MODUL PEMBELAJARAN ENKRIPSI BERBASIS ANDROID

SKRIPSI

Diajukan Untuk Memenuhi Sebagian Syarat Guna
Memperoleh Gelar Sarjana Komputer (S. Kom)
Pada Program Studi Teknik Informatika

Oleh :

MUH. TANJUNG ALFALAH
NPM : 10.1.03.02.0318

PROGRAM STUDI TEKNIK INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS NUSANTARA PGRI KEDIRI

2014

ABSTRAK

Muh. Tanjung Alfalah : Modul Pembelajaran Enkripsi Berbasis Android, Skripsi, Fakultas Tektik Program Studi Teknik Informatika UNP Kediri, 2014.

Kata kunci : modul, enkripsi, android.

Penelitian ini dilatar belakangi hasil pengamatan dan pengalaman peneliti, bahwa masih minimnya pemahaman seseorang mengenai enkripsi. Akibatnya banyak orang yang kurang mengerti betapa pentingnya enkripsi untuk mengamankan data pribadi.

Permasalahan penelitian ini adalah (1) Minimnya pemahaman masyarakat tentang enkripsi. (2) Kurangnya kesadaran masyarakat tentang pentingnya enkripsi untuk mengamankan data atau informasi penting. (3) Melihat banyaknya pengguna *Operating System* Android di Indonesia, belum banyak aplikasi yang mampu memberikan pemahan tentang enkripsi.

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Salah satu metode enkripsi adalah Caesar, dimana teks asli digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet.

Kesimpulan hasil penelitian ini adalah (1) Aplikasi ini dibuat sesederhana mungkin sehingga mudah dipahami. (2) Aplikasi ini dilengkapi video simulasi untuk memudahkan *user* dalam memahami teori. (3) Berdasarkan hasil pengujian aplikasi ini sudah dapat dipastikan bebas dari *syntax error, runtime error, dan logic error*.

Berdasarkan simpulan hasil penelitian ini, direkomendasikan : (1) Penambahan materi mengenai metode-metode enkripsi lainya. (2) Penambahan jenis latihan untuk menebak kata yang sudah dienkripsi. (3) Penyempurnaan desain *interface* agar lebih menarik lagi. (4) Penambahan fitur *update* melalui internet.

1. PENDAHULUAN

Orang sering mendengar istilah enkripsi, namun mayoritas hanya mengenal istilah enkripsi itu sebagai merubah atau mengganti sesuatu sehingga tidak dapat dimengerti atau diketahui orang lain, atau dapat dibilang enkripsi itu semacam sandi rahasia. Tidak banyak orang yang mengetahui bagaimana cara kerja enkripsi untuk merubah sesuatu menjadi sulit untuk dimengerti orang lain.

Enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. Salah satu metode yang paling sederhana dan paling terkenal dalam proses enkripsi adalah sandi Caesar atau sandi geser. Sandi Caesar termasuk sandi substitusi dimana setiap huruf pada teks terang (*plaintext*) digantikan oleh huruf lain yang memiliki selisih posisi tertentu dalam alfabet. Ada juga enkripsi dengan metode Vigenere, metode inti merupakan bentuk sederhana dari sandi substitusi polialfabetik. Kelebihan sandi ini dibanding sandi Caesar dan sandi monoalfabetik

lainnya adalah sandi ini tidak begitu rentan terhadap metode pemecahan sandi yang disebut analisis frekuensi.

Enkripsi sangat dibutuhkan untuk mengamankan informasi-informasi pribadi yang bersifat penting sehingga hanya orang yang berkepentinganlah yang mengetahui informasi tersebut. Di tengah kemajuan teknologi yang semakin memudahkan semua orang untuk mendapatkan informasi dari manapun, maka keamanan dan kerahasiaan sebuah data atau informasi menjadi sangat penting. Apalagi akhir-akhir ini marak beredar isu penyadapan yang dilakukan oleh pihak asing. Namun begitu kesadaran masyarakat tentang pentingnya keamanan data masih sangat rendah, seperti yang dikatan oleh Ashwin selaku Direktur Jendral Aplikasi Informatika Kominfo (November 2013) “Masih banyak kelemahan di sistem keamanan TI di lembaga pemerintahan dan swasta. Selain itu, kesadaran masyarakat terhadap data-data penting masih sangat rendah.”Menurut Onno W. Purbo (2013),enkripsi merupakan salah satu cara ampuh untuk mencegah tindakan penyadapan atau pencurian data pribadi di tengah isu penyadapan pihak asing yang akhir-akhir ini marak diberitakan.

Dewasa ini perkembangan teknologi semakin pesat, khususnya teknologi yang bersifat mobile. Analisis lembaga intelijen Amerika Serikat, CIA, menyebutkan bahwa jumlah pengguna ponsel di Indonesia cukup tinggi. Mencapai 236,8 juta pelanggan seluler. Dari jumlah itu, belum terdata berapa orang yang memiliki ponsel lebih dari satu. Indonesia pun menempati posisi kelima negara dengan jumlah pengguna ponsel terbanyak di dunia. Belum lagi penggunaan *smartphone* yang makin hari makin meningkat, terutama *smartphone* dengan *Operating System* android. "Android dalam beberapa bulan terakhir ini peluang pasarnya sangat besar," ujar Wandy Effendi, Bendahara Asosiasi Pengusaha Komputer Indonesia (Apkomindo) Sulawesi Selatan. "Pengguna Android di Indonesia meningkat 22%, dan kami perkirakan tak lama lagi akan mendominasi pasar smartphone," kata Darwin Lie, Associate Market Analyst for Client Devices Research, IDC Indonesia. Hal ini dikarenakan android yang bersifat *Open Source*, sehingga para pengembang aplikasi lebih tertarik untuk menanamkan karya mereka pada android.(Sumber: inet.detik.com,2012)

Berdasarkan paparan di atas, maka penulis tertarik untuk membuat aplikasi yang

mengenalkan proses enkripsi menggunakan metode Caesar. Aplikasi ini dibuat dengan berbasis mobile dengan OS android, sehingga lebih mudah dan praktis untuk dipelajari dimana saja dan kapan saja.

2. LANDASAN TEORI

A. Modul Pembelajaran

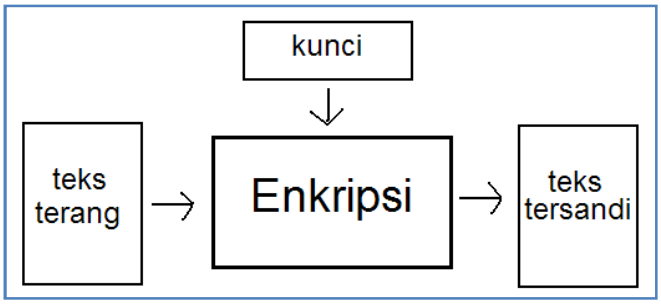
Modul pemberlajaran adalah bahan ajar yang disusun secara sistematis dan menarik yang mencakup isi materi, metode dan evaluasi yang dapat digunakan secara mandiri untuk mencapai kompetensi yang diharapkan (Anwar, 2010). Modul yang baik harus disusun secara sistematis, menarik, dan jelas. Modul dapat digunakan kapanpun dan dimanapun sesuai dengan kebutuhan pemakai. Beberapa karakteristik modul pembelajaran menurut Anwar (2010) adalah sebagai berikut :

a) *Self instructional*, Siswa mampu membelajarkan diri sendiri, tidak tergantung pada ihak lain.
b) *Self contained,* Seluruh materi pembelajaran dari satu unit kompetensi yang dipelajari terdapat di dalam satu modul utuh.
c) *Stand alone*, Modul yang dikembangkan tidak tergantung pada media lain atau tidak harus digunakan bersama-sama media lain.
d) *Adaptif*, Modul hendaknya memiliki daya *adaptif* yang tinggi terhadap perkembangan ilmu dan teknologi.
e) *User friendly*, Modul hendaknya juga memenuhi kaidah akrab dengan pemakainya.

B. Enkripsi

Di bidang kriptografi, enkripsi adalah proses mengamankan suatu informasi dengan membuat informasi tersebut tidak dapat dibaca tanpa bantuan pengetahuan khusus. (id.wikipedia.org/wiki/Enkripsi, diakses tanggal 12 November 2013). Dikarenakan enkripsi telah digunakan untuk mengamankan komunikasi di berbagai negara, hanya organisasi-organisasi tertentu dan individu yang memiliki kepentingan yang sangat mendesak akan kerahasiaan yang menggunakan enkripsi. Di pertengahan tahun 1970-an, enkripsi kuat dimanfaatkan untuk pengamanan oleh sekretariat agen pemerintah Amerika Serikat pada domain publik, dan saat ini enkripsi telah digunakan pada sistem secara luas. Enkripsi dapat

digunakan untuk tujuan keamanan, tetapi teknik lain masih diperlukan untuk membuat komunikasi yang aman, terutama untuk memastikan integritas dan autentikasi dari sebuah pesan. Contohnya, *Message Authentication Code* (MAC) atau *digital signature*. Penggunaan yang lain yaitu untuk melindungi dari analisis jaringan komputer.



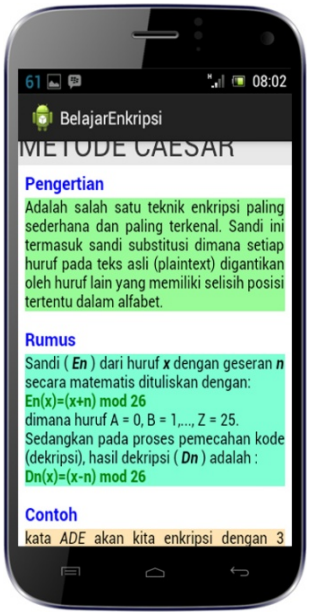
Gambar proses enkripsi secara sederhana

3. TAMPILAN PROGRAM

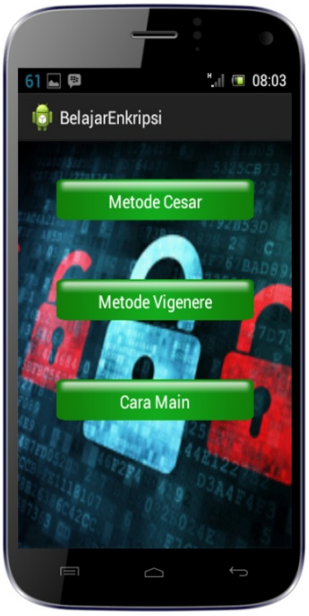
Berikut tampilan-tampilan dari aplikasi ini.

Gambar Halaman *Home*

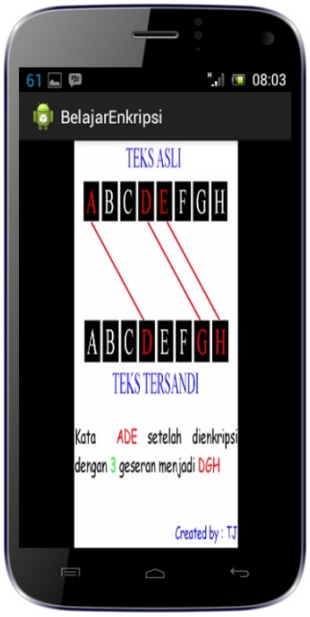
Gambar Halaman Materi



Gambar Halaman Materi Caesar

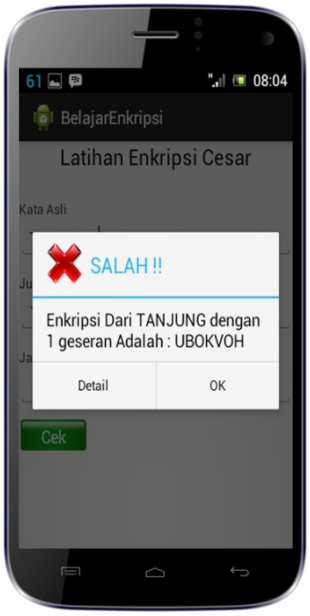


Gambar Halaman Latihan

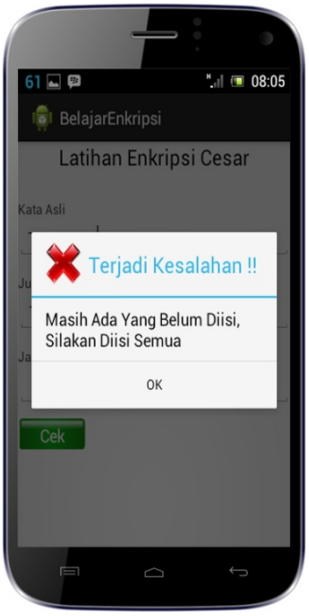


Gambar Video Simulasi Metode Caesar

Gambar Halaman Latihan Caesar

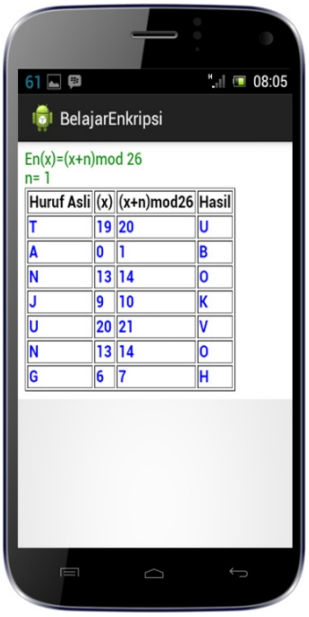


Gambar Pesan Jawaban Salah

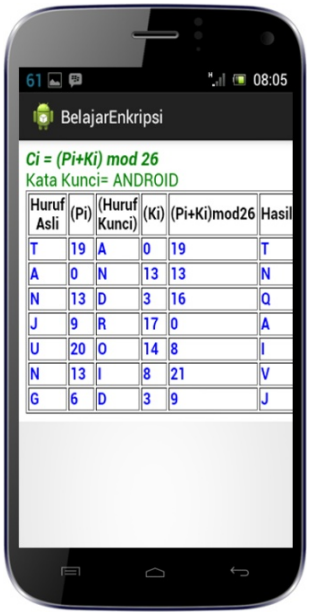


Gambar Pesan Kesalahan

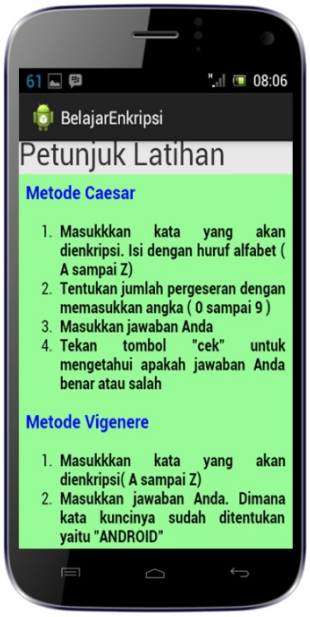
Gambar Pesan Jawaban Benar



Gambar Halaman Detail Caesar



Gambar Halaman Detail Vigenere



Gambar Halaman Petunjuk Latihan

4. KESIMPULAN

Setelah melalaui beberapa tahapan untuk menyelesaikan aplikasi ini, penulis dapat membuat kesimpulan sebagai berikut :

1. Aplikasi ini dibuat dengan sangat sederhana namun mudah dipahamai. Terbukti dari beberapa responden yang sebelumnya belum mengetahui apa itu enkripsi menjadi lebih mengerti tentang enkripsi.
2. Aplikasi ini dilengkapi dengan video simulasi yang memudahkan *user* untuk memahami materi yang dipelajari. Dari beberapa responden setelah menggunakan aplikasi ini mengatakan bahwa enkripsi itu sebenarnya sangat mudah.

DAFTAR PUSTAKA

Anwar, Ilham. 2010, *Pengembangan Bahan Ajar. Bahan Kuliah Online.* Bandung : Direktori UPI

Depapepe. 2006. *Canon.mp3.* tersedia : (www.4shared.com/mp3/depapepe_canon.mp3), diunduh 03 Oktober 2010.

Nugroho, Andy. 2012, *Iplementasi Algoritma Caesar Chiper ROT13 dan BASE64 untuk Enkripsi dan Dekripsi Pesan SMS pada*

Handphone Bebasis Android, tersedia : (http://repository.amikom.ac.id/files/Publikasi_07.11.1456.pdf), diunduh 03 Oktober 2013.

Purbo, Onno W. 2014. *Ini Jurus Anti Sadap Ala Onno Purbo*. www.detik.com ,diakses tanggal 20 Januari 2014.

Safaat H, Nazaruddin. 2012. *Pemrograman Aplikasi Mobile Smartphone dan Tablet PC Berbasis Android*(edisi revisi). Bandung: Penerbit INFORMATIKA.

Sandi Caesar. 2013. http://id.wikipedia.org/wiki/Sandi_Caesar, diakses tanggal 12 November 2013

Sandi Vigenere. 2013. http://id.wikipedia.org/wiki/Sandi_Caesar, diakses tanggal 05 Februari 2014

Sri, Dharwiyanti. 2003. *Pengantar Unified Modeling Language (UML)*, ilmukomputer.com, diakses tanggal 30 Desember 2013.