



Hak cipta dan penggunaan kembali:

Lisensi ini mengizinkan setiap orang untuk menggubah, memperbaiki, dan membuat ciptaan turunan bukan untuk kepentingan komersial, selama anda mencantumkan nama penulis dan melisensikan ciptaan turunan dengan syarat yang serupa dengan ciptaan asli.

Copyright and reuse:

This license lets you remix, tweak, and build upon work non-commercially, as long as you credit the origin creator and license it on your new creations under the identical terms.

BAB I

PENDAHULUAN

1.1 Latar Belakang

Tidak dapat dipungkiri bahwa teknologi berkembang sangat pesat. Hal ini dapat dibuktikan dengan banyaknya inovasi yang diciptakan oleh manusia, dari yang sederhana, hingga yang berpengaruh besar. Di sebagian besar bagian masyarakat, teknologi telah mampu membuktikan perannya dalam hal memperbaiki aspek ekonomi, pangan, sosial, dan sebagainya. Terutama setelah diciptakannya *personal computer* dan *mobile device*, dimana sekarang hampir semua pekerjaan manusia memiliki hubungan dengan kedua jenis benda elektronik tersebut.

Salah satu bagian penting dalam dunia teknologi adalah *E-mail (electronic mail)* atau surat elektronik. *E-mail* adalah salah satu jenis layanan di internet yang dapat digunakan untuk melakukan kirim-mengirim surat elektronik secara cepat dan mudah tanpa terhalangi oleh jarak dan waktu. Surat elektronik memerlukan *E-mail address* yang unik, sama seperti nomor telepon.

Dari statistik yang dimiliki oleh Wolfgang Jaegel, sudah lebih dari 3,2 miliar pengguna E-mail di seluruh dunia, dan 95% pengguna internet, menggunakan E-mail juga. Sedangkan dari data statistik yang dimiliki oleh pwnedlist.com, sudah lebih dari 30 juta akun E-mail bocor, dan 170 juta isi E-mail diakses oleh hacker. Sejak kehadiran *E-mail*, banyak pengguna baik individu maupun perusahaan, menggunakan *E-mail* sebagai cara untuk menyampaikan informasi atau data yang sangat penting dan data tersebut menjadi sebuah data rahasia yang tidak boleh

diketahui oleh pihak-pihak yang tidak berkepentingan. Perusahaan tidak hanya merahasiakan data-data penting dari pihak luar perusahaan, tetapi juga memiliki data rahasia antara divisi yang tidak boleh diketahui oleh divisi lain karena itu dibutuhkan suatu metode yang dapat menjaga kerahasiaan informasi perusahaan. Metode yang dimaksud adalah kriptografi yaitu sebuah seni dan bidang keilmuan dalam penyandian informasi atau pesan dengan tujuan menjaga keamanan informasi tersebut. Saat ini proses pengiriman suatu E-mail belum disertai adanya enkripsi, sehingga E-mail tersebut dapat dibuka oleh siapa saja yang memiliki akses. Oleh sebab itu perlu dibuat sistem enkripsi E-mail yang dapat melindungi isi E-mail.

Berikut ini adalah beberapa penelitian yang telah dilakukan sebelumnya terkait dengan topik yang dibahas mengenai enkripsi:

1. Judul: Perancangan Program Aplikasi Music Player Dengan Menggunakan Metode Kriptografi Triple Data Encryption Standard (2012)

Oleh: Shopyan Nuur

Penelitian ini merancang framework system keamanan music player berbasis kriptografi Triple Data Encryption Standard yang dapat membantu publisher dalam proses keamanan musik.

2. Judul: Implementasi Kombinasi Algoritma 3DES Dan Algoritma BASE64 Pada Sistem Keamanan Handshaking Animation Store (2013)

Oleh: Muhammad Abdul Rahim

Penelitian ini mengkombinasikan metode enkripsi dan dekripsi menggunakan algoritma 3DES dan algoritma Base64 pada satu protokol.

1.2 Rumusan Masalah

Dengan melihat latar belakang di atas, masalah yang dapat diteliti dalam penelitian ini adalah bagaimana membuat aplikasi yang dapat melindungi isi E-mail dengan sistem enkripsi E-mail menggunakan algoritma Triple DES dengan QR Code sebagai kunci.

1.3 Batasan Masalah

Dalam penulisan tugas akhir ini, penelitian memfokuskan masalah yang ada sehingga tidak menyimpang dari pokok bahasan perancangan sistem yang dibuat.

Pembatasan masalah ini diantaranya sebagai berikut:

- a. Metode yang digunakan pada aplikasi ini adalah metode Triple DES.
- b. Mail domain hanya menggunakan @gmail.com atau @yahoo.com
- c. Bahasa pemrograman yang digunakan adalah Java.
- d. Aplikasi dijalankan melalui desktop dengan OS Windows XP/Vista/7/8.
- e. Program dibuat menggunakan IDE Netbeans 7.4
- f. Password diserahkan secara manual
- g. Kode QR dipindai menggunakan *webcam*, atau dari file .png yang di-*generate* oleh aplikasi ini.

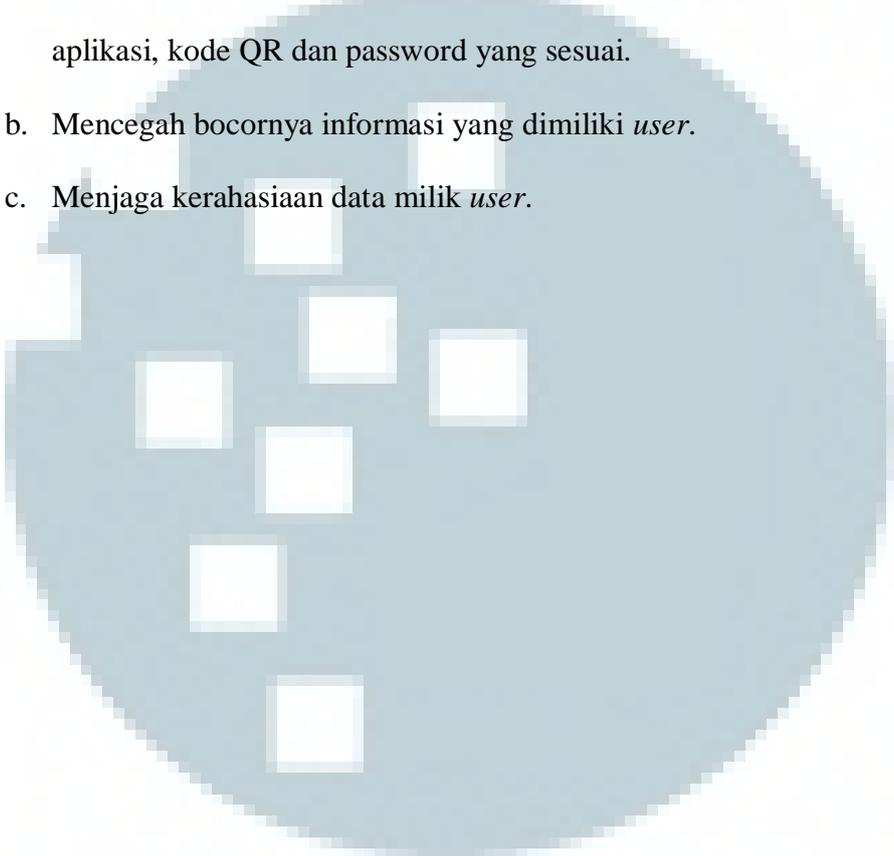
1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah membangun suatu aplikasi yang bisa melakukan penyandian (enkripsi dan dekripsi) terhadap E-mail, atau beberapa data pribadi maupun non-pribadi secara lokal menggunakan metode Triple DES untuk merahasiakan data yang dimiliki oleh pengguna, serta menggunakan password dan kode QR sebagai kunci untuk membuka data yang telah dienkripsi tersebut.

1.5 Manfaat Penelitian

Manfaat dari penelitian ini adalah:

- a. File yang dienkripsi tidak dapat dibaca oleh pihak yang yang tidak memiliki aplikasi, kode QR dan password yang sesuai.
- b. Mencegah bocornya informasi yang dimiliki *user*.
- c. Menjaga kerahasiaan data milik *user*.



UMMN