IMPLEMENTASI ALGORITMA KRIPTOGRAFI KODE CAESAR, VIGENERE, DAN TRANSPOSISI UNTUK SISTEM PROTEKSI PENGGUNAAN PESAN SINGKAT (SMS) PADA SMARTPHONE ANDROID

Damai Subimawanto[1]
Fuji Ihsani[2]
Jonathan Hindharta[3]
Melisa Chatrine Kamu[4]
Muhammad Rendianto[5]
Virgiawan Ananda Pratama[6]

Jurusan Teknik Informatika, Fakultas Teknologi Industri, Universitas Gunadarma
Jl. TB. Simatupang Kav. 38 Jakarta Selatan 12540, Indonesia
[1)]damai_subimawanto@student.gunadarma.ac.id ,[2)] ihsanifuji@gmail.com, [)] jonathanhindharta@gmail.com,[4)]melisachatrine@gmail.com,[5)]rendisigma@student.gunadarma.ac.id, [6)]virgiawanap@gmail.com

Abstrak

Pada era modernisasi saat ini, teknologi telepon selular berkembang pesat. Salah satu bentuk perkembangannya adalah dengan munculnya telepon pintar dengan sistem operasi Android yang memiliki beragam fitur menarik dan tingkat kompleksitas yang hampir sama dengan komputer. Berbagai aplikasi pengiriman pesan secara online, seperti BlackBerry Messenger dan LINE sudah banyak digunakan. Namun, salah satu fitur yang selalu ada dan masih digunakan hingga saat ini adalah SMS (Layanan Pesan Singkat). Keamanan bertukar informasi dan berkomunikasi sangat penting bagi semua orang. Untuk itu, enkripsi terhadap teks SMS perlu dilakukan untuk meningkatkan keamanan privasi pengguna dalam proses pengiriman pesan dan informasi penting. Dari berbagai teknik enkripsi yang ada, enkripsi berlapis dengan menggabungkan tiga algoritma enkripsi, yaitu Kode Caesar, Vigenere, dan Transposisi dipilih sebagai metode dalam pengamanan teks SMS. Dengan meningkatkan jumlah lapisan dan pemanfaatan kunci unik yang digunakan dalam proses enkripsi dan dekripsi diharapkan mampu mengurangi jumlah penyadapan teks SMS yang sering terjadi saat ini.

Kata Kunci: *dekripsi, enkripsi, kode caesar, transposisi, vigenere.*

PENDAHULUAN

Telepon seluler merupakan alat komunikasi yang umum digunakan pada saat ini. Zaman semakin berkembang, begitu pula dengan kegunaan telepon seluler tersebut. Salah satu fungsi utama telepon seluler yang sejak dahulu tidak pernah ditinggalkan adalah untuk berkirim

pesan singkat. Pesan singkat tersebut dikirimkan dalam bentuk teks yang dikenal sebagai Layanan Pesan Singkat (SMS). Keuntungan pemanfaatan fasilitas SMS dibandingkan dengan fasilitas bertukar pesan seperti layanan pesan sosial adalah SMS tidak memerlukan koneksi Internet dan dengan begitu mudahnya dapat digunakan untuk saling bertukar informasi tanpa batasan jarak dalam waktu yang lebih cepat. Celah keamanan terbesar pada komunikasi via SMS adalah pesan yang dikirimkan akan disimpan di SMSC (Pusat Layanan Pesan Singkat), yaitu tempat dimana SMS disimpan sebelum dikirim ke tujuan. Pesan yang sifatnya teks biasa ini dapat disadap oleh siapa saja yang berhasil memiliki akses ke dalam SMSC. Akibatnya, informasi penting seperti kode sandi, nomor PIN, ataupun jadwal pertemuan orang-orang penting dapat dibaca oleh orang lain yang tidak berhak mengetahuinya. Dengan demikian perlu adanya solusi untuk pengamanan data SMS menggunakan metode enkripsi data yang telah dikenal dan digunakan, dengan pengimplementasi annya yang berlapis-lapis untuk memperkuat hasil enkripsi.

Rumusan masalah dalam penelitian ini adalah bagaimana mengimplementasikan metode enkripsi dan dekripsi SMS dalam bentuk aplikasi mobile berbasis Android menggunakan metode Kode Caesar (Geser), Vigenere, dan Transposisi. Adapun batasan masalah yang digunakan pada penelitian ini, antara lain: 1) Menerapkan metode enkripsi tiga lapis, yaitu teknik Kode Caesar (Geser), Vigenere, dan Transposisi, 2) Masukan berupa pesan SMS, 3) SMS menggunakan tiga metode enkripsi dengan satu kunci yang sama untuk tiap satu SMS, 4) Kunci yang dikirimkan sama dengan kunci yang diterima sehingga pengirim dan penerima SMS dapat menerima pesan yang sesuai, 5) Hanya alfabet dan numerik yang akan dienkripsi, dengan ketentuan hasil enkripsi tidak membaca serta mengenkripsi spasi dan karakter lain, dan 6) Spesifikasi SMS (panjang 1 pesan SMS) disesuaikan dengan standar teknologi Sistem Global untuk Perangkat Komunikasi (GSM).

METODE PENELITIAN

Pada penelitian ini metode yang digunakan dalam membagun aplikasi adalah Waterfall. Menurut Pressman (Pressman, 2001), Waterfall adalah model klasik yang bersifat sistematis, berurutan dalam membangun perangkat lunak. Fase-fase dalam model Waterfall menurut Pressman adalah tahapan antara komunikasi, rancangan, pemodelan, konstruksi, penyebaran.

Berikut adalah tahapan Waterfall yang dilakukan dalam penelitian ini :

Komunikasi
Menganalisa kebutuhan dari perangkat lunak dan telaah pustaka dari berbagai sumber mengenai algoritma yang digunakan untuk mengenkripsi SMS.

Rancangan
Melakukan perencanaan bagaimana nantinya pe rangkat lunak dapat berkerja dengan baik sehingga pengguna dapat dengan mudah menggunakannya.

Pemodelan
Pada tahap ini dilakukan perancangan berdasarkan pe rencanaan yang telah dilakukan sebelumnya dengan menggunakan diagram alur, di mana akan dijelaskan alur dari masing-masing algoritma yang digunakan untuk mengenkripsi SMS.

Penyebaran

Pada tahap ini dilakukan implementasi dari perancangan yang telah dibuat ke dalam aplikasi Android dengan menggunakan ADT dari Eclipse.

HASIL DAN PEMBAHASAN

Pada penulisan ini pembuatan aplikasi enkripsi SMS berbasis Android yang dilakukan dengan meng gunakan 3 algoritma kriptografi dengan alur sebagai berikut (Caroline, 2011), pertama teks dienkripsi menggunakan algoritma Kode Caesar, kemudian dilanjutkan menggunakan algoritma Vigenere, dan terakhir dienkripsi menggunakan algoritma Transposisi, sedangkan untuk proses dekripsi dilakukan proses dengan urutan sebaliknya. Dalam penggunaan ketiga algoritma aplikasi ini dibutuhkan sebuah kata kunci. Kunci ditentukan sendiri oleh pengguna yang mana untuk melakukan enkripsi dan dekripsi harus menggunakan kunci yang sama (Sasongko, 2005). Oleh karena itu, kedua belah pihak pengguna harus sepakat untuk menggunakan kata kunci apa yang diinginkan, bisa dengan cara bertatap muka langsung dan sepakat menentukan kata kunci, ataupun dengan cara menggunakan media lain. Isi dari kata kunci digunakan dalam algoritma Vigenere, sedangkan jumlah karakter dari kata kunci digunakan untuk menentukan banyaknya langkah pergeseran dari Kode Caesar dan digunakan sebagai angka pembagi dalam algoritma Transposisi. Penjelasan mengenai ketiga algoritma tersebut adalah sebagai berikut :

Algorima Kode Caesar

- Seperti terlihat pada gambar 1 (kiri), berikut ini adalah penjelasan alur enkripsi untuk algoritma Kode Caesar yang digunakan dalam pembuatan aplikasi enkripsi SMS
- Program membuat variabel pengubah (A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #) sebagai
- pengubah karakter-karakter pada teks biasa menjadi teks cipher 1.

Program mengambil jumlah karakter dari kata kunci sebagai penentu banyaknya pergeseran masing-masing karakter teks biasa.

- Program mengubah masing-masing karakter teks biasa dengan menggesernya sebanyak variabel pengubah sesuai jumlah karakter kunci.
- Proses kerja variabel pengubah pada program ini dapat dilakukan secara manual dengan melakukan pergeseran karakter, seperti contoh pada tabel 1 (disebut juga dengan konsep ROT_5).
- Program menghasilkan teks cipher 1.

ROT5

Pi	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#
Key	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	*	#	0	1	2	3	4	5	6	7	8	9	A	B	C	D	E

Tabel 1. Tabel pergeseran karakter dengan ROT_5

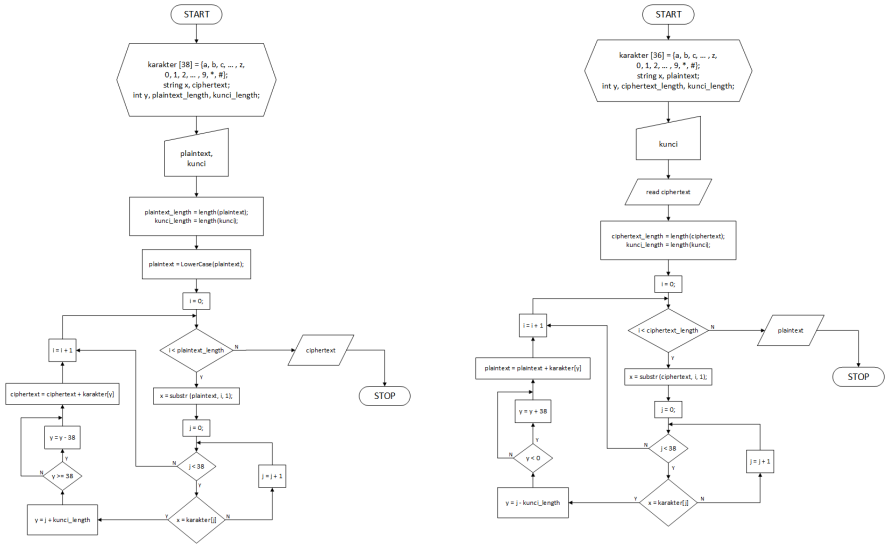
Algoritma Vigenere

Seperti terlihat pada gambar 2 (kiri), berikut ini adalah penjelasan alur

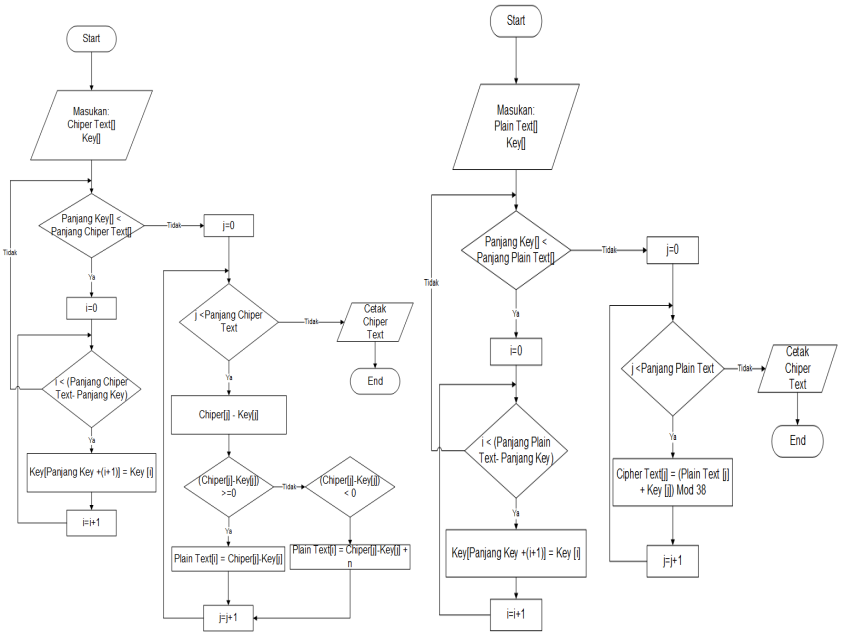
enkripsi untuk algoritma Vigenere yang digunakan dalam pembuatan aplikasi enkripsi SMS : (Arjana, 2012)

- Program membuat variabel pengubah (A, B, C, D, E, F, G, H, I, J, K, L, M, N, O, P, Q, R, S, T, U, V, W, X, Y, Z, 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #) dengan menjadikannya nilai integer sebagai perwakilan masing-masing indeks karakter (1, 2, 3, …, 38).
- Program mengambil kunci yang dimasukkan dan menjadikan kunci tersebut sebagai pembentuk teks cipher 2 dari masukan yang berupa teks cipher 1.
- Program membuat formula c(‘chip[i]’) = (‘chip[i]’ + ‘kunci[i]’) mod 38. Variabel chip[i] merupakan karakter-karakter dari teks cipher 1, variabel kunci[i] merupakan karakter-karakter pada kunci yang dimasukkan, dan variabel c(‘chip[i]’) merupakan karakter-karakter yang tercipta dari penjumlahan indeks karakter-karakter teks cipher 1 dengan kunci.
- Formula pada program dapat dilakukan secara manual dengan melakukan persilangan pada tabel 2.
- Program menghasilkan teks cipher 2.

Untuk proses dekripsi, dapat dilihat pada gambar 2 (kanan).



Gambar 1. Diagram alur proses enkripsi (kiri) dan dekripsi (kanan) menggunakan Kode Caesar



Gambar 2. Diagram alur proses enkripsi (kiri) dan dekripsi (kanan) menggunakan Vigenere

Algoritma Transposisi

Seperti terlihat pada gambar 3, berikut ini adalah penjelasan alur enkripsi untuk algoritma transposisi yang digunakan dalam pembuatan aplikasi enkripsi SMS :

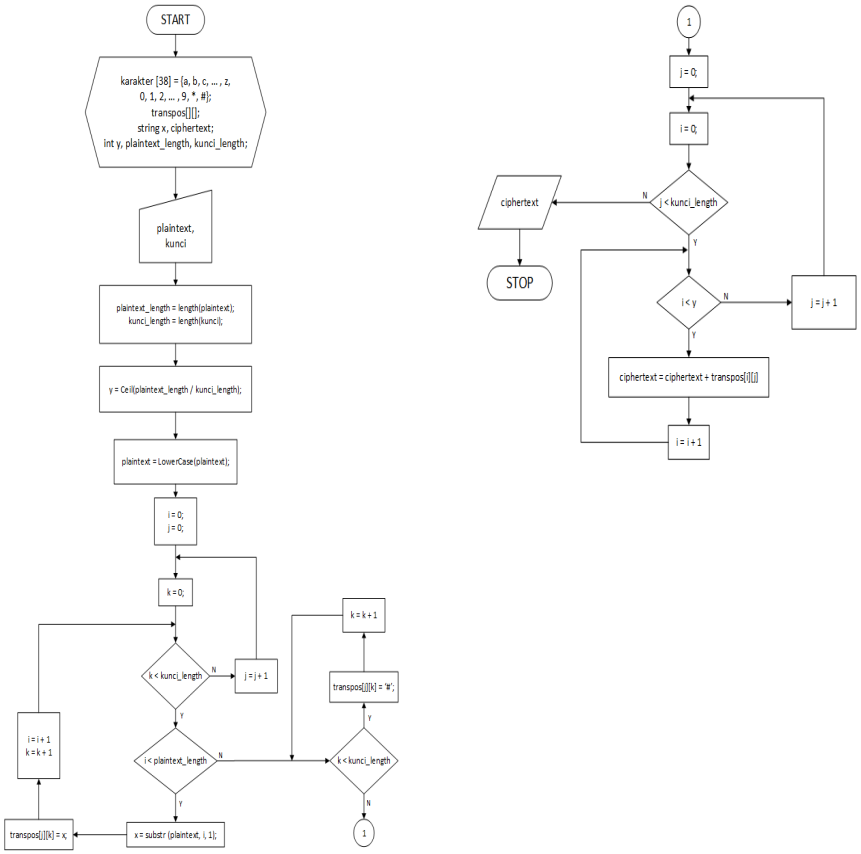
- Program menghitung jumlah karakter kunci yang dimasukkan oleh pengirim sebagai penentu jumlah karakter dalam sebaris saat akan melakukan transposisi.
- Program menghitung jumlah karakter teks cipher 2 dan memotongnya sebanyak jumlah karakter kunci yang telah dilakukan sebelumnya, sehingga terbentuk matriks baris dan kolom.
- Program menambahkan karakter '#' sebagai perwakilan karakter kosong/sisa (jika ada) pada matriks, sehingga karakter-karakter memenuhi ruang baris dan kolom.
- Program membaca teks secara vertikal dimulai dari kolom pertama hingga kolom terakhir secara berurutan, dan memodelkannya dalam 1 baris.
- Proses kerja program ini dapat dicontohkan seperti tabel 3 (dengan jumlah karakter kunci sebanyak 5 dan teks "SARMAG*TI*2010").
- Program menghasilkan teks cipher 3, yaitu "SAI1AG*0R*2#MT0#".
- Untuk proses dekripsi, dapat dilihat pada gambar 4

Tabel 2. Tabel Persilangan Karakter

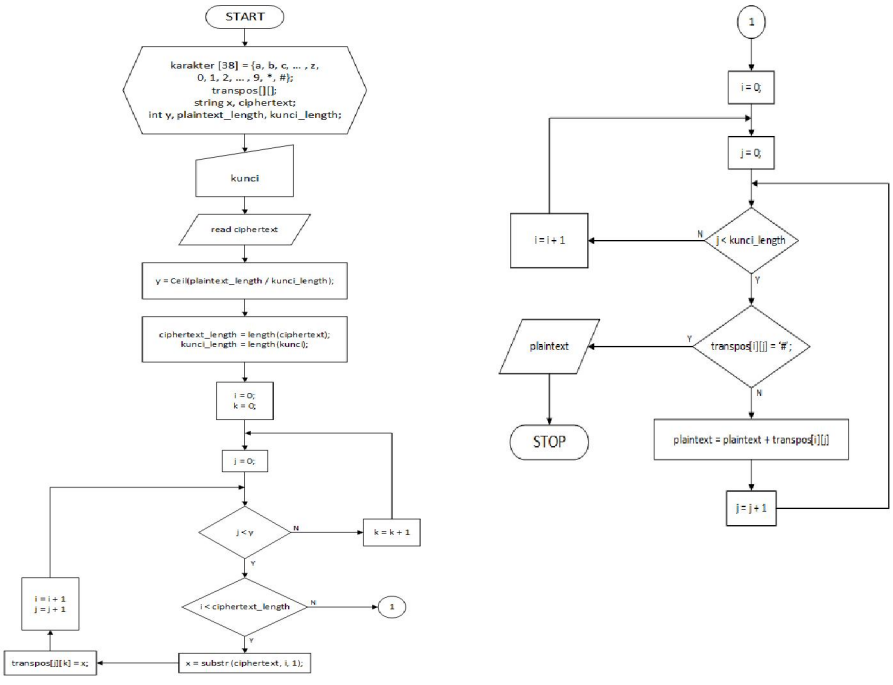
	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#
a	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#
b	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A
c	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B
d	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C
e	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D
f	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E
g	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F
h	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G
i	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H
j	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I
k	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J
l	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K
m	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L
n	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M
o	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N
p	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
q	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
r	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
s	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
t	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
u	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
v	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
w	W	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
x	X	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
y	Y	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
z	Z	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
0	0	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
1	1	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0
2	2	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1
3	3	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2
4	4	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3
5	5	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4
6	6	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5
7	7	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6
8	8	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7
9	9	*	#	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	0	1	2	3	4	5	6	7	8

Tabel 3. Penggambaran Proses Transposisi

S	A	R	M
A	G	*	T
I	*	2	0
1	0	#	#

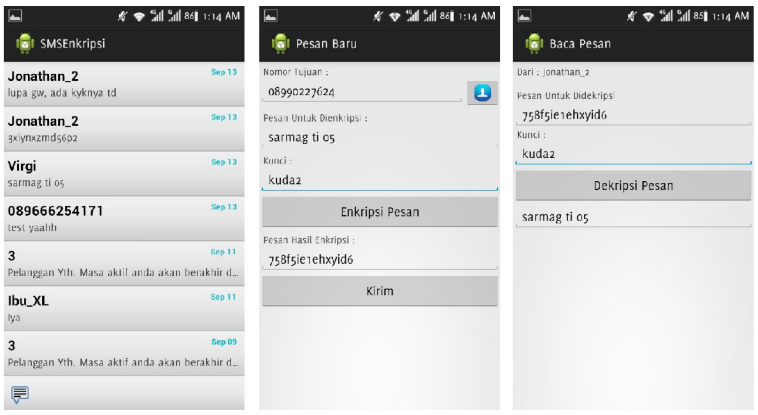


Gambar 3. Diagram alur untuk proses enkripsi menggunakan Transposisi



Gambar 4. Diagram alur untuk proses dekripsi menggunakan Transposisi

Tampilan Aplikasi



Gambar 5. Tampilan Aplikasi

SIMPULAN DAN SARAN

Kesimpulan

Pembuatan aplikasi ini ditujukan untuk mem proteksi pertukaran data SMS dengan menggunakan algoritma kriptografi berlapis yang diimplemen tasikan pada perangkat Android. Algoritma kriptografi yang digunakan adalah sebanyak 3 lapis berurut, yaitu algoritma Kode Caesar, algoritma Vigenere dan algoritma Transposisi.

Dibutuhkan kata kunci dalam penggunaan ketiga algorima tersebut. Kata kunci tersebut harus sama untuk proses enkripsi dan dekripsi, sehingga kedua pihak pengguna harus sepakat memilih kata kunci yang diinginkan. Isi dari kata kunci digunakan dalam algoritma Vigenere, sedangkan jumlah karakter dari kata kunci digunakan untuk menentukan banyaknya langkah pergeseran dari Kode Caesar dan digunakan sebagai angka pembagi dalam algoritma Transposisi.

Proses enkripsi teks melalui tiga lapis algoritma, yaitu langkah pertama adalah teks biasa dienkripsi menggunakan Kode Caesar yang akan menghasilkan teks cipher 1, dilanjutkan dengan menggunakan algorima Vigenere yang akan menghasilkan teks cipher 2 dan terakhir teks cipher 2 tersebut akan dienkripsi menggunakan algoritma Transposisi yang menghasilkan teks cipher 3 atau teks cipher utama. Untuk proses dekripsinya, dilakukan proses algoritma dekripsi dengan urutan secara terbalik dari proses enkripsi, yaitu dengan urutan algoritma Transposisi, Vigenere, dan Kode Caesar.

Saran

Pengembangan aplikasi ini diharapkan tidak hanya mampu untuk mengirimkan pesan berupa karakter teks saja, namun juga diharapkan mampu melakukan pengiriman pesan berupa gambar, audio, maupun video dengan menggunakan algoritma yang telah diimplementasi dalam program ini, sehingga pengguna dapat lebih leluasa dalam menggunakan aplikasi ini.

DAFTAR PUSTAKA

Arjana, P. H., Dkk. 2012. "*Implementasi Enkripsi Data dengan Algoritma Vigenere Cipher.*" Seminar Nasional Teknologi Informasi dan Komunikasi 2012 (SENTIKA 2012).

Caroline, M. L. 2011. "*Metode Enkripsi Baru: Triple Transposition Vigènere Cipher."* Makalah IF3058 Kriptografi – Sem. II Tahun 2010/2011. Bandung.

Pressman, R. S. 2001. "*Software Engineering : A Practitioner's Approach*." McGraw-Hill. New York.

Sasongko, J. 2005. "*Pengamanan Data Informasi Menggunakan Kriptografi Klasik.*" Jurnal Teknologi Informasi DINAMIK, volume X.