ENKRIPSI SMS PADA *SMARTPHONE* BERBASIS ANDROID DENGAN METODE VIGENERE DAN TRANSPOSISI KOLOM

Shaom Shabara[1], Solichul Huda[2]
[1,] Jurusan Teknik Informatika, Fakultas Ilmu Komputer, Universitas Dian Nuswantoro
Jl. Imam Bonjol No. 205-207,Semarang, 50131, (024) 3517261
E-mail : shaombara@gmail.com[1], huda3171gmail.com[2]

Abstrak

Perangkat mobile saat ini yang disebut dengan smartphone memiliki fitur dari teknologi terbaru untuk menjalankan berbagai fungsi layaknya sebuah komputer biasanya. Fasilitas standar smartphone untuk mengirimkan informasi berupa pesan singkat adalah fasilitas Short Message Service (SMS), namun timbul pertanyaan mengenai keamanan informasi jika seseorang ingin mengirimkan suatu pesan melalui fasilitas ini. Oleh karena itu, penulis memutuskan untuk melakukan penelitian tentang algoritma kriptografi Vigenere dan Transposisi Kolom terhadap pesan yang akan dikirimkan.

***Kata Kunci** : enkripsi, dekripsi, SMS, kriptografi, vigenere, transposisi kolom, smartphone android*

Abstract

Todays mobileware called by smartphone has a feature from latest technologi to run anyfunction like a general computer. Smartphone standard facility to send information like short massage is short message service (SMS), but a question risen up about information secureness if someone want to send a message using this facility. Therefore, author decide to do a research about vigenere cryptography algorithm and column transposition to message which sent.

***Keywords:** encryption, decryption, SMS, cryptography, vigenere, column transposition, android smartphone*

1. PENDAHULUAN

Perangkat mobile saat ini yang disebut dengan smartphone memiliki fitur dari teknologi terbaru untuk menjalankan berbagai fungsi layaknya sebuah komputer biasanya, menjadi alasan utama kenapa teknologi smartphone menjadi lebih diminati[1]. Salahsatu sistem yang saat ini populer digunakan pada perangkat smartphone adalah Android[1].

Beberapa fasilitas standar yang disediakan smartphone untuk berkomunikasi pada dasarnya sama dengan ponsel biasa, salah satunya adalah fasilitas untuk mengirimkan informasi berupa pesan singkat melalui *Short Message Service* (SMS). Fasislitas SMS pada umumnya sangat dominan digunakan oleh pengguna untuk mengirimkan sebuah informasi, karena sangat mudah dan dengan harga yang murah. Namun dengan fasilitas SMS yang ada, membuat peluang adanya ancaman terhadap pengubahan dan pencurian pesan[11].

Masalah keamanan, menjadi isu penting pada era teknologi informasi ini. Pelaku kejahatan memanfaatkan celah keamanan yang ada untuk dimasuki dan melakukan manipulasi [4]. Banyak celah keamanan pada fasilitas SMS ini, diantaranya adalah orang lain yang membaca pesan tersebut, dan penyadapan pesan yang tersimpan pada Service center saat melakukan pengiriman pesan. Maka dari itu dalam penelitian ini diambil judul "Enkripsi Sms Pada Smartphone Berbasis

Android Dengan Metode Vigenere Dan Transposisi Kolom".

Beberapa penelitian terkait dengan pembuatan karya ilmiah ini salah satunya penelitian yang dibuat oleh Defni, Indri Rahmayun, dalam penelitiannya telah dikembangkan enkripsi sms dengan metode RC6 yang diimplementasikan pada smartphone berbasis android.

Penulis mencoba untuk mengimplementasikan metode lain dari penelitian sebelumya, yaitu menggunakan metode vigenere dan transposisi kolom. Dengan menggabungkan dua metode, akan menambah tingkat kerumitan enkripsi pesan, sehingga pesan dapat tersandikan dengan baik.

2. TINJAUAN PUSTAKA

2.1 Android

Android adalah sistem operasi berbasis Linux yang dirancang untuk perangkat seluler layar sentuh seperti telepon pintar dan komputer tablet[5]. Android berjalan didalam *Dalvik Virtual Machine* (DVM) bukan di *Java Virtual Machine* (JVM), sebenarnya banyak persamaannya dengan Java virtual machine, seperti Java ME (*Java Mobile Edition*), tetapi Android menggunakan *Virtual Machine* sendiri yang dikustomisasi dan dirancang untuk memastikan bahwa beberapa feature-feature berjalan lebih efisien pada perangkat mobile[5].

2.2 SMS(*Short Message Service*)

Short Message Service atau biasa disingkat SMS merupakan sebuah layanan yang banyak diaplikasikan pada sistem komunikasi tanpa kabel, memungkinkan dilakukannya pengiriman pesan dalam bentuk alphanumeric antara terminal pelanggan[7].

Aplikasi SMS merupakan aplikasi yang paling banyak peminat dan penggunanya. Sifat transmisi SMS yang merupakan short burst membuat jenis aplikasi yang memanfaatkan SMS biasanya berupa aplikasi pengiriman data yang ringkas dan pendek[6]. Sifat perangkat SMS yang mobile dan dapat mengirimkan informasi dari mana saja selama masih dalam cakupan layanan operator, memunculkan aplikasi lapangan dimana informasi-informasi yang dikumpulkan dari lapangan dikirim secara berkala kepada pusat pengolahan informasi[7].

Saat kita menerima pesan SMS dari *smartphone*, pesan tersebut tidak langsung dikirimkan ke *smartphone* e tujuan, akan tetapi dikirim terlebih dahulu ke SMS *Center* (SMSC) yang biasanya berada di kantor operator telepon, baru kemudian pesan tersebut diteruskan ke handphone tujuan[7].

2.3 Sandi Ceasar

Sandi ceasar merupakan sistem persandian klasik berbasis subtitusi yang sederhana[4]. Enkripsi dan dekripsi pada sistem persandian ceasar menggunakan operasi *shift*[4].

Operasi shift adalah mensubtitusi suatu huruf menjadi menjadi huruf pada daftar alfabet disebelah kanan atau sebelah kiri huruf itu[4].

Sandi ceasar juga disebut dengan algoritma ROT3 karena menggantikan posisi huruf awal dari alfabet[3]. Jika penggeseran yang dilakukan sebanyak 3 kali maka kunci dekripsinya adalah 3 [3].

Misalkan, kita akan mengenkripsi kata 'UDINUS' dengan penggeseran kunci 3, Maka hasilnya adalah "XGLQXV".

Sandi caesar dapat dipecahkan dengan cara brute force attact, suatu bentuk serangan yang dilakukan dengan mencoba coba berbagai kemungkinan untuk menemukan kunci[3].

2.4 Sandi *Vigenere*

Vigenere Chiper adalah salah satu jenis kriptografi klasik yang dasarnya melakukan subtitusi cipher abjad

majemuk(polyalphabetic subtitution)[3]. Metode ini pertama kali dipublikasikan oleh seseorang diplomat prancis, Blaise de Vigenere pada abad ke-16, tepatnya pada tahun 1586[3].
Vigenere merupakan pemicu perang sipil di Amerika dan kode vigenere digunakan oleh tentara Konfiderasi pada Perang Sipil Amerika[3]. Kode vigenere berhasil dipecahkan oleh Babbage dan Kasiski pada pertengahan Abad 19[3].
Ide dasarnya sama dengan Caesar Chiper dalam metode enkripsinya, perbedaannya jika pada Caesar Chiper setiap huruf digeser sebanyak 1 huruf yang sama(sesuai konstanta nilai pergeseran) sedangkan pada Vigenere huruf setiap huruf pesan asli digeser sebanyak satu huruf pada kuncinya. Proses penyandian dapat menggunakan bujur sangkar vigenere yang dirumuskan dengan :
$(P + K) \bmod 26 = C$
P adalah plaintext,
K adalah kunci,
C adalah ciphertext.

3. METODE

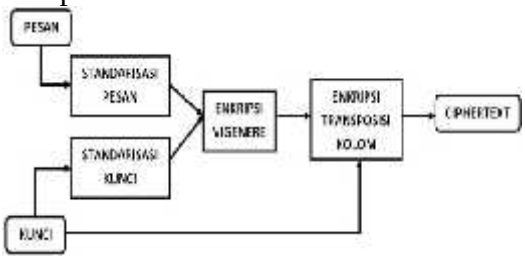
Dalam melakukan penelitian diperlukan metode penelitian, dalam metode tersebut dilakukan beberapa tahapan untuk mendapatkan hasil yang baik. Sehingga penelitian ini dapat berjalan dengan lancar.

3.1 Pengumpulan Data

Proses pengumpulan data yaitu proses atau cara yang dilakukan oleh penulis untuk menginginkan data-data yang dibutuhkan. Peneliti menyebarkan quisioner pada beberapa mahasiswa di Universitas Dian Nuswantoro Semarang. Disini peneliti mendapatkan data berupa pesan SMS.

3.2 Enkripsi

Enkripsi berguna sebagai proses untuk mengubah pesan asli menjadi pesan yang tersandikan. Enkripsi ini menggunakan metode vigenere dan transposisi kolom.



Gambar 3.1 proses enkripsi

3.2.1 Standarisasi pesan(*plaintext*)

Standarisasi pesan disini berfungsi untuk menstandarkan pesan masukan menjadi *hexadesimal*.

3.2.2 Standarisasi kunci

Standarisasi kunci dilakukan untuk membangkitkan huruf dari kunci masukan, sehingga tidak terjadi perulangan kunci. Standarisasi kunci ini menggunakan teknik *Ceasar* dengan *shift* yang diperoleh dari panjang kunci.

3.2.3 Enkripsi Vigenere

Proses ini merupakan penyandian pesan dengan kunci masukan yang sudah distandarisasikan, dengan metode Vigenere. Enkripsi dengan algoritma Vigenere dapat dirumuskan sebagai $(P + K) \bmod 43 = C$, dimana P adalah plaintext, K adalah kunci, dan C adalah ciphertext.

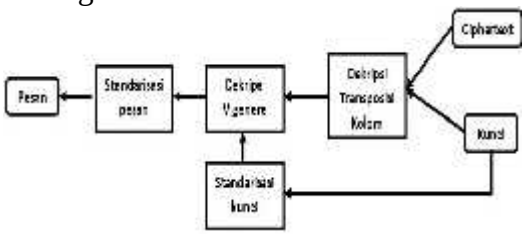
3.2.4 Enkripsi Transposisi Kolom

Pada tahap ini ciphertext yang dihasilkan dari enkripsi Vigenere akan dienkripsi lagi dengan metode Transposisi Kolom. Enkripsi Transposisi Kolom yaitu dengan cara menuliskan pesan asli(plainteks) secara baris (biasa) dengan panjang yang telah ditentukan sebagai kunci-nya. Teks sandi-nya dibaca secara kolom demi kolom dengan pengacakan melalui permutasian angka kuncinya.

3.3 Dekripsi

Pada proses ini berfungsi untuk mengubah pesan yang tersandikan (ciphertext) menjadi pesan alsi (plaintext). Proses dekripsi

menggunakan metode transposisi kolom dan vigenere.



Gambar 3.2 proses dekripsi

3.3.1 Dekripsi Transposisi Kolom

Pada tahap ini ciphertext akan didekripsi dengan metode transposisi kolom. Proses ini dilakukan dengan cara menuliskan beberapa karakter ciphertext pada tiap kolom karakter kunci. Untuk mencari berapa karakter yang harus di tulis pada setiap kolomnya, yaitu dengan cara membagi panjang ciphertext dengan panjang kunci. Setelah semua kolom kunci terisi karakter ciphertext, baru plaintext ditulis secara baris.

3.2.2. Standarisasi Kunci

Standarisasi kunci dilakukan untuk membangkitkan huruf dari kunci masukan. Proses ini sama dengan standarisasi kunci pada proses enkripsi, yaitu menggunakan pergeseran dengan teknik ceasar dengan shift.

3.3.2 Dekripsi Vigenere

Pada tahap ini, plaintext dari hasil dekripsi transposisi kolom akan didekripsi lagi dengan kunci masukan menggunakan metode vigenere. Proses dekripsi bisa menggunakan bujur sangkar vigenere yang dirumuskan ($K + P$) mod 43 = C, dimana P adalah plaintext, K adalah kunci, dan C adalah ciphertext.

3.3.3 Standarisasi Pesan

Pada tahap standarisasi pesan, akan menstandarkan pesan yang berformat unicode hexadesimal menjadi karakter.

4. HASIL DAN PEMBAHASAN

4.1 Hasil Eksperimen

Pengujian program ini dimaksudkan untuk mendapatkan hasil eksperimen dari beberapa pengujian terhadap pesan SMS. Pengujian ini menggunakan data yang sudah dikumpulkan penulis. Dari data pesan yang sudah diambil tadi kemudian diinputkan dalam program yang sudah dibuat sebelumnya lalu akan mendapatkan hasil berupa ciphertext dan dikirimkan ke nomer tujuan.

Sebelum melakukan pengujian aplikasi ini, penenulis menyiapkan dua *Smartphone*. *Smartphone* yang digunakan untuk pengujian aplikasi adalah samsung galaxy young2 dengan nomer Sam: “0989652601794” dan andromax c2(dual sim)dengan nomer Andro: “088215313502”. Dua smartphone tersebut digunakan sebagai pengirim pesan maupun penerima pesan.

Berikut adalah 20 data pesan SMS yang diujikan dalam program beserta hasil yang didapatkan dalam program :

Tabel 4.1: Hasil Eksperimen

No	Pesan Sms	Key	Enkripsi	dari	ke	dekripsi
1	Ryan besuk kuliah jam 13.30 di gedung A	Satu	CFIRVU3;>KRC0JRR04:8X22:?>GJNRVWZ4;;CHKM037<?CGKKSSX14<fDHHg3C49LPUGJORY23fBCXGg	Andro	Sam	Ryan besuk kuliah jam 13.30 di gedung A
2	Posisi dimana bos?	Satu	AHLMZVZ49X376>BFJOZ37;?CCKLf7;:NSB15	Sam	andro	Posisi dimana bos?
3	Gimana kabarnya pak?	Satu	HY3MRVC36LW266>BFJORZ37;?DHGOP3Z3H<fKFK9	Andro	Sam	Gimana kabarnya pak?
4	Sayang lagi apa?	Satu	DN3MR3Z3X366>BFJZ37;??HHVZ9I	Sam	andr	Sayang lagi apa?

			A>B1		o	
5	Bawain minuman dari indomaret	Satu	CLRMZZZ27CGFZLRW366>CFFNRVZ38<Z37;?CGKPOW048gVZGJORWJLN<A08g	Andro	Sam	Bawain minuman dari indomaret
6	Semoga dirimu akan selalu teringat padaku	Satu	DYPMZ3337:CCKNP<WZ48@X266>BGJNNVZ48<?CCKOTZ37;fCCKOTW008<fEILPgZD3:<RBX4Q:>Z8@BCCK2g	Sam	andro	Semoga dirimu akan selalu teringat padaku
7	Kamu ini kenapa, orang kok nyontekan!	Satu	SYI7QZZ36<SB1JW<00W22::BFJJSVV33<?CGZ47;?CHGOSW048<ADHV3;?LSBY5OY=AHM?QX	Andro	Sam	Kamu ini kenapa, orang kok nyontekan!
8	Aku masuk lewat pitu belakang ya	Satu	BJ2P8=566>>GGKU0W36;>BGKOSRZ37;fZZ7<;CGGOTW0488f<Y3;:CCFSST>AH7<	Sam	andro	Aku masuk lewat pitu belakang ya
9	Besuk berangkat jam berapa?	Satu	CH0OS?f6GNfDF5W36:?BFKNRV044Z43;?CGGOOW04gZ32;;ECFKNWW0g	Andro	Sam	Besuk berangkat jam berapa?
10	Selamat menempuh hidup Baru.	Satu	DX2Q:?B76CCBGOX26;>BFKJRWV38Z377?CHKOSXY54ZZ36?CBNRRRX1H	Sam	andro	Selamat menempuh hidup Baru.
11	Terserah kamu aja	Satu	EGNNQV337X36::BGJNZ48;?CCKgZ14>LRBWg	Andro	Sam	Terserah kamu aja
12	Ilham kenapa tidak berangkat???	Satu	JM24;UY;7:CCMK9=W26:>CBJNNVZ378<Z33;?CHKOSX0499g=Z2;;?FJ1PTfA7Mg	Sam	andro	Ilham kenapa tidak berangkat???
13	To thine own self be true	Satu	EEQ7Q1Y7<<>DKXY6::CBJNRR03Z47;?CHKKSX1gf2;;PSEYJSV0g	Andro	Sam	To thine own self be true
14	Semangat kaka	Satu	DY3NQVZX26::BFZ37<?CgZZ9:LPg	Sam	andro	Semangat kaka
15	Good luck	Satu	H0IR8W22;>Z37;gf2E9g	Andro	Sam	Good luck
16	Bismillah uas	Satu	CHR5YZ1W36:>CGZ37;;Cg3BE7:?g	Sam	andro	Bismillah uas
17	Ujian loh ham	Satu	FN35Y2BX26:>BFZ33;;Cg;Z2L:?g	Andro	Sam	Ujian loh ham
18	Semoga dirimu Selalu akan teringat padaku. Aku mah apah atuh? Gua mah gitu orangnya. diduain gapapa. diselingkuhin gapapa.	Satu	DYPMZ335IM>T0NP<WZ48f?UGLOS419NCAXPSTTZFJ:=JJRMRVZ2??GIKSNSW0X266>BGINRRZ38<?CCKOTS0088ADHMMRX159>=FIMQQY366>BFFNRVZ477?CGZ37;fCCKOTW008<fEILPPV259=AAJMMVU22:?BFJONVZ37;fDCKPSW048<AEDZD	Sam	andro	Semoga dirimu Selalu akan teringat padaku. Aku mah apah atuh? Gua mah gitu orangnya. diduain gapapa. diselingkuhin gapapa.

			3:<RBKKSSWZ8fBCCK29T1D<9=fHPLUTY1>>SBLR7UYZG=:>WJM6<=7H>;?X			
19	Semangat...	Satu	DY3N;?X26::>Z37<;gZZ9:Og	Andro	Sam	Semangat...
20	Tugasku rung bar : (kp. Animasi 3d. Dkv IV : (	Satu	ELLRS?Y36:>BF47UV33I;ETOX27;?BBJJNR0Z7;f?GGOOVX00377fCGLLOWW28<fADJQRTXgZZD6?EDH0V9f0<8DBXKQXSWg	Sam	andro	Tugasku rung bar : (kp. Animasi 3d. Dkv IV : (

Dari hasil eksperimen di atas menunjukan bahwa pesan yang dienkripsi dan dikirimkan kenomer tujuan dapat di dekripsi kembali, sehingga penerima pesan dapat mengerti informasi pesan dari ciphertext yang diterima.

4.2 Pengujian

Setelah dilakukan uji enkripsi dan dekripsi pesan, kemudian ciphertext hasil dari aplikasi akan di uji pecahkan dengan teknik *vigenere analysis* dan *brute force attack*, dan dibandingkan dengan *ciphertext* hasil enkripsi teknik vigenere dan transposisi yang umum digunakan. Pengujian ini digunakan untuk menguji keamanan dari serangan kriptanalisi terhadap metode yang diterapkan pada aplikasi enkripsi SMS yang dibuat penulis. Berikut ciphertext yang akan diujikan:

Pesan : Die im 16. Jahrhundert entstandene Vigenère-Verschlüsselung (nach Blaise de Vigenère) galt lange als sicherer Chiffrieralgorithmus („Le Chiffre indéchiffrable“, deutsch: „Die unentzifferbare Verschlüsselung“).[1] Ein Schlüsselwort bestimmt, wie viele und welche Alphabete genutzt werden. Die Alphabete leiten sich aus der Caesar-Substitution ab.

Kunci : dasite

1.*Ciphertext Vigenere* : Giw qf 16. Ndhjpnrgejb xrwslighhnw Dbkhnèjm-Oiusupeüwvedcgk (qaup Updikm wi Yiymgèvh) gstm pdnym tpv sakaiuej Kamifjqxvdlywkmwhecl („Ph Czqyjue avwégkixnkeelw“, lxywsup: „Wmh ufmgxcixnxveajm Oiusupeüwvedcgk“).[1] Hif Avloüskmearrl jxwwieum, ale nqxph ufl pioczm Tpshsjxxh gwvnxct omkhhn. Vqx Eopziuiwe dmbxhn kqvl duk lxv Fawatv-Vutammwulqhr db.

2.*Ciphertext* Gabungan : i1hewhk-pdqpwm ptk jyePyvxwy uiauwk]Akliaxlzh chqz n xatlbG dgrhbmue(U y) ajflh„qailx: ceiüg1 srw qfcshxkVpehllwuudfNrxgDjsv mihmmseidw(z kelphxvOec[fürw,nuopxnm owxv aVw .pblwniügui èsnviaxkl ué k,sWmnmue)Hlejuehp jw n umku vmhw6jjsnhOecadiggdpaKqwchjwn“w „fxjsv“ vm elp msgthxid dvtaq.q n i èuwkpkYvty umvm Cege umgx pd.ioaxm iTxvo.EibqkF-mr

3.*Ciphertext Vigenere* :

HEYRZJLG4X54RM7V8WX=<0?=7ZF>H4=<MAMMC>RGT@JDTHYIO04R5MVP9U::0V?4@@62A5E7<<KBL<BN3D2EIAWLTWMK2R4KUN8V9WZ9K1K=6ZE7E5;EK?KKA?L@MDGSVGWEMLXL0JS27S8WZS=2:T4ZC8@Z97IBJ<@<OT2>QEVGVFHLWK1NRJ698QTO<?=T3?B9C350H9IG@9J>P=EETGUHKG0L0KRJ1P4OWV;4<X2ZB3B684H9H4>HMDNOE=SLUCJIY20JQJ0O1S:O<U>;Z;@5=W51F>G;=:LBN:C?NBSGIUXL;GZO3Q4RUU9Z:V1T?0@X6@E:U3>3NNHJ>9QERBIDXKYFNH2U0ZPKGU;O2;<2?351@4F5;GJ?KKB<QQQEGDVLWGNF1N2ITL7W4NXV=2?V5YC6D7:DV<VHA:PBP@FPVJVVLJ?M3GU12Z37W69X<<ZU@7C79ED8H7?9NFOMR?5WVCLEZO0YRO5;7NXR7V<T2YB4C188GKHG?9IPJ9EBSLTDFAZOZNPL475PRM;Z;;1W<0B373FIG5=<LAI8A;RUT>IHXIYFOK4R4OQL90:U0<@4AZ7>F9B1=:K@M9B=QFRRDTSGVGNN2RZIRL8;:OZY>Z?W51E8E572JMK;AAQDQAGSRFXEMM1O2POJ7S9SZS9X>X40D5@Z84I:J:A:O@Q=BQTHWFLE1N2KRR7U8RYS<5=>3?>2CZ92DM

4.*Ciphertext* Gabungan :

EGM=Z<>D0PV2<NAKN9ZE?SL2SZ7<ELJO?09E

GJVZ4H=IJO;1:?UOUTf39DHK;1G<DFLVYD:PJ16UE9?EORY89BALMW3<;HKL<>:=TNLY12ASMJS04:QERS?2HLRX7=CJOV06<BIMUZ6;AGMSZ49fQHRT35fEKRW28>EJQ:Z5=CIZU16>>INP25;BGNTX5:AFLUWZ9?RLRX28?EFPR17=AIOQ07=BDNRZ57AGMOZ48ABLRY39J4W=4MfIM:f7<EWKW=5KDEJWTZ<>FNQT3G=HKOX64OCJS;W;:GGRVX3JBFZO35KEGINV7HfVG7<77MCYNT1G9DNP;358>FOUZ19RGIOW5;AEPSXZ:=FKR>ZgRXV0>AGHRU45BDLRV17?fGLS28BTGK9?99>GLP439DL2OU5>BBLQZ0:NEKUU24?QLNW26<BJMZX78FWO;V4KPLO7Z0IAUIR049fFGR;Z8MDFOSX5:fHNU52MY47<FMRT49?AK3W28KEKLVX7=CIOVW6<BHJT01;BHMSY0<fFLNX39?ENQX2G<fJQV17=CVPV?29fDN5Z57BGISZ4;<FLRX49fFKQS28>EJQR179DIOT17<>DZ58?HMTY5:fEL2T49KEKMW08:fJ2V18=CIPU04<BHNU01>=GNS;4:fUHRY0;?FKQW24?DVPV33<CHOV07<CHJTZ5;BGITY4:ABMRVZ:?EKQX29>fJQW28=Cg

Ciphertext **1** dan **2** merupakan hasil dari enkripsi metode yang umum digunakan. Sedangkan, ciphertext **2** dan **4** merupakan hasil enkripsi metode yang digunakan penulis. Ciphertext **1** dan **3** diuji dengan vigenere analysis, sedangkan ciphertext **2** dan **4** diuji dengan brute force attack.

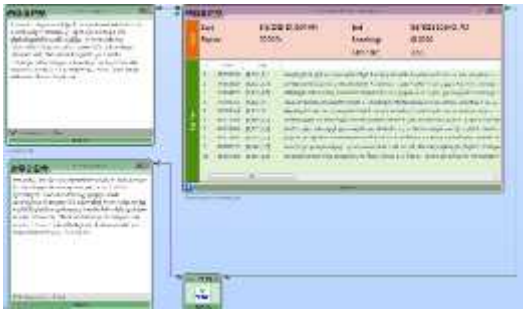
Vigenere analysis adalah sebuah tool untuk menganalisa kunci dan dapat memecahkan ciphertext yang didapatkan dari hasil enkripsi algoritma vigenere.

Gambar 4.1 pengujian vigenere *analysis(kasiski) ciphertext* 1

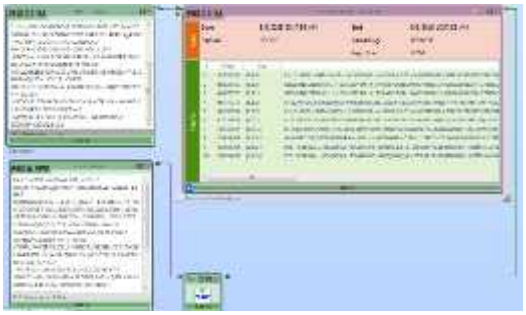
Gambar 4.2 pengujian *vigenere analysis(kasiski) ciphertext* 3

Gambar 4.1 dan 4.2 Merupakan tampilan hasil dari proses vigenere analysis untuk menganalisa dan memecahkan ciphertext vigenere. Dapat dilihat bahwa proses analisa kunci dan hasil teks pada Gambar 4.1, menunjukan bahwa ciphertext dapat dipecahkan. Sedangkan, pada Gambar 4.2 menunjukan ciphertext hasil dari aplikasi yang dibuat penulis, tidak dapat dipecahkan.

Untuk pengujian dengan *brute force attack*, ciphertext yang akan diujikan adalah ciphertext 2 dan 4. *Brute force attack* adalah sebuah teknik serangan terhadap sistem keamanan komputer yang menggunakan percobaan terhadap semua kunci yang mungkin.



Gambar 4.3 Pengujian dengan *brute force attack, ciphertext* 2



Gambar 4.41 Pengujian dengan *brute force attack, ciphertext* 4

Gambar 4.3 dan 4.4 Merupakan tampilan hasil Transposition analyzer saat melakukan serangan brute force attack terhadap ciphertext **2** dan **4**. Dapat dilihat bahwa gambar 4.3 dan 4.4 proses analisa kemungkinan kunci dan hasil teks, menunjukan bahwa chipertext sulit terpecahkan. Metode transposisi kolom jika digabung dengan vigenere, akan memperkuat teknik enkripsinya.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

Dari penelitian yang telah dilakukan, maka penulis dapat menarik beberapa kesimpulan, yaitu sebagai berikut :

1. Aplikasi enkripsi sms dengan metode Vigenere dan Transposisi Kolom dapat mengamankan pesan yang dikirim.
2. Kekurangan dari enkripsi dengan metode Vigenere dan Transposisi Kolom, menghasilkan panjang ciphertext dua kali lebih panjang dari pesan aslinya.

5.2 Saran

Dari kesimpulan yang telah diuraikan di atas, maka penulis memberikan saran untuk proses pengembangan lanjutnya dan guna penyempurnaan, adalah sebagai berikut :

1. Setelah dilakukan pengujian pada pada penelitian ini, maka penulis menyarankan untuk melanjutkan penelitian untuk dapat mengenkripsi gambar dan suara.
2. Penelitian dengan menggunakan metode yang sederhana, dengan menambahkan suatu teknik, sehingga didapatkan metode yang lebih optimal dalam pengamanan pesan.

DAFTAR PUSTAKA

[1] Defni, dan Rahmayun Indri. 2014. Enkripsi Sms (Short Message Service) Pada Telepon Selular Berbasis Android Dengan Metode RC6. Vol.16 No.1. Februari 2014.

[2] Munir Rinaldi. 2007. *Kriptografi*. Bandung : Informatika.

[3] Ariyus Dony. 2008. Pengantar ilmu kriptografi teori analisis dan implementasi. Yogyakarta : Andi.

[4] Sadikin Rifki.2012. *Kriptografi untuk keamanan jaringan.*Yogyakarta : Andi.

[5] Safaat H, Nazruddin. 2012. *Pemrograman Aplikasi Mobile Smartphone Dan Tablet PC Berbasis Android. Bandung*: Informatika.

[6] Boboy. “Pengertian dan Penggunaan Eclipse IDE”. 6 Januari 2015. https://boboy09.wordpress.com/2011/07/06/mari-kenali-pengertian-dan-kegunaan-aplikasi-ide/

[7] “Cara Kerja SMS”. 5 Januari 2015 http://forum.kompas.com/teras/76499-sms-dan-cara-kerjanya.html

[8] “Kartu SIM”. 8 Januari 2015. http://id.wikipedia.org/wiki/Kartu_SIM

[9] Cucu Tri Eka Yuliana, “Implementasi Algoritma Kriptografi Blowfish Dan Metode Steganografi End Of File Untuk Keamanan Data”, Universitas Dian Nuswantoro, Semarang, Laporan Tugas Akhir 2014.

[10] Eko Hari Rachmanto, “Teknik Keamanan Data Menggunakan Kriptografi Dengan Algoritma Vernam Chiper Dan Steganografi Dengan Metode End Of File(EOF)”, Universitas Dian Nuswantoro, Semarang, Laporan Tugas Akhir 2010.

[11] vinkel. ”Perbedaan GSM DAN CDMA”. 10 Januari 2015. http://apaperbedaan.blogspot.com/2013/08/perbedaan-gsm-dan-cdma.html

[12] Ir. Yusuf kurniawan, MT. 2004. *Kriptografi Keamanan Internet Dan Jaringan Telekomunikasi*. Bandung : Informatika.

[13] “apakah-smartphone-itu”. 10 Maret 2015 http://www.tasikisme.com/apakah-smartphone-itu