IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

Skripsi

oleh
DESSY SUTANTI
71110020

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

©UKDW

IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

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

DESSY SUTANTI
71110020

PROGRAM STUDI TEKNIK INFORMATIKA FAKULTAS TEKNOLOGI INFORMASI
UNIVERSITAS KRISTEN DUTA WACANA
2015

©UKDW

PERNYATAAN KEASLIAN SKRIPSI

Saya menyatakan dengan sesungguhnya bahwa skripsi dengan judul:

IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

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, 15 Juni 2015

DESSY SUTANTI
71110020

©UKDW

iii

HALAMAN PERSETUJUAN

Judul Skripsi	:	IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA
Nama Mahasiswa	:	DESSY SUTANTI
N I M	:	71110020
Matakuliah	:	Skripsi (Tugas Akhir)
Kode	:	TIW276
Semester	:	Genap
Tahun Akademik	:	2014/2015

Telah diperiksa dan disetujui di
Yogyakarta,
Pada tanggal 15 Juni 2015

Dosen Pembimbing I	Dosen Pembimbing II
Willy Sudiarto Raharjo, S.Kom.,M.Cs.	Junius Karel, M.T.

©UKDW

iv

HALAMAN PENGESAHAN

IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

Oleh: DESSY SUTANTI / 71110020

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 12 Juni 2015

Yogyakarta, 15 Juni 2015
Mengesahkan,

Dewan Penguji:

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs.
2. Junius Karel, M.T.
3. Aloysius Airlangga Bajuadji, S.Kom., M.Eng.
4. Aditya Wikan Mahastama, S.Kom

Dekan	Ketua Program Studi
(Budi Susanto, S.Kom., M.T.)	(Gloria Virginia, Ph.D.)

©UKDW

v

UCAPAN TERIMA KASIH

Puji dan syukur penulis panjatkan ke hadirat Tuhan Yang Maha Esa yang telah melimpahkan rahmat dan anugerah, sehingga penulis dapat menyelesaikan Tugas Akhir dengan judul Implementasi *Zero Knowledge Proof* Menggunakan Protokol *Feige-Fiat Shamir* Untuk Verifikasi Tiket Rahasia.

Dalam menyelesaikan pembuatan program dan laporan Tugas Akhir ini, penulis telah banyak menerima bimbingan, saran, dan masukan dari berbagai pihak, baik secara langsung maupun tidak langsung. Untuk itu dengan segala kerendahan hati, pada kesempatan ini penulis menyampaikan ucapan terima kasih kepada :

1. Willy Sudiarto Raharjo, S.Kom.,M.Cs. selaku dosen pembimbing I yang telah memberikan bimbingannya dengan sabar dan baik kepada penulis.
2. Junius Karel, M.T. selaku dosen pembimbing II atas bimbingannya, petunjuk dan masukan yang diberikan selama pengerjaan tugas akhir ini.
3. Keluarga tercinta yang telah memberi dukungan dan semangat.
4. Teman-teman terdekat yang selalu berjuang bersama selama 4 tahun yang telah memberikan dukungan dan semangat.
5. Alexander, yang memberikan saran dan kritik dalam perancangan dan pembuatan sistem, serta dukungan dan semangat yang selama ini tidak pernah berhenti mengalir.
6. Teman-teman lain yang tidak dapat disebutkan satu per satu, terima kasih atas dukungan dan doa kalian.
7. Pihak lain yang tidak dapat disebutkan satu per satu, sehingga Tugas Akhir ini dapat terselesaikan dengan baik.

Penulis menyadari bahwa program dan laporan Tugas Akhir ini masih jauh dari sempurna. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun dari pembaca sekalian, sehingga suatu saat penulis dapat memberikan karya yang lebih baik lagi.

©UKDW

Akhir kata penulis ingin meminta maaf apabila ada kesalahan baik dalam penyusunan laporan maupun yang pernah penulis lakukan sewaktu membuat program Tugas Akhir.

Yogyakarta, 17 Juni 2015

Penulis

©UKDW

INTISARI

IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

Keamanan dalam pengiriman dan penerimaan informasi sangat dibutuhkan pada masa sekarang ini. Salah satu bentuk proses pengiriman informasi yang membutuhkan pengamanan adalah tiket. Tiket yang dimaksud merupakan sebuah kunci utama untuk mendapatkan akses masuk dan hanya diketahui oleh pihak berwenang. Namun terdapat beberapa resiko kecurangan yang dapat dilakukan pihak lain, seperti membuat tiket palsu atau bahkan menggandakan tiket.

Untuk mengatasi permasalahan tersebut, maka penulis mengimplementasikan *Zero Knowledge Proof* dengan protokol *Feige-Fiat Shamir* pada sistem yang dibuat. *Zero Knowledge Proof* akan menjamin bahwa pihak yang tidak berwenang tidak akan mendapatkan informasi penting apapun baik pada saat proses pembuatan tiket maupun pada proses verifikasi tiket. Dengan penerapan *Zero Knowledge Proof* dan *Feige-Fiat Shamir* pada sistem maka akan memperkecil kemungkinan terjadi pemalsuan atau penggandaan tiket.

Berdasarkan penelitian yang telah dilakukan, hasil verifikasi selalu memenuhi ketiga syarat *Zero Knowledge Proof*, yaitu *completeness* (membuktikan kepemilikannya terhadap tiket), *soundness* (apabila gagal verifikasi maka tidak akan pernah mendapatkan akses masuk), dan *Zero Proof* (*verifier* percaya bahwa tiket memang milik *prover* namun *verifier* tidak mengetahui informasi apapun mengenai tiket tersebut). Keamanan proses verifikasi terdapat pada enkripsi file kode rahasia (representasi kunci privat), dimana proses verifikasi membutuhkan kata sandi yang hanya diketahui oleh *prover*, sehingga kemungkinan untuk pemalsuan / penggandaan tiket oleh pihak tidak berwenang sangat kecil.

Kata kunci : *Zero Knowledge Proof, Feige-Fiat Shamir*, verifikasi

©UKDW

DAFTAR ISI

©UKDW

©UKDW

BAB 5 KESIMPULAN DAN SARAN

©UKDW

DAFTAR TABEL

©UKDW

DAFTAR GAMBAR

©UKDW

©UKDW

DAFTAR LAMPIRAN

©UKDW

INTISARI

IMPLEMENTASI ZERO KNOWLEDGE PROOF MENGGUNAKAN PROTOKOL FEIGE-FIAT SHAMIR UNTUK VERIFIKASI TIKET RAHASIA

Keamanan dalam pengiriman dan penerimaan informasi sangat dibutuhkan pada masa sekarang ini. Salah satu bentuk proses pengiriman informasi yang membutuhkan pengamanan adalah tiket. Tiket yang dimaksud merupakan sebuah kunci utama untuk mendapatkan akses masuk dan hanya diketahui oleh pihak berwenang. Namun terdapat beberapa resiko kecurangan yang dapat dilakukan pihak lain, seperti membuat tiket palsu atau bahkan menggandakan tiket.

Untuk mengatasi permasalahan tersebut, maka penulis mengimplementasikan *Zero Knowledge Proof* dengan protokol *Feige-Fiat Shamir* pada sistem yang dibuat. *Zero Knowledge Proof* akan menjamin bahwa pihak yang tidak berwenang tidak akan mendapatkan informasi penting apapun baik pada saat proses pembuatan tiket maupun pada proses verifikasi tiket. Dengan penerapan *Zero Knowledge Proof* dan *Feige-Fiat Shamir* pada sistem maka akan memperkecil kemungkinan terjadi pemalsuan atau penggandaan tiket.

Berdasarkan penelitian yang telah dilakukan, hasil verifikasi selalu memenuhi ketiga syarat *Zero Knowledge Proof*, yaitu *completeness* (membuktikan kepemilikannya terhadap tiket), *soundness* (apabila gagal verifikasi maka tidak akan pernah mendapatkan akses masuk), dan *Zero Proof* (*verifier* percaya bahwa tiket memang milik *prover* namun *verifier* tidak mengetahui informasi apapun mengenai tiket tersebut). Keamanan proses verifikasi terdapat pada enkripsi file kode rahasia (representasi kunci privat), dimana proses verifikasi membutuhkan kata sandi yang hanya diketahui oleh *prover*, sehingga kemungkinan untuk pemalsuan / penggandaan tiket oleh pihak tidak berwenang sangat kecil.

Kata kunci : *Zero Knowledge Proof, Feige-Fiat Shamir*, verifikasi

©UKDW

BAB 1
PENDAHULUAN

1.1 Latar Belakang

Dalam pengiriman informasi dengan beberapa teknik kriptografi, kita membutuhkan suatu cara agar informasi yang ingin kita sampaikan dapat diterima dengan aman oleh orang yang memang berwenang mendapatkannya. Saat seseorang menerima atau mengirimkan pesan, terdapat tiga persoalan yang sangat penting, yaitu kerahasian, autentifikasi, dan keutuhan. Kerahasian memberi garansi data tidak dapat dibaca oleh orang yang tidak berkepentingan. Autentifikasi memberi garansi tentang keaslian data dan dengan siapa berhubungan. Keutuhan memberi garansi bahwa data tidak mengalami perubahan sewaktu perjalanan, atau dengan kata lain data yang dikirim adalah data yang diterima.

Salah satu contoh penerapan yang membutuhkan kemanan dalam pengiriman dan penerimaan adalah tiket. Tiket seharusnya hanya diketahui oleh pemilik tiket serta pihak yang mengirimkan tiket tersebut. Dalam studi kasus tugas akhir ini, informasi yang dikirimkan terdiri dari dua jenis, yang pertama adalah tiket (representasi kunci publik) dan tiket rahasia (representasi kunci privat). Tiket pertama bersifat publik sehingga dapat dibaca oleh siapapun, sedangkan untuk proses verifikasi diperlukan tiket rahasia yang hanya diketahui *prover*. Namun terdapat beberapa resiko kecurangan yang dapat dilakukan pihak lain seperti membuat tiket palsu atau bahkan menggandakan tiket.

Untuk menghindari kecurangan, maka diperlukan verifikasi tiket dengan menggunakan *Zero Knowledge Proof* dan protokol *Feige-Fiat Shamir*. Di dalam penerapannya, terdapat tiga *stakeholder* yaitu pemilik tiket, *verifier (*diasumsikan sebagai penjaga), dan pihak ketiga (*arbiter*) yang mengatur proses pengiriman tiket dan tiket rahasia. Pemilik tiket disebut sebagai *prover* yang akan membuktikan kepada *verifier* bahwa tiket tersebut memang asli, sedangkan *verifier* yang bertugas memastikan keaslian tiket (melakukan verifikasi).

©UKDW

1.2 Rumusan Masalah

Perumusan masalah yang menjadi dasar penulisan tugas akhir ini yaitu :

a. Bagaimana proses verifikasi tiket agar kerahasiaan tiket tetap terjaga ?
b. Bagaimana mencegah duplikasi tiket oleh pihak *verifier ?*
c. Bagaimana memastikan bahwa pihak *verifier* melakukan verifikasi dengan benar ?
d. Bagaimana cara mengidentifikasi pihak yang tidak memiliki tiket atau memalsukan tiket ?

1.3 Batasan Sistem

Agar tulisan ini tidak menyimpang dari ruang lingkup pembahasan, diperlukan batasan masalah sebagai berikut :

a. Protokol Z*ero Knowledge Proof* yang digunakan untuk melakukan pembuktian adalah protokol *Feige-Fiat Shamir.*
b. *Arbiter* merupakan *trusted third party.*
c. Kerahasiaan dan integritas tiket sepenuhnya menjadi tanggung jawab pemilik tiket.
d. Adanya jalur komunikasi yang aman antara *arbiter* dengan *prover* dan *arbiter* dengan *verifier.*

1.4 Tujuan Penelitian

Tujuan dari penulisan tugas akhir ini adalah membangun sistem yang mengimplementasikan *Zero Knowledge Proof* dengan protokol *Feige-Fiat Shamir.*

1.5 Metode Penelitian

Tahapan yang dilakukan dalam penelitian ini adalah :

1. Mengumpulkan bahan-bahan referensi

   Mengumpulkan dan mempelajari bahan-bahan referensi yang berhubungan dengan kriptografi, *Zero Knowledge Proof,* Protokol *Feige-Fiat-Shamir.*
2. Analisis Masalah dan Perancangan Sistem

©UKDW

Melakukan analisis masalah yang dimulai dengan identifikasi masalah, memahami kerja sistem yang akan dibuat, menganalisis dan membuat laporan tentang hasil analisis, serta membuat rancangan dan *interface* sistem.

3. Implementasi Sistem

   Perancangan sistem diimplementasikan dalam bentuk kode program *(coding).*

4. Pengujian Sistem

   Pengujian dilakukan terhadap program yang telah dibuat.

5. Dokumentasi Sistem

   Penyusunan laporan tugas akhir lengkap dengan analisis yang didapatkan.

1.6 Sistematika Penulisan

Sistematika penulisan pada tugas akhir ini adalah :

BAB 1 PENDAHULUAN

Bab ini menjelaskan latar belakang masalah, rumusan masalah, batasan sistem, tujuan penelitian, metode penelitian, dan sistematika penulisan dari tugas akhir ini.

BAB 2 TINJAUAN PUSTAKA

Bab ini menjelaskan penelitian-penelitian yang pernah dilakukan sebelumnya mengenai *Zero Knowledge Proof* dan *Feige-Fiat Shamir*, serta menjelaskan teori mengenai kriptografi, *Zero Knowledge Proof* dan protokol *Feige-Fiat Shamir*.

BAB 3 ANALISIS DAN PERANCANGAN SISTEM

Pada bab ini akan dijelaskan mengenai analisis dan perancangan yang terdapat dalam sistem, digambarkan dalam bentuk diagram alir, *activity* diagram, *mockup* (perancangan *interface* / antarmuka sistem).

BAB 4 IMPLEMENTASI DAN ANALISIS SISTEM

Bab ini menguraikan hasil implementasi dari sistem yang telah dibuat, antara lain *interface* / antarmuka sistem, serta pengujian dan analisis. Analisis dilakukan terhadap proses verifikasi dari protokol *Feige-Fiat Shamir* yang telah diimplementasikan ke dalam sistem.

BAB 5 KESIMPLUAN DAN SARAN

Bab ini berisi kesimpulan yang didapat dari hasil pengujian yang dilakukan serta saran-saran yang diberikan untuk penelitian selanjutnya.

©UKDW

BAB 5

KESIMPULAN DAN SARAN

5.1 Kesimpulan

Berdasarkan hasil implementasi dan analisis yang telah dibuat dibahas pada bab sebelumnya, maka dapat disimpulkan sebagai berikut :

1. Proses verifikasi tiket menggunakan protokol *Feige-Fiat Shamir* dapat berjalan dengan baik dan aman. Salah satu keamanan proses verifikasi terdapat pada enkripsi file kode rahasia (representasi kunci privat). Sebelum memulai verifikasi, file kode rahasia harus didekripsi terlebih dahulu menggunakan kata sandi yang hanya diketahui oleh *prover*, sehingga kemungkinan untuk pemalsuan / penggandaan tiket oleh pihak tidak berwenang sangat kecil.
2. Pihak *verifier* tidak dapat mencurangi tiket rahasia, karena saat proses verifikasi sistem memerlukan kata sandi yang hanya diketahui oleh *prover*. Walaupun *verifier* memalsukan tiket, namun sistem tetap mengenali tiket tersebut sebagai tiket palsu, sehingga hasil yang dikeluarkan oleh sistem akan memberikan keputusan yang tepat (memberikan akses atau tidak). Keberhasilan sistem mengenali tiket palsu ini didapatkan melalui hasil penghitungan dengan protokol *Feige-Fiat Shamir*.
3. Tiket rahasia dan kata sandi menjadi kunci utama yang dimiliki oleh *prover* untuk melakukan verifikasi. Dengan kata lain jika ada pihak yang tidak memiliki tiket rahasia dan kata sandi namun mencoba untuk melakukan verifikasi, maka sistem akan mengidentifikasi pihak tersebut menggunakan tiket palsu.
4. Dalam proses verifikasi, *prover* selalu dapat membuktikan kepemilikannya terhadap tiket (*completeness*) dan apabila gagal verifikasi maka tidak akan mendapatkan akses masuk (*soundness*).
5. Proses pembuatan tiket belum maksimal dari segi waktu, hal ini disebabkan karena pemanggilan fungsi *great common divisor* berulang kali.

©UKDW

5.2 Saran

Saran yang diberikan untuk perbaikan sistem adalah :

1. Optimalisasi waktu pembuatan tiket, sehingga jika menggunakan angka random yang cukup besar, sistem dapat berjalan lebih cepat.
2. Jika optimalisasi sudah berhasil dilakukan, maka angka random dapat diperbesar sehingga data tiket semakin sulit dipalsukan.

©UKDW

Daftar Pustaka

Aronsson, H.A. (1995). Zero Knowledge Protocols and Small System. Department of Computer Science : Helsinki University of Technology.

Boneh, D. (2012). Intro Number Theory. California : Standford University.

Franco, J. (2009). Feige-Fiat-Shamir Zero Knowledge Proof. Ohio : University of Cincinnati.

Gunawan, T. (2012). Sistem Otentikasi Berbasis Zero Knowledge Protocol Pada Sistem Operasi Android. Salatiga : Universitas Kristen Satya Wacana

Huqing, Wang & Zhixin, Sun. (2013). Research on Zero-Knowledge Proof Protocol. Nanjing : International Journal of Computer Science Issues (IJCSI).

Knapp, J. (2009). Overview of Zero Knowledge Protocols. New York : Rochester Institute of Technology.

Mollin, R.A. (2007). An Introduction to Cryptography (2nd edition). Florida: Chapman & Hall/CRC.

Munir, R. (2004). Teori Bilangan (Number Theory). Bandung : Departemen Teknik Informatika Institut Teknologi Bandung

Raffo, D. (2012). Digital Certificates and the Feige-Fiat Shamir Zero Knowledge Protocol. France : Traineeship report.

Schneier, B. (1996). Applied Cryptography : Protocols, Algorithms, and Source Code in C (2nd edition). New Jersey : John Wiley & Sons,Inc.

©UKDW

Sidiq, A.Z. (2007). Perbandingan Algoritma RSA dan Algoritma berbasis Zero Knowledge untuk Autentikasi pada SmartCard. Bandung : Institut Teknologi Bandung.

Situngkir, T.N. (2013). Implementasi Zero Knowledge Proof dengan Feige Fiat Shamir dan Quadratic Linear Congruential Generator (Skripsi). Medan : Universitas Sumatera Utara.

Wong, Chung Kei & Lam, Simon S. (1999). Digital Signatures for Flows and Multicasts. Austin : University of Texas at Austin.

©UKDW