JISKa (Jurnal Informatika Sunan Kalijaga), Vol. 2, No. 3, Januari, 2018, Pp. 175–180
ISSN 2527-5836

Perancangan Aplikasi Email Menggunakan Algoritma Caesar CIPHER dan Base64

Dwi Nurani
Universitas AMIKOM Yogyakarta Jl. Ringroad Utara Condong Catur
e-mail : dwinurani@amikom.ac.id

Abstract

Send news or documents into individual or group communication media. The nature of news or documents are also used to be very secret. Increasingly sophisticated technology makes it increasingly easy to send a message or document. For example, in the advancement of the internet many parties that provide email management services, from sending or receiving also in terms of archiving. Convenience offered technology is not no risk. News or documents sent over the Internet are vulnerable to crime. In order for news or document can be up to the recipient safely and intact then takes the role of cryptography. Cryptography is the science to encrypt a message to make it more secure. In this study, using algorithms and Base64 Cipher Caesar. Caesar algorithm is an algorithm that is old and easily. While Base64 using ASCII format. So that the two algorithms can be used as it is complex. As a result, the security level is higher than not using cryptography. The encryption process and decryption not complicated and does not require a long time. If there are those who are not responsible to know the content of news or documents then he should know the key to reading and ensured key that only the sender and receiver know.

Keywords: ***email, cryptography, secret messages, Caesar Cipher, Base6***

Abstrak

Mengirim berita atau dokumen menjadi media berkomunikasi perseorangan atau kelompok. Sifat berita atau dokumen juga biasa menjadi sangat rahasia. Teknologi yang semakin canggih membuat semakin mudah dalam mengirim berita atau dokumen. Contohnya dalam kemajuan internet banyak pihak yang menyediakan jasa pengelolaan email, dari mengirim atau menerima juga dalam hal pengarsipan. Kemudahan yang ditawarkan teknologi bukan tidak punya resiko. Berita atau dokumen yang dikirim melalui internet rentan terhadap kejahatan. Agar berita atau dokumen yang dikirim bisa sampai kepada penerima dengan aman dan utuh maka dibutuhkan peran kriptografi. Kriptografi adalah ilmu untuk menyandikan pesan agar lebih aman. Dalam penelitian ini menggunakan algoritma Caesar Cipher dan Base64. Algoritma Caesar merupakan algoritma yang tua dan mudah. Sedangkan Base64 menggunakan format ASCII. Sehingga kedua algoritma tersebut dapat dijadikan hal yang komplek. Hasilnya, tingkat keamanannya lebih tinggi dibandingkan tidak menggunakan kriptografi. Proses enkripsi dan dekripsi tidak rumit dan tidak membutuhkan waktu yang lama. Bila ada pihak yang tidak bertanggungjawab ingin mengetahui isi berita atau dokumen maka dia harus tahu key untuk membaca dan dipastikan key itu hanya pengirim dan penerima yang tahu

Kata Kunci: ***mail*****, kriptografi, pesan rahasia,** ***Caesar Chiper*****,** ***Base64***

1. PENDAHULUAN

Kriptografi sudah dipakai orang sejak empat abad yang lalu, perkembangan kriptografi begitu pesatnya sampai sekarang. Caesar cipher yang pertama dalam dunia penyandian pada waktu pemerintahan Yulius Caesar yang dikenal dengan Caesar Cipher, dengan mengganti posisi huruf awal dari alphabet (Ariyus, 20106). Base64 salah satu algoritma untuk encoding dan decoding

suatu data ke format ASCII, yang didasarkan. pada bilangan dasar 64. Base64 banyak digunakan di dunia internet sebagai media data format untuk mengirimkan data (Kurniawan, 2013).

Surat adalah sarana atau wahana komunikasi tertulis yang ditujukan kepada orang lain atau suatu instansi dengan tujuan untuk menyampaikan suatu hal baik itu berupa informasi, perintah atau sebuah pemberitahuan (Gantini dan Griffin, 2011). Fungsinya mencakup lima hal yaitu sarana pemberitahuan, permintaan, buah pikiran, dan gagasan; alat bukti tertulis; alat pengingat; bukti historis; dan pedoman kerja. Untuk mengkirim pesan atau berita dapat menggunakan jasa kurir yang biaya bayarnya berdasakan jarak. Jadi semakin jauh tempat tujuan surat maka biayanya semakin mahal. Sekarang juga ada beberapa jenis layanan dalam mengirim surat. Mulai dari yang biasa, kilat khusus maupun express. Untuk yang biasa estimasi surat sampai ketujuan anatar 4-5 hari, kilat khusu estimasi surat sampai tujuan antara 2-3 hari sedangkan yang express estimasi hanya 1 hari.

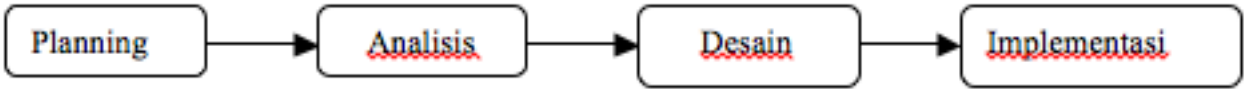
Email merupakan singkatan dari *Electronic Mail*. Kegunaan email itu sendiri adalah sama dengan surat biasa untuk berkomunikasi dengan orang lain, yang membedakan adalah alat atau perangkat yang digunakan untuk mengirim berita atau surat tersebut. Kalau email membutuhkan perangkat keras, perangkat lunak serta koneksi internet untuk mengirim suatu berita. Selain itu email memungkinkan untuk melampirkan data seperti dokumen, gambar, video dan lain sebaginya dan tanpa ada batasan wilayah. Dari segi waktu email membutuhkan waktu yang cepat untuk sampai ke tujuan dibandingkan dengan surat yang kita kirim melalui kurir surat karena waktu yang dibutuhkan untuk mengirim dalam hitungan detik. Kemudian dari segi biaya relatif lebih murah karena kemudahan untuk mendapatkan akses internet untuk saat ini lebih mudah, di tempat-tempat umum sudah menyediakan layanan *free wifi* sehingga kapanpun dan dimanapun kita bisa mengirim surat secara elektonik. Penyedia jasa email itu sendiri banyak dan gratis seperti gmail, yahoo.

Salah satu dampak negatif dalam perkembangan teknologi adalah adanya penyedapan terhadap data, dimana tindakan penyadapan tersebut merupakan salah satu masalah yang paling ditakuti oleh pengguna jaringan komunikasi khususnya dalam proses pengiriman dan penerimaan *email* (Kurniawan, 2013). Berdasarkan hal tersebut maka dibuat rancangan pengiriman dan penerimaan email yang melalui tahapan enkripsi dan dekripsi yang tujuannya antara lain untuk mengamankan berita atau informasi yang dikirim. Proses enkripsi dan dekripsi merupakan suatu proses penyandian pesan dalam ilmu kriptografi.

Melihat pada kenyataan semakin banyak data yang diproses dengan komputer dan dikirim melalui perangkat komunikasi elektronik maka ancaman terhadap pengamanan data semakin meningkat (Kurniawan, 2013). Informasi yang dikirim melalui email apalagi informasi yang bersifat sangat rahasia perlu diamankan salah satunya dengan cara mengenkripsi.

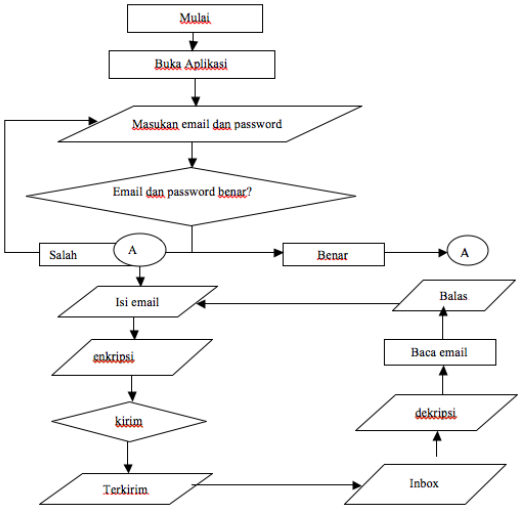
2. METODE PENELITIAN

Langkah dalam pembuatan aplikasi ini adalah *planning*, analisis kebutuhan sistem, mendesain aplikasi, implementasi. Pada tahap *planning* ini terdapat proses perumusan masalah dan mencari data-data yang akurat sebagai penunjang penyelesaiaan masalah. Tahap analisis memuat tentang kebutuhan fungsional pengguna aplikasi, misalnya pada sisi pengirim email ada dibutuhkan proses enkripsi *email* yang akan dikirim kedalam bentuk chipertext sehingga menjadi pesan yang tidak bias dipahami oleh orang lain dan membutuhkan kunci untuk membaca pesan tersebut. Sedangkan kebutuhkan pada sisi penerima pesan terdapat proses dekripsi yaitu proses mengubah *chipertext* menjadi *plaintext* dengan kunci yang telah ditetapkan sehingga pesan menjadi mudah dimengerti penerima. Dengan demikian pengirim *email* yakin kerahasiaan dan keutuhannya terjaga sampai ke penerima.



Gambar 1. Alur Penelitian

Setelah *planning* dan analisis sudah selesai selanjutnya desain. Pada tahapan ini akan dibuat desain yang sesuai dengan kebutuhan user dan diharapakan bisa menyelesaikan masalah yang ada.



Gambar 2. Proses dekripsi dan enkripsi

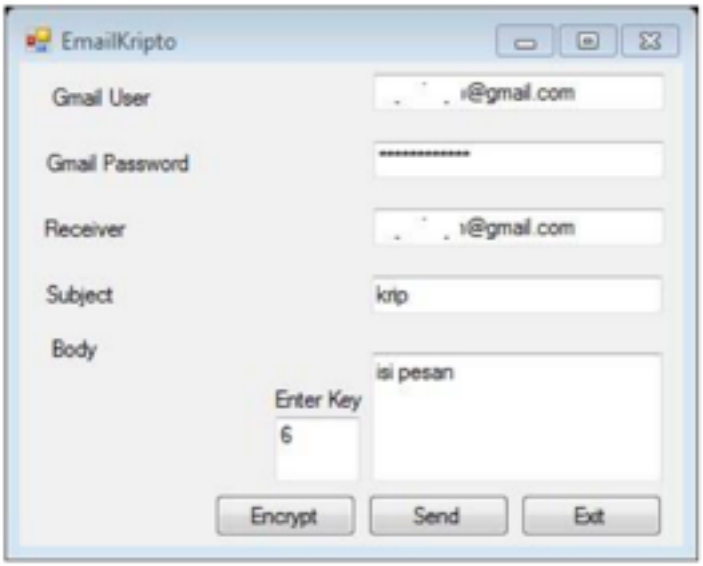
3. HASIL DAN PEMBAHASAN

Untuk mengetahui apakan aplikasi yang dibuat berjalan dengan baik maka akan dilakukan tahap pengujian. Uji coba kali ini menggunakan email dari Gmail. Sebelum menggunakan program pastikan 2Step Verification pada akun Gmail statusnya turn off dan access for less secure appsstatusnya turn on.

Gambar 3. Menu Utama Aplikasi

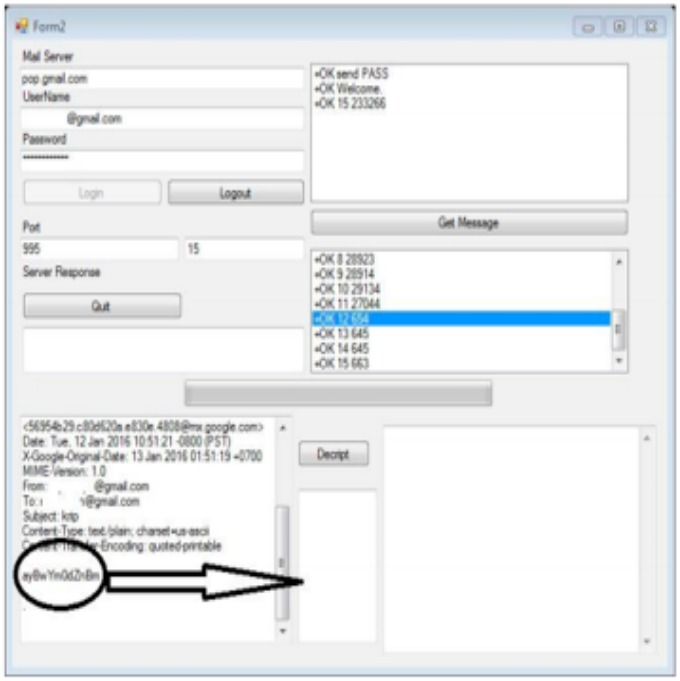
Terdiri dari tiga sub menu dalam menu utama, yaitu sender, receiver dan close. Dalam aplikasi ini terdapat pengirim yang bisa mengirim email dalam bentuk pesan yang sudah terenkripsi dan

receiver sebagai penerima pesan atau email terenkripsi yang bisa mendeskripsi pesan menjadi pesan yang bisa dipahami. Serta menu close untuk menutup aplikasi.



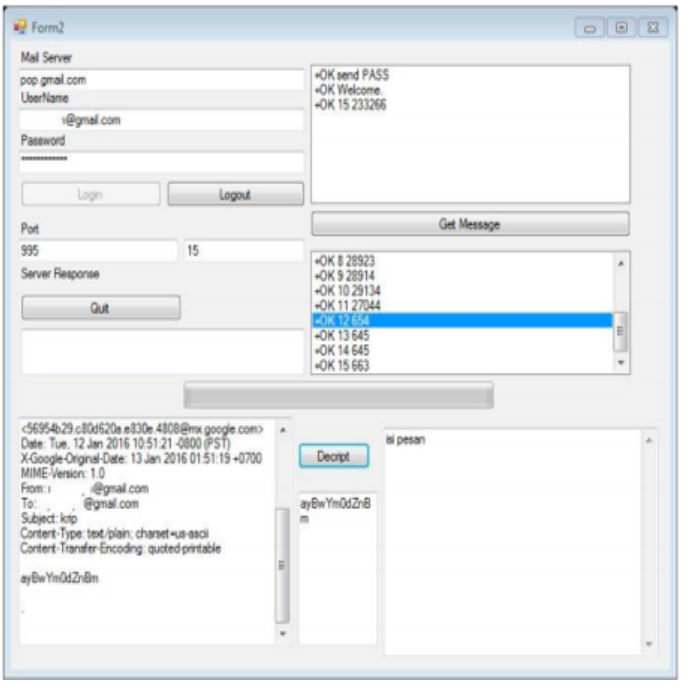
Gambar 4. Pengujian Aplikasi

Pada menu sender atau pengirim terdapat form dengan isian email gmail dan password sender, email dari receiver atau email tujuan, subject pesan, *body* yang merupakan isi email atau pesan, serta terdapat *Enter key* dan *button Encrypt* untuk mengenkripsi pesan didalam *body* tersebut. Kemudaian *button send* untuk mengirim pesan dan *Exit* untuk keluar dari form sender.



Gambar 5. Menu Recaiver

Sebagai penerima pesan atau receiver yang dilakukan pertama kali adalah login email. Kemudian ada button get message bila diklik pada tombol tersebut semua email yang masuk akan tampil semua, contohnya seperti Gambar 5. Klik salah satu email yang ingin dibaca. Isi email beserta data pengirim dan tanggalnya akan muncul di bagian pojok kiri. Contoh isi pesan terenkipsi yang dilingkari.



Gambar 6. Proses Deskripsi

Pesan tersebut akan tidak dimengerti oleh orang lain. Cara mendekripsikannya dengan mengcopy pesan yang akan dideskripsikan kemudian pindahkan kebawa botton Decript lalu klik button Decript maka pesan tersebut menjadi pesan biasa yang bisa dibaca dan dipahami semua orang. Proses enkripsi dan dekripsi dengan aplikasi *email* ini membutuhkan waktu tambahan 1 menit sampai pesan yang diketikan menjadi ciphertext untuk proses enkripsi dan 1 menit untuk mengubah kembali menjadi plaintext.

Tabel 1. Pengujian pada Smartphone yang berbeda

Algoritma	Waktu Proses	Keamanan	Memori
Menggunakan algoritma	1 menit	97 %	450 KB
Tanpa algoritma	Langsung kirim	70 %	400 KB

4. KESIMPULAN

Berikut kesimpulan dari hasil penelitian ini,

1. Lebih aman 97% dari pada tanpa proses enkripsi karena jika tanpa enkripsi bila ada yang mencekal pesan yang dikirim langsung bias dibaca sedangkan jika melalui proses enkripsi harus mendeskripsi dan mencari tau jenis algoritma yang digunakan serta kuncinya.
2. Jika mengunakan proses enkripsi lebih lama karena ketika selesai menulis pesan harus dienkripsi dahulu baru dikirim.

3. Membutuhkan kapasitas yang lebih besar namun masih normal.

DAFTAR PUSTAKA

References

Ariyus Dony, 2006, Kriptografi Keamanan Data dan Komunikasi, Graha Ilmu, Yogyakarta.

Gantini Tiur; Griffin Glenn, 2011, Perancangan dan Implementasi Aplikasi Pencatatan Surat dan Disposisi Pada TAUD Polresta Bandung Barat, Jurnal Sistem Informasi, Vol.6, No. 2, September 2011: 173-183.

Gultom Halasson, 2013, Penyandian email menggunakan algoritma kriptografi wake (Word auto ke encryption), Pelita Informatika Budi darma, Volume: IV, Nomor:1, ISSN : 2301-9425.

Kurniawan Helmi, 2013, Sistem Pengamanan Data Pesan Teks Dengan

Abdullah, S.N.H.S. 2009. Intelligence License Plate Recognition System Based on Multi Feature Extractor and Support Vector Machine, Tesis Dr. Falsafah, Universiti Teknologi Malaysia.