berdasarkan tabel Google telah merilis sebanyak 20 sistem operasi yang berbeda. Artinya Google terus mengembangkan produknya agar selalu mudah digunakan oleh para pengguna.

Tabel.2.1 Daftar rilis system operasi Android

Versi	Rilis	Kode

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

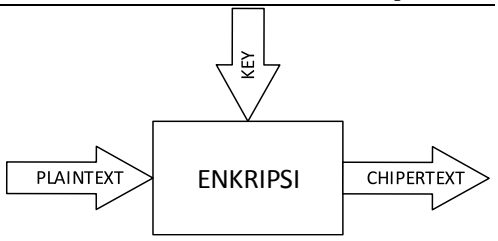
1.1	9 Feb 2009	
1.5	30 Apr 2009	Cupcake
1.6	15 Sept 2009	Donut
2.0/2.1	26 Okt 2009	Eclair
2.2	20 Mei 2010	Froyo
2.3	6 Des 2010	Gingerbread
3.0	9 Feb 2011	Honeycomb
4.0	19 Okt 2011	Ice Cream Sandwich
4.1	9 Jul 2012	Jelly Bean
4.2	13 Nov 2012	
4.3	24 Jul 2013	
4.4	31 Okt 2013	Kitkat
5.1	3 Nov 2014	Lollipop
5.2	9 Mar 2015	
6.0	5 Okt 2015	Marsmallow
7.0	22 Agst 2016	Nougat
7.1	4 Okt 2016	
8.0	21 Agst 2017	Oreo
8.1	5 Des 2017	
9.0	6 Agst 2018	Pie

2.2 Kriptografi

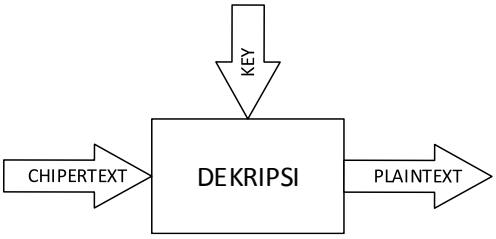
Kriptografi adalah teknik mengubah pesan menjadi kode unik [3]. Pemanfaatan kriptografi adalah untuk melindungi informasi yang sifatnya privasi dan sensitif, sehingga pengirim dan penerima saja yang boleh mengakses informasi tersebut.

Ada beberapa istilah yang digunakan pada ilmu kriptogrfi yaitu, key, plaintext, ciphertext, enkripsi, dan dekripsi. Pengertian dari plaintext adalah informasi atau pesan asli sebelum proses enkripsi yang nantinya dikirim ke penerima [3]. Kemudian ciphertext adalah informasi setelah proses enkripsi, dimana informasi sudah diubah kedalam bentuk unik [3]. Key atau kunci adalah sebuah variabel yang biasanya berbentuk angka yang berfungsi untuk mengubah pesan dari plaintext menjadi chipertext, atau sebaliknya. Kemudian yang terakhir dekripsi adalah kebalikan dari enkripsi yaitu proses mengubah ciphertext ke plaintext, sehingga penerima mendapatkan pesan asli.

Gambar 2.1 menjelaskan proses enkripsi.



Gambar 2.1 Enkripsi



Gambar 2.2 Dekripsi

Gambar 2.2 menjelaskan proses dekripsi pada kriptografi. Didalam ilmu kriptografi ada beberapa teknik dasar seperti transposisi atau permutasi, subtitusi, block cipher, expansi, pemampatan dan stream cipher [6].

2.3 Teknik Subtitusi

Subtitusi adalah salah satu teknik dasar pada ilmu kriptografi, dimana huruf pada pesan diganti dengan angka atau symbol untuk melindungi pesan tersebut [6]. Metode Caesar Chiper salah satu yang menggunakan teknik subtitusi yang sering digunakan dalam ilmu kriptografi dasar. Berikut dibawah ini langkah dari proses enkripsi dan dekripsi Caesar cipher:

1. Diketahui pengirim memiliki plaintext "JAKARTA" yang nantinya dikirim ke penerima.
2. Sebelumnya pengirim dan penerima sepakat menggunakan angka 3 sebagai kunci, kemudian penerima dan pengirim memiliki tabel hash yang berisi 26 karakter alfabet.

Tabel 2.2 Tabel Hash

A	B	C	D	E	F	..	X	Y	Z

3. Selanjutnya proses enkripsi, dari angka 3 yang sebelumnya sudah disepakati antara kedua belah pihak, kemudian tabel hash digeser sebanyak 3 kali dari kanan kekiri, dan menghasilkan urutan seperti tabel 2.3.

Tabel 2.3 Tabel Hash Setelah di Geser

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

D	E	F	G	H	I	..	A	B	C

Selanjutnya setiap karakter pada plaintext diubah menjadi J = M, A = D, K = N, A = D, R = U, T = W, dan A = D. Dibawah ini adalah persamaan dari metode chaesar chiper:

$$E_n(x) = (x + n)\ mod\ 26 \quad (1.1)$$

Dimana E_n menyatakan variabel enkripsi, x menyatakan kunci dan n menyatakan jumlah index dari karakter.

4. Melihat dari proses diatas maka plaintext "JAKARTA" diubah menjadi "MDNDUWD".

Kemudian dibawah ini dijelaskan langkah dan proses dekripsi Caesar cipher:

1. Penerima mendapatkan ciphertext "MDNDUWD".
2. Kemudian angka 3 menjadi kunci yang sudah disepakati untuk mengacak tabel hash yang berisi 26 karakter alfabet. Sehingga ciphertext "MDNDUWD" diubah menjadi "JAKARTA" sebagai plaintext atau pesan asli.

2.3 Teknik Permutasi

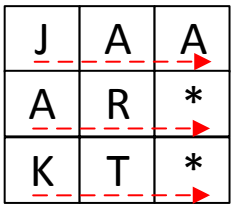
Permutasi adalah salah satu teknik dasar yang digunakan untuk mengubah plaintext ke chipertext yang umum dilakukan pada ilmu kriptografi. Teknik ini dilakukan dengan cara memindahkan setiap karakter pada plaintext [6]. Ada beberapa model kriptografi dengan teknik permutasi diantaranya segitiga, spiral, diagonal zigzag. Berikut dibawah ini langkah dari proses enkripsi dan dekripsi dengan menggunakan teknik permutasi diagonal.

1. Diketahui pengirim memiliki plaintext "JAKARTA" yang nantinya dikirim ke penerima.
2. Kita menyusun kata menjadi matrik 3*3, jika ada huruf yang kurang akan diisi dengan symbol bintang (*), kemudian kita memasukan plaintext menjadi 3 baris atau kolom secara diagonal seperti pada gambar 2.3.

J	A	A
A	R	*
K	T	*

Gambar 2.3 Kolom enkripsi matrik 3*3

3. Kemudian kita baca secara diagonal, sehingga menghasilkan chipertext "JAAAR*KT*", proses dapat dilihat pada gambar 2.4.



Gambar 2.4 Proses enkripsi

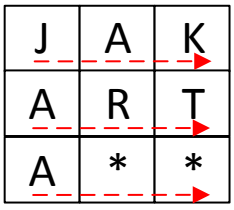
Proses dekripsi dilakukan sebaliknya, langkahnya sebagai barikut:

1. Penerima memiliki chippertext "JAAAR*KT*". Kemudian dibentuk matrik 3*3 secara diagonal, dapat dilihat pada gambar 2.5.

J	A	K
A	R	T
A	*	*

Gambar 2.5 Kolom dekripsi matrik 3*3

4. Kemudian kita baca secara diagonal, sehingga menghasilkan pesan asli "JAKARTA**", proses dapat dilihat pada gambar 2.6.



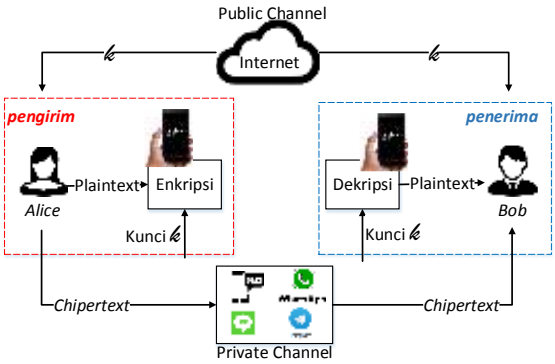
Gambar 2.6 Proses dekripsi

3. METODE PENELITIAN

Penelitian yang dilakukan adalah mengaplikasikan metode kriptografi pada Android, dengan teknik subtitusi dan permutasi yang telah dimodifikasi. Gambar 3.1 menjelaskan proses komunikasi antara pengirim dan penerima dengan menggunakan

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

metode kriptografi. Sebelumnya pengirim dan penerima menentukan kunci yang telah disepakati untuk proses enkripsi dan dekripsi.



Gambar 3.1 Desain Proses

Skenario pada gambar diatas adalah dimana Alice mengirimkan plaintext "JAKARTA" kepada Bob, sebelumnya mereka sudah sepakat menggunakan kunci 27 melalui public chanel.

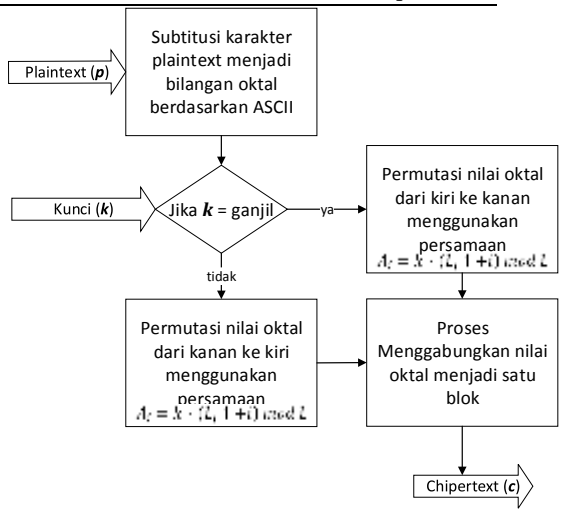
Alice akan mengenkripsi plaintext tersebut menggunakan aplikasi android menjadi kode unik atau chipertext. Kemudian alice mengirimkan chipertext melalui private chanel kepada Bob.

Pada sisi penerima Bob sudah sepakat dengan alice menggunakan kunci 27 yang iya dapatkan pada public chanel. Kemudian Bob juga sudah mendapatkan chipertext yang dikirim oleh Alice. Langkah selanjutnya penerima mendeskripsi chipertext dank unci tersebut menggunakan aplikasi di Android, sehingga Bob mendapatkan pesan asli yang dikirim oleh Ailice.

Dari skenario tersebut, penulis membuat variable ***k*** sebagai representasi dari kunci, ***p*** sebagai plaintext, dan ***c*** representasi dari chipertext.

3.1 Enkripsi

Pada bagian ini dijelaskan proses enkripsi dari metode yang diusulkan, dimana plaintext diubah menjadi chippertext menggunakan kriptografi dengan teknik subtitusi dan permutasi yang dimodifikasi.



Gambar 3.1 Desain Proses Enkripsi

Berikut ini adalah penjelasan dari langkah-langkah enkripsi dari metode yang diusulkan:

1. Pengirim memiliki variabel ***p*** = "JAKARTA", dan ***k*** = 27, dan panjang karakter ***n*** = 7. Kemudian pada proses subtitusi, setiap karakter plaintext diubah dalam bentuk bilangan octal berdasarkan ASCII (bilangan octal pada ASCII selalu menggunakan 3 digit angka), sehingga karakter berubah menjadi J = 112, A = 101, K = 113, A = 101, R = 122, T = 124, dan A = 101.
2. Langkah kedua adalah membuat nilai acak untuk permutasi menggunakan persamaan 3.1, dimana variable ***A*** sebagai penampung nilai persamaan, ***k*** sebagai nilai kunci, ***L*** sebagai panjang karakter, dan ***i*** nilai index yang bertambah sesuai panjang karakter plaintext.

$$A_i = k * (L \uparrow + i) \; mod \; L \qquad (3.1)$$

Dari persamaan diatas, maka didapatkan hasil:

$A_0 = 27 * (7 + 0) \; mod \; 7 = 0$
$A_1 = 27 * (8 + 1) \; mod \; 7 = 5$
$A_2 = 27 * (9 + 2) \; mod \; 7 = 3$
$A_3 = 27 * (10 + 3) \; mod \; 7 = 1$
$A_4 = 27 * (11 + 4) \; mod \; 7 = 6$
$A_5 = 27 * (12 + 5) \; mod \; 7 = 4$
$A_6 = 27 * (13 + 6) \; mod \; 7 = 2$

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

3. Langkah ketiga adalah melakukan proses permutasi, sebelum melakukan proses permutasi, algoritma mengecek terlebih dahulu kunci yang dikirim, jika kunci bernilai ganjil maka nilai index ke 0 atau kiri ditukar dengan index berdasarkan proses 2, dan diulang sebanyak jumlah karakter plaintext, tapi sebaliknya jika nilai kunci adalah genap maka ditukar dengan nilai index terakhir atau sebelah kanan. Misalnya, pada proses 1 kita memiliki nilai octal sebagai berikut:

index	0	1	2	3	4	5	6
oktal	112	101	113	101	122	124	101

Kemudian kita memiliki nilai $A_0 = 0, A_1 = 5, A_2 = 3, A_3 = 1, A_4 = 6, A_5 = 4, A_6 = 2$. Maka nilai oktal index ke 0 ditukar dengan index berdasar perhitungan proses 2.

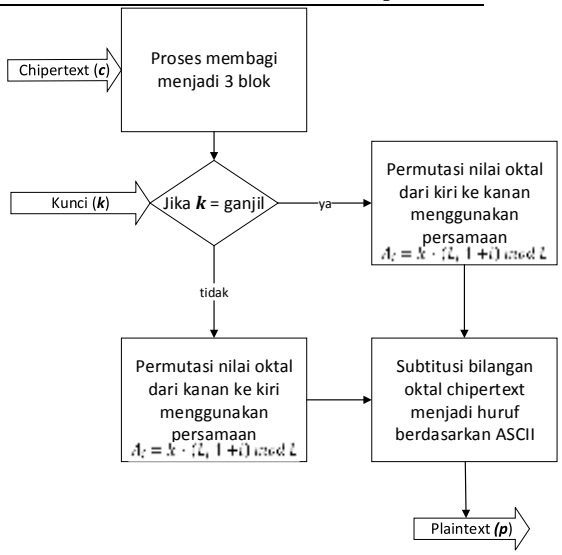
Tabel 3.1 Proses permutasi $A_0 - A_6$

index	**0**	**1**	**2**	**3**	**4**	**5**	**6**
$A_0 = 0$	112	101	113	101	122	124	101
$A_1 = 5$	124	101	113	101	122	112	101
$A_2 = 3$	101	101	113	124	122	112	101
$A_3 = 1$	101	101	113	124	122	112	101
$A_4 = 6$	101	101	113	124	122	112	101
$A_5 = 4$	122	101	113	124	101	112	101
$A_6 = 2$	113	101	122	124	101	112	101

4. Berdasarkan langkah ke tiga, maka proses selanjutnya menggabungkan nilai octal tersebut dan mengirim chipertext "1131011221241011121 01" kepada penerima menggunakan private chanel.

3.2 Dekripsi

Pada proses deskripsi pada skenarionya penerima sudah terlebih dahulu mendapatkan kunci yang sudah disepakati melalui public chanel dan chipertext melalui private chanel, dimana variabel ***c*** = "1131011221241011121 01", dan ***k*** = 27.



Gambar 3.2 Desain Proses Dekripsi

Berikut ini dijelaskan langkah-langkah dekripsi:

1. Langkah pertama adalah membagi chipertext menjadi 3 blok, untuk mendapatkan nilai octal, maka menghasilkan nilai "113 101 122 124 101 112 101".

2. Langkah kedua adalah membuat nilai acak untuk permutasi menggunakan persamaan 3.1, sehingga mendapatkan nilai $A_0 = 0, A_1 = 5, A_2 = 3, A_3 = 1, A_4 = 6, A_5 = 4, A_6 = 2$.

3. Langkah ketiga adalah melakukan proses permutasi, langkah ini sama dengan proses enkripsi, perbedaannya adalah nilai awal adalah $A_6 = 2 \ldots A_0 = 0$

Tabel 3.2 Proses permutasi $A_6 - A_0$

index	**0**	**1**	**2**	**3**	**4**	**5**	**6**
$A_6 = 2$	113	101	122	124	101	112	101
$A_5 = 4$	122	101	113	124	101	112	101
$A_4 = 6$	101	101	113	124	122	112	101
$A_3 = 1$	101	101	113	124	122	112	101
$A_2 = 3$	101	101	113	124	122	112	101
$A_1 = 5$	124	101	113	101	122	112	101
$A_0 = 0$	112	101	113	101	122	124	101

4. Berdasarkan langkah ke tiga, maka proses selanjutnya adalah subtitusi nilai octal ke huruf berdasarkan ASCII sehingga penerima mendapatkan pesan asli yaitu "JAKARTA".

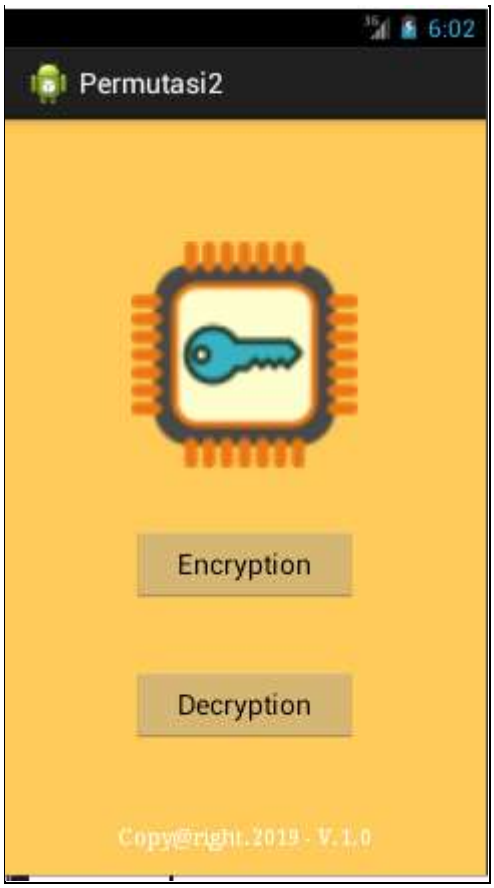
p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

4. HASIL DAN PEMBAHASAN

Berdasarkan hasil Penelitian yang dilakukan oleh penulis, maka metode kriptografi dengan menggunakan teknik subtitusi dan permutasi di implementasikan pada Android.

4.1 Tampilan Pengguna Android

Pada bagian ini menampilkan hasil aplikasi yang telah dibangun dengan menggunakan metode yang diusulkan. Pada gambar 4.1 menjelaskan tampilan awal yang menggunakan dua tombol yaitu enkripsi dan dekripsi. Jika kita mengklik tombol enkripsi maka masuk kehalaman enkripsi dan sebaliknya.



Gambar 4.1 Tampilan Utama Aplikasi

Kemudian pada gambar 4.2 memperlihatkan tampilan yang dibangun menggunakan Android untuk proses enkripsi dari sisi pengirim.

Gambar 4.2 Tampilan Enkripsi

Kemudian pada gambar 4.3 menampilkan proses dekripsi dari sisi penerima.

Dalam mengembangkanaplikasi ini, penulis menggunakan Bahasa pemograman Android dan Java. Kemudian hardware yang digunakan Personal komputer dengan spesifikasi; processor intel Core-i5-3470 dengan kecepatan 3.20 GHz, RAM 4.00 GB, dan Operasi sistemyang digunakan windows 10 (64-bit).

p-ISSN: 2085-7993
e-ISSN: 2580-3239
Volume 18 No. 01, April 2019

Gambar 4.3 Tampilan Dekripsi

5. KESIMPULAN

Berdasarkan hasil penelitian yang telah dilakukan maka metode keriptografi dengan menggunakan teknik subtitusi dan permutasi yang diterapkan pada Android dapat berkerja sesuai dengan fungsinya.

Adapun kelemahan yang terdapat pada metode yang diusulkan adalah kunci yang digunakan tidak bisa dengan angka 0 dan angka berdasarkan jumlah karakter pesan, karena jika menggunakan nilai tersebut makan pembangkit nilai acak menghasilkan nilai 0 sebanyak karakter plaintext yang digunakan.

Kedepannya kami berharap kelemahan dari metode dan aplikasi ini dapat diselesaikan dipenelitian selanjutnya.

6. REFERENSI

[1] C Alexia, N Christoforos, K Georgios, and X Christos, *Evaluation of Cryptography Usage in Android Applications*, ICST, ISBN: 978-1-63190-100-3, May 2016.

[2] M Konstantinos, N.M Raja, and G.M Mehari, *Secure and Trusted Application Execution on Embedded Devices*, ICTC, 2015.

[3] Network Associates dan Affiliated Companies, *An Introduction to Cryptography*, Version 6.5.2, 1990-1999.

[4] Henk C.A. van Tilborg, *FUNDAMENTALS OF CRYPTOLOGY A Professional Reference and Interactive Tutorial*, Dept. of Mathematics and Computing Science Eindhoven University of Technology

[5] W.M Lee, *Beginning Android Application Developtment*, Wiley Publishing, 2011

[6] Kuo Cheng-Jing, *Cryptography*, 2015