IMPLEMENTASI ALGORITMA SCHMIDT-SAMOA PADA ENKRIPSI DEKRIPSI EMAIL BERBASIS ANDROID

Skripsi

© UKDW

oleh
WILLY RISTANTO
22084396

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2012

IMPLEMENTASI ALGORITMA SCHMIDT-SAMOA PADA ENKRIPSI DEKRIPSI EMAIL BERBASIS ANDROID

Skripsi

Diajukan kepada Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana
Sebagai Salah Satu Syarat dalam Memperoleh Gelar
Sarjana Komputer

Disusun oleh

WILLY RISTANTO
22084396

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2012

© UKDW

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

Implementasi Algoritma Schmidt-Samoa pada Enkripsi Dekripsi Email Berbasis Android

yang saya kerjakan untuk melengkapi sebagian persyaratan menjadi Sarjana Komputer pada pendidikan Sarjana Program Studi Teknik Informatika Fakultas Teknologi Informasi Universitas Kristen Duta Wacana, bukan merupakan tiruan atau duplikasi dari skripsi kesarjanaan di lingkungan Universitas Kristen Duta Wacana maupun di Perguruan Tinggi atau instansi manapun, kecuali bagian yang sumber informasinya dicantumkan sebagaimana mestinya.

Jika dikemudian hari didapati bahwa hasil skripsi ini adalah hasil plagiasi atau tiruan dari skripsi lain, saya bersedia dikenai sanksi yakni pencabutan gelar kesarjanaan saya.

Yogyakarta, 5 November 2012

WILLY RISTANTO
22084396

© UKDW

INTISARI

IMPLEMENTASI ALGORITMA SCHMIDT-SAMOA PADA ENKRIPSI DEKRIPSI EMAIL BERBASIS ANDROID

Saat ini email merupakan alat komunikasi yang umum dipakai oleh banyak orang. Dengan email kita dapat begitu mudah bertukar pesan tanpa batasan jarak dan waktu. Secara umum email tidak menjamin kerahasiaan pesan yang dikirimkan oleh pengguna. Penyampaian pesan email membutuhkan suatu sistem keamanan yang menggunakan teknik penyandian yang disebut dengan kriptografi.

Pada penelitian ini penulis membuat aplikasi email client berbasis android yang mengimplementasikan algoritma Schmidt-Samoa. Algoritma ini termasuk dalam kriptografi kunci publik, dimana kunci publik yang digunakan untuk mengenkripsi pesan berbeda dengan kunci privat yang digunakan untuk melakukan dekripsi pesan. Algoritma ini melakukan proses enkripsi dan dekripsi pesan teks yang mendasarkan pada perhitungan matematika dalam operasi eksponensial dan modulus. Pada aplikasi ini digunakan kunci dalam rentang 512 bit sampai 1024 bit. Penelitian ini menggunakan pesan teks dengan berbagai variasi jumlah karakter dalam rentang 5 – 10.000 karakter untuk mengetahui seberapa cepat proses enkripsi dan dekripsi pesan dengan menggunakan algoritma tersebut.

Aplikasi yang telah dibuat telah mampu melakukan enkripsi dekripsi pesan dengan menggunakan algoritma Schmidt-Samoa. Pada sistem yang telah dibuat, 99,074% data penelitian menunjukkan proses dekripsi lebih cepat dibandingkan proses enkripsi. Untuk pesan teks dengan rentang 5-10.000 karakter yang menggunakan kunci 512 bit, sistem mampu melakukan proses enkripsi dengan waktu 520 – 18.256 milidetik dan proses dekripsi dengan waktu 487 – 5.688 milidetik. Pada kunci 1024 bit, dengan rentang 5 hingga 10.000 karakter, sistem mampu melakukan proses enkripsi dengan waktu 5626 – 52.142 milidetik (7,388 kali lebih lama dibandingkan 512 bit) dan proses dekripsi dengan waktu 5463 – 15.808 milidetik atau 8,290 kali lebih lama dibandingkan 512 bit.

Kata kunci : Schmidt-Samoa, Enkripsi, Dekripsi, Android.

© UKDW

HALAMAN PERSETUJUAN

Judul Skripsi	:	Implementasi Algoritma Schmidt-Samoa pada Enkripsi Dekripsi Email Berbasis Android
Nama Mahasiswa	:	WILLY RISTANTO
N I M	:	22084396
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Gasal
Tahun Akademik	:	2012/2013

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 5 November 2012

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, SKom.,M.Cs	Antonius Rachmat C., SKom.,M.Cs

© UKDW

HALAMAN PENGESAHAN

IMPLEMENTASI ALGORITMA SCHMIDT-SAMOA PADA ENKRIPSI DEKRIPSI EMAIL BERBASIS ANDROID

Oleh: WILLY RISTANTO / 22084396

Dipertahankan di depan Dewan Penguji Skripsi
Program Studi Teknik Informatika Fakultas Teknologi Informasi
Universitas Kristen Duta Wacana - Yogyakarta
Dan dinyatakan diterima untuk memenuhi salah satu syarat memperoleh gelar
Sarjana Komputer
pada tanggal 23 November 2012

Yogyakarta, 13 Desember 2012
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, SKom.,M.Cs
2. Antonius Rachmat C., SKom.,M.Cs
3. Rosa Delima, S.Kom., M.Kom.
4. Theresia Herlina R., S.Kom.,M.T.

Dekan

(Drs. Wimmie Handiwidjojo, MIT.)

Ketua Program Studi

(Nugroho Agus Haryono, M.Si)

© UKDW

DAFTAR ISI

© UKDW

© UKDW

DAFTAR TABEL

© UKDW

DAFTAR GAMBAR

© UKDW

DAFTAR GRAFIK

© UKDW

INTISARI

IMPLEMENTASI ALGORITMA SCHMIDT-SAMOA PADA ENKRIPSI DEKRIPSI EMAIL BERBASIS ANDROID

Saat ini email merupakan alat komunikasi yang umum dipakai oleh banyak orang. Dengan email kita dapat begitu mudah bertukar pesan tanpa batasan jarak dan waktu. Secara umum email tidak menjamin kerahasiaan pesan yang dikirimkan oleh pengguna. Penyampaian pesan email membutuhkan suatu sistem keamanan yang menggunakan teknik penyandian yang disebut dengan kriptografi.

Pada penelitian ini penulis membuat aplikasi email client berbasis android yang mengimplementasikan algoritma Schmidt-Samoa. Algoritma ini termasuk dalam kriptografi kunci publik, dimana kunci publik yang digunakan untuk mengenkripsi pesan berbeda dengan kunci privat yang digunakan untuk melakukan dekripsi pesan. Algoritma ini melakukan proses enkripsi dan dekripsi pesan teks yang mendasarkan pada perhitungan matematika dalam operasi eksponensial dan modulus. Pada aplikasi ini digunakan kunci dalam rentang 512 bit sampai 1024 bit. Penelitian ini menggunakan pesan teks dengan berbagai variasi jumlah karakter dalam rentang 5 – 10.000 karakter untuk mengetahui seberapa cepat proses enkripsi dan dekripsi pesan dengan menggunakan algoritma tersebut.

Aplikasi yang telah dibuat telah mampu melakukan enkripsi dekripsi pesan dengan menggunakan algoritma Schmidt-Samoa. Pada sistem yang telah dibuat, 99,074% data penelitian menunjukkan proses dekripsi lebih cepat dibandingkan proses enkripsi. Untuk pesan teks dengan rentang 5-10.000 karakter yang menggunakan kunci 512 bit, sistem mampu melakukan proses enkripsi dengan waktu 520 – 18.256 milidetik dan proses dekripsi dengan waktu 487 – 5.688 milidetik. Pada kunci 1024 bit, dengan rentang 5 hingga 10.000 karakter, sistem mampu melakukan proses enkripsi dengan waktu 5626 – 52.142 milidetik (7,388 kali lebih lama dibandingkan 512 bit) dan proses dekripsi dengan waktu 5463 – 15.808 milidetik atau 8,290 kali lebih lama dibandingkan 512 bit.

Kata kunci : Schmidt-Samoa, Enkripsi, Dekripsi, Android.

© UKDW

Bab I
PENDAHULUAN

1.1 Latar Belakang

Saat ini email merupakan alat komunikasi yang umum dipakai oleh banyak orang. Dengan email kita dapat begitu mudah bertukar pesan tanpa batasan jarak dan waktu. Secara umum email tidak menjamin kerahasiaan pesan yang dikirimkan oleh pengguna. Suatu pesan teks yang dikirim dapat bersifat rahasia atau pribadi, sehingga pengguna menginginkan pesan email tersebut tidak ingin diketahui oleh pihak-pihak yang tidak memiliki hak atau wewenang untuk mengaksesnya.

Penyampaian pesan email membutuhkan suatu sistem keamanan. Pembuatan sistem keamanan tersebut menggunakan suatu teknik penyandian yang disebut dengan kriptografi. Dalam kriptografi terdapat dua konsep utama yakni enkripsi dan dekripsi. Enkripsi adalah proses mengamankan suatu informasi / pesan dengan suatu algoritma tertentu yang membuat informasi tersebut tidak dapat dibaca. Supaya pesan tersebut dapat dibaca, dilakukan proses yang disebut dengan dekripsi . Dekripsi adalah kebalikan dari enkripsi yaitu mengubah kembali bentuk tersamar tersebut menjadi informasi awal. Dalam melakukan proses dekripsi pesan dibutuhkan suatu pengetahuan khusus, yaitu kunci.

Pada penelitian ini akan dibuat suatu aplikasi yang mengimplementasikan teknik kriptografi. Penerapan kriptografi ini akan difokuskan bagaimana kriptografi dapat mengamankan pesan email dengan tetap memperhatikan integritas pesan yang menggunakan algoritma Schmidt-Samoa. Algoritma ini mendasarkan pada perhitungan matematika dalam operasi eksponensial dan modulus.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dikemukakan sebelumnya, masalah yang akan diteliti penulis adalah : Bagaimana mengimplementasikan algoritma Schmidt-Samoa untuk mengamankan pesan dalam email?

© UKDW

1.3 Batasan Masalah

Batasan dalam sistem ini adalah sebagai berikut :

- Panjang kunci terletak antara 512 bit dan 1024 bit
- Kode ASCII yang dienkripsi dalam rentang 0-255
- Platform yang digunakan adalah Android
- Pesan yang dikirimkan dalam bentuk teks

1.4 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengamankan pesan email supaya hanya dapat dibaca oleh orang yang dimaksud dengan mengimplementasikan algoritma Schmidt-Samoa.

1.5 Metode Penelitian

Metode yang digunakan di penelitian ini adalah :

1. Studi Pustaka

Studi Pustaka bertujuan untuk memberikan pengetahuan mengenai hal – hal yang terkait dengan enkripsi, kriptografi kunci publik dan algoritma Schmidt-Samoa yang digunakan untuk membantu penyelesaian Tugas Akhir ini. Studi Pustaka dilakukan dengan cara membaca buku, literatur, jurnal dan artikel dari internet yang berhubungan dengan masalah yang dibahas.

2. Konsultasi

Melakukan konsultasi dengan dosen pembimbing yang menguasai materi terkait, khususnya dengan kesulitan yang ditemui saat pelaksanaan Tugas Akhir.

3. Pembuatan sistem dengan langkah langkah sebagai berikut :

a. Mengindentifikasi permasalahan
b. Perancangan Desain Aplikasi dan Antarmuka
c. Pembuatan sistem
d. Pengujian Program dan evaluasi

© UKDW

e. Pelaporan

1.6 Sistematika Penulisan

Laporan ini memiliki sistematika penulisan yang terbagi menjadi 5 bab yaitu :

Bab 1 Pendahuluan , berisi mengenai gambaran umum mengenai apa yang diteliti dalam penulisan tugas akhir ini.

Bab 2, Tinjauan Pustaka, berisi landasan teori yang digunakan dalam penelitian ini dan penjelasan algoritma yang digunakan dalam pengembangan sistem ini.

Bab 3, Analisis dan Perancangan Sistem, berisi penjelasan mengenai sistem yang akan dibuat, seperti kebutuhan hardware dan software, arsitektur sistem, spesifikasi sistem, desain sistem dan rancangan antar muka sistem.

Bab 4, Implementasi dan Analisis Sistem, berisi pembahasan implementasi dan pengujian sistem yang telah dibuat beserta analisisnya.

Bab 5, Kesimpulan dan Saran, berisi kesimpulan dan saran dari hasil penelitian yang telah dilakukan.

© UKDW

Bab V
KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan analisis sistem, maka diperoleh kesimpulan sebagai berikut :

1. Sistem telah dapat mengimplementasikan sistem keamanan dalam pesan email dengan menggunakan algoritma Schmidt-Samoa.
2. Berdasarkan hasil penelitian proses dekripsi pesan 97,67% lebih singkat dibandingkan proses enkripsi, disebabkan karena pada proses enkripsi sebelum dilakukan perhitungan matematis, dilakukan proses padding terlebih dahulu.
3. Dibandingkan dengan kunci 512 bit, sistem pada kunci 1024 bit melakukan proses enkripsi 8,43 kali lebih lama dan proses dekripsi 9,34 kali lebih lama, dan *ciphertext* yang dihasilkan 99,637% lebih panjang.
4. Peningkatan jumlah karakter plaintext yang dienkripsi, belum tentu akan diikuti peningkatan waktu proses enkripsi dan dekripsi. Tetapi untuk setiap rentang 100 karakter pesan dienkripsi, waktu rata-rata proses enkripsi dan dekripsi akan selalu meningkat. Pada kunci 512 bit, proses enkripsi rata-rata meningkat 10,288% dan proses dekripsi rata-rata meningkat 3,74% dalam setiap rentang 100 karakter. Sedangkan pada kunci 1024 bit, proses enkripsi rata-rata meningkat 5,90% dan proses dekripsi meningkat 1,75% dalam setiap rentang 100 karakter.

5.2 Saran

Adapun saran untuk pengembangan sistem ini adalah sebagai berikut :

1. Pesan yang dikirimkan dapat diinputkan dalam text editor WYSIWYG.
2. Sistem dapat digunakan tidak hanya untuk email Gmail dan Yahoo saja tetapi juga untuk email lainnya.
3. Karakter pesan yang dienkripsi sebaiknya lebih luas cakupannya tidak hanya kode ASCII 0-255 saja.

© UKDW

DAFTAR PUSTAKA

Coppersmith, D. (2001). *Finding Small Solutions to Small Degree Polynomials.* Diakses 5 September 2012, dari http://cr.yp.to/bib/2001/coppersmith.pdf

Diffie, W. & Hellman, M.E. (1976). *New Directions in Cryptography.* Diakses 5 September 2012, dari http://www.cs.berkeley.edu/~christos/classics/diffiehellman.pdf

Forouzan, Behrouz.A.(2008). *Cryptography* and Network Security;McGraw-Hill.

Lehtinen, R.,Deborah Russel,G.T. Gangemi Sr.(2006). *Computer Security Basics*; O'Reilly Media Inc.

LinuxMail. (2007). How Email Works. Diakses 5 September 2012, dari http://www.linuxmail.info/how-email-works/

Schmidt-Samoa, K.(2006). *A New Rabin-type Trapdoor Permutation Equivalent to Factoring and Its Applications.*Diakses 4 Juli 2012 dari http://eprint.iacr.org/2005/278.pdf

Stallings, William. (2006). *Cryptography and Network Security Principles and Practices 4th Edition;* Pearson Prentice Hall.

Techotopia.com.(2011*).An Overview of the Kindle Fire Android Architecture.* Diakses 5 September 2012, dari http://www.techotopia.com/index.php/An_Overview_of_the_Kindle_Fire_Android_Architecture.

© UKDW