# Sistema de SMS Seguro
# PCS2050 - Projeto de Formatura II
# Apresentação Final

Eduardo de Souza Cruz
Geovandro Carlos Crepaldi Firmino Pereira
Rodrigo Rodrigues da Silva
Orientador: Prof. Dr. Paulo S. L. M. Barreto

Departamento de Engenharia de Computação e Sistemas Digitais
Escola Politécnica da Universidade de São Paulo

São Paulo, 09/12/2008

# Agenda

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)

- Plataforma leve e barata, com grande base de usuários:

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

  72,5 bilhões de dólares para operadoras em 2006

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

  72,5 bilhões de dólares para operadoras em 2006
- Ausência de uma solução universalmente adotada.

# Motivação e Cenário

- Crescimento do uso do SMS no mundo:

  2,3 trilhões de mensagens em 2010 (previsão)
- Plataforma leve e barata, com grande base de usuários:

  2,4 bilhões de pessoas
- Diversas oportunidades econômicas:

  72,5 bilhões de dólares para operadoras em 2006
- Ausência de uma solução universalmente adotada.
- Possibilidade de produzir pesquisa: inovação

# Objetivo

"Projetar, implementar e implantar um sistema capaz de prover confidencialidade, integridade e autenticidade ao serviço de *SMS* sem extrapolar as limitações de recursos típicas do ambiente."

# Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos

# Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema

# Metodologia

- Estudo do cenário, detalhamento do problema e levantamento de requisitos
- Estudo de esquemas de segurança em busca de uma solução adequada ao problema
- Projeto, implementação e testes

# Agenda

# Aplicações Potenciais

- Comunicação interpessoal

# Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos

# Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa

# Aplicações Potenciais

- Comunicação interpessoal
- Transações bancárias e pagamentos
- Comunicação corporativa e governamental sigilosa
- Monitoração remota

# Serviços de Segurança

- Confidencialidade

# Serviços de Segurança

- Confidencialidade
- Integridade

# Serviços de Segurança

- Confidencialidade
- Integridade
- Autenticidade

# Serviços de Segurança

- Confidencialidade
- Integridade
- Autenticidade
- Irretratabilidade

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado
- *RSA*: cerca de *20 mensagens* para trocar *um* certificado

# Definição do Problema

- SMS armazenado em aberto nas integradoras e operadoras
- Recursos limitados: processamento, memória, largura de banda
- Algoritmo *A5* da rede *GSM* quebrado
- Poucas soluções de segurança no mercado
- *RSA*: cerca de *20 mensagens* para trocar *um* certificado
- Algoritmos simétricos: Dificuldade em gerenciar as chaves

# Métricas e Requisitos

- Tempo de espera

# Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem

# Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem
- Tamanho da chave

# Métricas e Requisitos

- Tempo de espera
- Espaço útil da mensagem
- Tamanho da chave
- *Overhead* do protocolo

# Agenda

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado
- Publicação de artigo no SBSEG'08 definindo o novo esquema

# Esquema de segurança desenvolvido

Ao longo do trabalho, foi bolado um esquema de segurança inovador

- Curvas elípticas
- Chaves menores
- Criptografia auto-certificada
- Criptografia baseada em identidades
- Gerenciamento de chaves simplificado
- Publicação de artigo no SBSEG'08 definindo o novo esquema
- Publicação de artigo no WTICG'08 sobre o nosso projeto de formatura (menção honrosa)

# Arquitetura

# Agenda

# Classes

- Esquema implementado em J2ME

# Classes

- Esquema implementado em J2ME
- Testes de viabilidade: OK

# Classes

- Esquema implementado em J2ME
- Testes de viabilidade: OK
- Implementação de protocolo de mensagens

# Classes

- Esquema implementado em J2ME
- Testes de viabilidade: OK
- Implementação de protocolo de mensagens
- Implementação de persistência: Floggy

# Classes

# Resultados

# Agenda

# Conclusão

- Projeto motivou a criação de um esquema criptográfico inovador

# Conclusão

- Projeto motivou a criação de um esquema criptográfico inovador
- Solução implementada com sucesso, alta portabilidade

aplic

# Contato

## Site do projeto

**http://secure-sms.googlecode.com**

## E-mail

**secure-sms@googlegroups.com**