 ISSN: 1411-3201

APLIKASI ENKRIPSI SMS DENGAN MODIFIKASI VIGENERE CIPHER PADA PONSEL ANDROID

Riris Tri Harini [1] **, Ema Utami** [2]

[1,2] *STMIK AMIKOM Yogyakarta*
Email : ema.u@amikom.ac.id [2]

Abstraksi

Communicating is one of the earth's human nature as a means of communicating to understand each other. As for how communication has developed very rapidly from era to era. One way is through writing or message. Messages a delivery of information that can be read and have meaning.
In recent years, rapid development occurs on mobile phone technology (cell phones). One of them is a smart phone that has a full feature with complex operating system like a computer. Various operating system for mobile phones were introduced, such as Android.
Although equipped with premium features and the operating system, for the security of the delivery of messages through SMS facility, is still considered inadequate. By encrypting the content of messages to be sent, then the level of information security of the message can be improved. Of the various techniques of encryption, encryption method Vigenere cipher Caesar cipher with modifications and Eulerian numbers chosen as the method with a light workload. Access to the message of the application must be secured with the password, so the message will be safe from unauthorized parties.

***Kata Kunci* :**
SMS, Euler, Vigenere, Decryption, Encryption

Pendahuluan

Berkomunikasi merupakan salah satu sifat manusia sejak ada dimuka bumi. Berkomunikasi merupakan sarana untuk saling memahami satu sama lain. Cara berkomunikasi manusia juga mengalami perkembangan yang sangat pesat dari zaman ke zaman.

Salah satu cara berkomunikasi adalah melalui tulisan. Sebuah tulisan berfungsi untuk menyampaikan pesan kepada orang lain. Pesan merupakan informasi yang dapat dibaca dan mempunyai makna. Cara penulisan dari zaman dulu sampai sekarang juga terus mengalami perkembangan. Zaman dulu, manusia menyampaikan pesan melalui simbol, gambar yang ditulis pada batu, tulang, juga pada dinding-dinding goa atau yang lain. Media penyimpanan pesan yang menjadi asal muasal kertas pertama kali ditemukan oleh Bangsa Mesir berupa benda bernama papyrus yaitu sejenis nama suatu tumbuhan yang banyak tumbuh di sungai Nil. Penemuan kertas pertama kali pada tahun 105 Masehi oleh pegawai istana dari Cina yaitu Ts'ai-Lun yang terbuat dari campuran kulit kayu pohon mulbery, hemp, kain perca, serat bambu dan air yang yang diproses jadi pulp yang kemudian di jemur di bawah sinar matahari.

Seiring perkembangan media untuk pendokumentasian suatu informasi, berbagai ilmu pengetahuan dapat disimpan dalam bentuk buku, file yang disimpan dalam bentuk softcopy di dalam media compact disc, hard disc, dan media lainnya. Sebelum penemuan media dokumentasi suatu informasi, pengiriman informasi dari satu tempat ke tempat lain sudah terjadi. Dari latar belakang inilah suatu informasi rahasia disembunyikan agar pesan atau informasi yang dikirim tidak diketahui oleh orang yang tidak berhak.

Di zaman yang serba canggih ini, pesan pendek atau yang lebih popular disebut dengan SMS (short message service) merupakan salah satu bentuk komunikasi antar manusia yang paling banyak digemari karena penggunaannya yang mudah dan murah.

Bertolak belakang dengan kemudahan tersebut dari segi keamanan ternyata kurang memadai. System tidak bisa menjamin jika pesan tersebut salah kirim maka siapapun yang menerimanya, pesan tersebut bisa dibuka dan diketahui isinya. Hal ini tentu saja membuat ketidaknyamanan bagi sebagian orang yang ingin privasinya terjaga. Android merupakan salah satu system operasi yang sedang trend akhir-akhir ini. Namun ponsel yang menggunakan system operasi android juga masih sama dengan ponsel lainnya mengenai pengiriman pesan pendek yang keamanan masih kurang memadai.

Melihat permasalahan diatas penulis berkeinginan untuk membuat sebuah aplikasi enkripsi

 ISSN: 1411-3201

SMS dengan modifikasi Vigenere cipher pada ponsel Android.

Tinjauan Pustaka

Kriptografi

Kriptografi berasal dari bahasa Yunani, crypto dan graphia. Crypto berarti secret (rahasia) dan graphia berarti writing (tulisan). Kriptografi menurut terminologinya adalah sebuah ilmu dan seni untuk menjaga keamanan pesan ketika pesan dikirim dari suatu tempat ke tempat lain. Secara istilah kriptografi didefinisikan sebagai ilmu sekaligus seni untuk menjaga kerahasiaan pesan baik berupa data maupun informasi yang mempunyai arti atau nilai dengan cara menyamarkan (mengacak) menjadi bentuk yang tidak dapat dimengerti menggunakan suatu algoritma tertentu.

Vigenere cipher

Digambarkan pertama kali oleh Giovan Batista Belaso pada tahun 1553 yang ditulis didalam buku La Cifra del Sig2, yang kemudian di publikasikan oleh diplomat sekaligus kriptologis Prancis bernama Blaise de Vigenere pada abad 16 tepatnya tahun 1586.

Vigenere Cipher menggunakan Bujur Sangkar Vigenere untuk melakukan enkripsi . Pada bujur sangkar tersebut, kolom paling kiri menyatakan huruf-huruf kunci dan baris paling atas menyatakan teks-ali, sedangkan karakter-karakter lainnya menunjukkan karakter ciphertext. Table Vigenere berisi alphabet yang dituliskan dalam 26 baris, masing-masing baris digeser satu urutan ke kiri dari baris sebelumnya sehingga membentuk ke-26 kemungkinan sandi Caesar.

Penyandian dengan sandi Vigenere juga dapat dirumuskan sebagai berikut :

$$C_i \equiv (P_i + K_i) \bmod 26$$

$$P_i \equiv (C_i - K_i) \bmod 26 \quad \text{……..…….. (1)}$$

Keterangan :
Ci = huruf ke-i teks-tersandi
Pi = huruf ke-i teks-asli
Ki = huruf ke-i pada kata kunci
Ki = huruf ke-i pada kata kunci

Tes Kasiski

Tes Kasiski pertama kali ditemukan pada tahun 1863 oleh Frederich Kasiski. Didasari oleh observasi yang menyebutkan dua segmen yang sama/identik dari teks-asli akan dienkripsi menjadi teks-kode yang sama bilamana terjadi pada teks-asli segmen terpisah dengan jarak x posisi, dimana $x \equiv 0 \bmod m$. Sebaliknya, jika diperhatikan dua segmen yang identik pada teks-kode, yang panjang setiap segmennya adalah tiga, maka peluang bahwa segmen-segmen tersebut memiliki hubungan dengan segmen yang ada dalam teks-asli tadi.

Modifikasi Vigenere Chipher dengan Memanfaatkan Bilangan Euler

Dari penjelesan diatas sudah dapat dilihat kelemahan dari metode Vigenere Chipher yaitu jika panjang kunci lebih pendek dari panjang plainteks, sehingga akan menyebabkan penggunaan kunci yang berulang-ulang. Hal ini bisa menyebabkan kemungkinan timbulnya perulangan string pada cipherteks hasil enkripsi yang dapat dimanfaatkan untuk memecahkan panjang kunci sehingga dapat dimanfaatkan untuk memecahkan cipherteks tersebut.

Agar tidak terjadi hal tersebut yaitu dengan menggunakan panjang kunci sebanyak panjang teks-asli. Hal ini sedikit rumit karena untuk mengingat panjang kunci yang tidak memiliki arti tersendiri tentu akan merepotkan. Untuk itu penulis menggunakan metode pembangkitan suatu kunci baru yang memiliki perulangan string pada kunci tersebut yang memiliki panjang kunci sama dengan panjang plainteks dengan memodifikasi metode Vigenere Cipher ini. Untuk membangkitkan kunci tersebut, penulis menggunakan perkalian sistematis dengan menggunakan perkalian matematis dengan menggunakan bilangan Euler yang kemudian disebut sebagai bilangan e merupakan bilangan yang diperoleh dari pendekatan nilai $(1+\frac{1}{n})^n$ untuk n menuju tak hingga yang ditemukan oleh Jacob Bernoulli (O'connor & Robertson, 2001).

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Pada tahun 1748, Euler memberikan ide mengenai bilangan e yaitu :

$$e = 1 + \frac{1}{1!} + \frac{1}{2!} + \frac{1}{3!} + \cdots$$

bahwa

$$e = \lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Dari formulasi tersebut, Euler memberikan pendekatan untuk bilangan e 18 digit dibelakang koma, yaitu: e = 2.718281828459045235.

 ISSN: 1411-3201

Pada tahun 1884 Boorman menghitung e sampai dengan 346 digit dibelakang koma dan telah terhitung sampai dengan 869.894.101 digit dibelakang koma oleh Sebastian Wedeniwski.

e=2.7182818284590452353602874713526624977572470936999595749669676277240766303535475945713821785251664274274663919320030599218174135966290435729003342952605956307381323286279434907632338298807531952510190115738341879307021540891499348841675092447614606680822648001684774118537423454424371075390777449920695517027618386062613313845830007520449338265602976067371132007093287091274437470472306969772093101416928368 19

Keutamaanya dengan metode bilangan e ini adalah pengelompokan perkalian antara kunci dengan bilangan e yang sangat sulit untuk diterka serta bentuknya yang acak dan cukup panjang sehingga menyulitkan untuk ditembus oleh kriptanalis.

Eclipse

Eclipse merupakan sebuah perangkat IDE (*Integrated Development Environment*) yang digunakan untuk mengembangkan perangkat lunak dan dapat dijalankan oleh semua platform10. Dikembangkan oleh IBM untuk menggantikan perangkat lunak IBM Visual Age for Java 4.0. Produk ini diluncurkan oleh IBM pada tanggal 5 November 2001. Android merupakan *system operasi* yang berbasis Linux atau *Open Source*.

Hasil dan Pembahasan

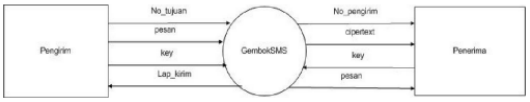
Rancangan flowchart

Rancangan ini untuk mendesain dan mempresentasikan program. Fungsinya adalah untuk memudahkan dalam penentuan alur logika yang akan dibuat.

Gambar 1. Flowchart Sistem

Data Context Diagram (DCD)

Pendefinisian dengan Data Context Diagram (DCD) atau DFD level 0 memberikan data yang mengalir antara system dan lingkungan yang digambarken secara global.



Gambar 2. DFD level 0

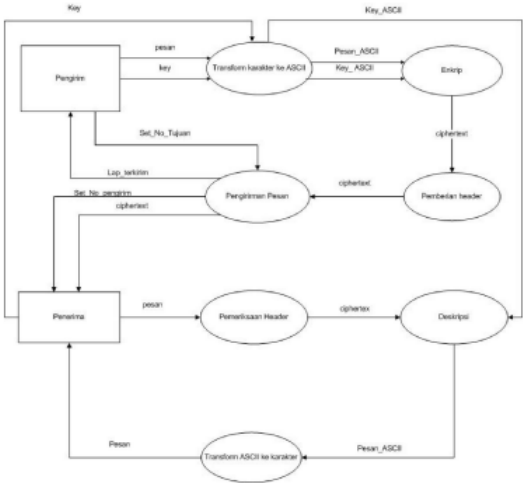
Pada gambar diatas, user (pengirim) menginputkan nomor tujuan, pesan dan kunci kepada system. Selanjutnya system akan memberikan output konfirmasi bahwa pesan telah terkirim. Selanjutnya penerima akan menerima teks-kunci (ciphertext), dan nomor pengirim.

Penerima pesan harus menginputkan kunci kepada system, kemudian system akan mengirimkan output pesan asli kepada penerima.

Data Flow Diagram

Dari alur Data Context Diagram atau DFD lever 0 pada gambar 3.5 diatas dapat dibuat diagram alir Data Flow Diagram yang lebih rinci dari DCD pada setiap tahapan.

 ISSN: 1411-3201



Gambar 3. DFD Level 1

Gambar diatas merupakan DFD level 1 dari aplikasi perangkat lunak GembokSMS.

Pada DFD level 1, system akan dipecah menjadi proses-proses kecil sehingga dapat menjelaskan proses-proses dan arus data yang mengalir dalam system.

Proses-proses yang terdapat dalam DFD level 1 adalah:

1. Transformasi kode ASCII

   Proses ini melakukan transformasi pesan dan kunci ke dalam kode ASCII.

2. Enkripsi

   Proses ini melakukan pengenkripsian pesan dengan metode enkripsi vigenere cipher dengan kunci yang diinputkan.

3. Pemberian Header

   Pesan yang telah dienkripsi menjadi ciphertext akan diberikan header sebagai penanda bahwa pesan tersebut adalah pesan GembokSMS.

4. Pengiriman pesan

   Pesan ini melakukan pengiriman pesan yang telah dienkripsi dan memberikan laporan pengiriman kepada pengirim bahwa pesan telah dienkripsi dan dikirimkan ke nomor yang diinputkan.

5. Pemeriksaan header

   Pada proses ini pesan yang masuk akan diperiksa apakah memiliki header GembokSMS. Apabila pesan memiliki header maka pesan akan diteruskan ke proses selanjutnya yaitu deskripsi. Jika pesan tidak memiliki header maka sistem akan mengabaikan pesan tersebut. Selain itu pemeriksaan header juga akan memisahkan SMS sehingga masuk dalam kotak masuk aplikasi GembokSMS.

6. Deskripsi

   Proses ini melakukan pendeskripsian pesan sesuai dengan kunci yang diinputkan. Apabila kunci benar maka ciphertext akan menjadi pesan asli (plaintext). Jika kunci salah maka pesan akan tetap terdeskripsi akan tetapi pesan yang didapat bukan pesan asli.

Rancangan antar muka

Perancangan antarmuka adalah proses membuat perancangan form-form tampilan layar.

Gambar 4. Rancangan tulis pesan

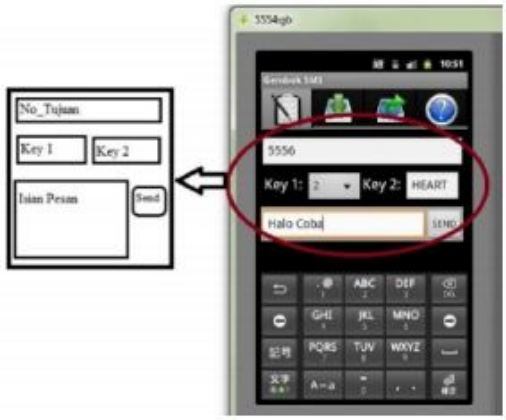
Gambar 5. Rancangan kotak masuk

 ISSN: 1411-3201

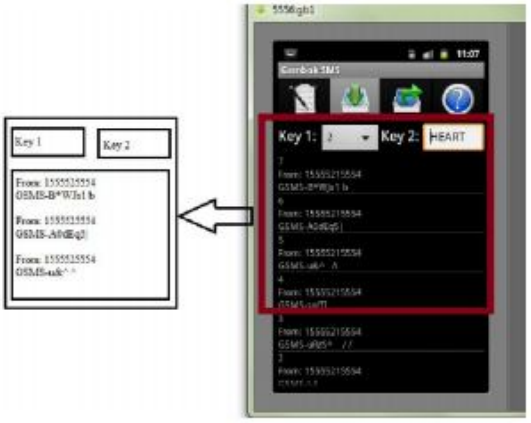
Gambar 6. Rancangan kotak keluar

Gambar 7. Rancangan menu seting

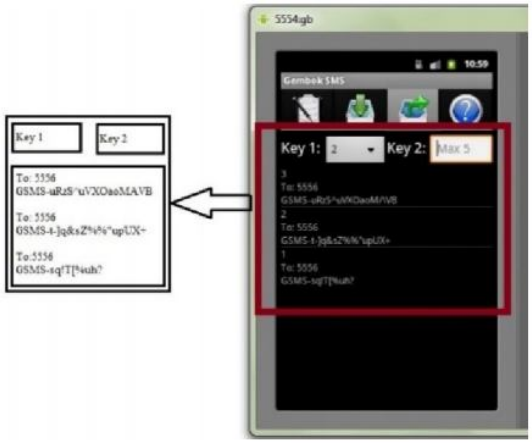
Dari rancangan system dapat dibentuk aplikasi sebagai berikut :



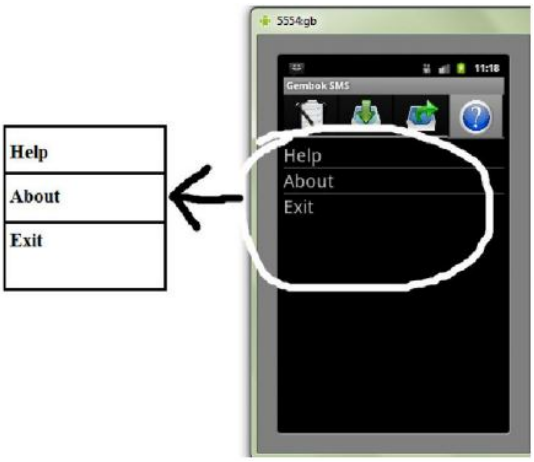
Gambar 8. Menu tulis pesan



Gambar 9. Menu kotak masuk



Gambar 10. Menu kotak keluar



Gambar 11. Menu help

 ISSN: 1411-3201

Materi pengujian

Materi yang akan diujikan pada aplikasi GembokSMS ini adalah sebagai berikut:

1. Pengiriman pesan

   Akan dilakukan pengujian pada proses pengiriman pesan apakah aplikasi GembokSMS dapat mengenkripsi pesan dan mengirimkan pesan yang telah dienkripsi ke nomor yang dituju atau tidak.

2. Penerimaan pesan

   Akan dilakukan pengujian pada proses penerimaan pesan apakah aplikasi GembokSMS dapat menerima sebuah pesan dan mendekripsinya menjadi pesan asli

3. Laporan

   Akan dilakukan pengujian apakah akan keluar laporan apabila pesan telah dienkripsi maupun didekripsi.

4. Menampilkan menu Help

   Akan dilakukan pengujian apakah fungsi Help berfungsi atau tidak.

5. Memberikan header pada ciphertext

   Akan dilakukan pengujian apakah terdapat header pada ciphertext atau tidak.

Hasil penelitian

Pada hasil pengujian ini didapatkan bahwa:

1. Hampir semua ponsel Android OS yang diujicobakan dapat menjalankan fungsi-fungsi aplikasi dengan baik.

2. Kecepatan akses aplikasi dari setiap ponsel akan berbeda sesuai dengan memori yang dimilikinya.

3. Aplikasi ini dapat dijalankan dengan sempurna hanya pada ponsel Android OS versi 2.3 dan versi diatasnya.

Kesimpulan dan Saran

Kesimpulan yang dapat diambil dari penulisan skripsi ini adalah sebagai berikut:

1. Metode enkripsi Vigenere Cipher adalah metode enkripsi substitusi klasik yang telah ketinggalan jaman dan mudah dipecahkan oleh cryptanalysis. Kelemahan ini ditutup dengan cara pesan ke kode ASCII lalu dienkripsi dengan metode vigenere cipher. Dengan cara ini ciphertext akan lebih sulit dipecahkan cryptanalysis.

2. Aplikasi enkripsi pesan teks ini telah berhasil meningkatkan keamanan dalam pengiriman pesan teks melalui telepon seluler khususnya ponsel Android OS. Pesan teks terenkripsi ini tidak dapat dibaca, jika tidak dideskripsikan dengan kunci yang benar.

3. Algoritma hasil modifikasi dari vigenere cipher yang memanfaatkan bilangan euler dapat diimplementasikan dengan baik untuk enkripsi pesan teks yang bekerja pada jaringan GSM dengan mengirimkan pesan dalam bentuk karakter dan symbol pada ponsel Android OS.

4. Hasil pengujian terhadap metode enkripsi modifikasi algoritma Vigenere cipher untuk proses enkripsi pesan teks menunjukkan bahwa perangkat lunak tersebut secara fungsional mengeluarkan hasil yang sesuai dengan yang diharapkan.

5. Aplikasi tersebut dapat berjalan dan berfungsi normal pada semua jenis ponsel Android OS yang berbeda seri.

Daftar Pustaka

[1] Ariyus, Dony. "Pengantar Ilmu Kriptografi". Yogyakarta: Andi Offset.
[2] Elmastri, R & Navasthe, B. "Fundamental Of Database System 2nd Edition". Addison Wesley, 1994.
[3] H., Nazaruddin Safaat. "Android Pemrograman Aplikasi Mobile Smartphone Dan Tablet PC Berbasis Android". Bandung: Informatika, 2011.
[4] Harianto, B." Esensi-Esensi Pemrograman Java". Bandung: Informatika, 2007.
[5] O'connor J.J., And Robertson, E.F.." History Topic The Number of E". 2001.
[6] Rinaldi, Munir. "Diktat Kuliah Kriptografi. Bandung: STIE ITB, 2006.
[7] Sutejo, B & Handoko Y. Teleakses: Database Pendidikan Berbasis Ponsel. Yogyakarta: Andi Offset, 2003.
[8] Zulfadli. Aplikasi Supply Chain Management Berbasis SMS. FMIPA UGM Yogyakarta, 2005.
[9] http://www.mu.org/~doug/exp/100000.html.
[10] http://ozeki.hu/index.php?ow-page-number=489&page-name=sms-basic.concepts.