# Construção de um Sistema de SMS Seguro

**Eduardo de Souza Cruz**[1], **Geovandro C. F. Pereira**[1],
**Rodrigo Rodrigues da Silva**[1], **Paulo S. L. M. Barreto**[1]*.

[1] Departamento de Engenharia de Computação e Sistemas Digitais,
Escola Politécnica, Universidade de São Paulo, Brasil.
{eduardo.cruz,geovandro.pereira,rodrigo.silva1}@poli.usp.br, pbarreto@larc.usp.br

***Resumo.*** *Este trabalho consiste na especificação e implementação de um sistema que garanta serviços de segurança na troca de mensagens SMS entre aparelhos de telefonia celular. Ao longo da monografia, apresentaremos aspectos da nossa solução, um esquema criptográfico inovador que viabilizou a implementação, métricas, resultados de testes de desempenho, além de considerações sobre o andamento do trabalho.*

## 1. Introdução

Atualmente não existem soluções universalmente adotadas para garantir segurança em mensagens SMS. Pelo método tradicional, as mensagens trafegam pela rede celular de forma insegura, passando obrigatoriamente por pelo menos um intermediário não 100% confiável: a operadora do serviço de telefonia. As mensagens podem ficar armazenadas em texto plano no banco de dados da operadora [Ng 2006], de forma que pessoas mal intencionadas infiltradas no sistema podem ser capazes de visualizar, alterar e até enviar mensagens em nome de outra pessoa. Há também outros métodos para interceptar mensagens SMS. [Enck et al. 2005].

O sistema desenvolvido foi designado por "Aplicativo Seguro de SMS", ou, em uma forma abreviada e internacionalizada mais adequada ao mercado, "Secure-SMS", ou ainda "SSMS". O objetivo do sistema é prover uma camada de segurança a nível de aplicação para mensagens SMS em redes de telefonia móvel. O software é capaz de assinar, cifrar, decifrar e verificar mensagens enviadas por SMS, de forma a garantir a identidade do remetente, e garantir que ela somente poderá ser lida pelo destinatário real, oferencendo assim os serviços de segurança: autenticidade, confidencialidade e integridade.

Apesar de implementado especificamente para ser executado em um telefone celular, garantindo a comunicação pessoal sigilosa, o mesmo esquema pode ser facilmente portado para outras plataformas que têm acesso à comunicação por SMS, como PDAs ou servidores. Desta forma, o esquema pode ser aplicado em áreas que requerem alto nível de segurança da informação que trafega nas redes de telefonia móvel, por exemplo aplicações militares, bancárias, e de comércio eletrônico.

### 1.1. Cenário

O ambiente em questão não se mostra muito propício para práticas criptográficas. A largura de banda é muito pequena, visto que em cada mensagem SMS podem ser trafegados apenas 140 bytes binários. Além disto, existem limitações de processamento no

*Orientador do trabalho. Bolsista de Produtividade em Pesquisa CNPq, processo 312005/2006-7.

dispositivo celular, que podem comprometer a usabilidade de um esquema criptográfico tradicional.

Talvez devido a estas dificuldades, o cenário atual não apresenta uma grande variedade de soluções abrangindo objetivos similares aos de nosso sistema, e não há uma solução universalmente adotada.

## 2. Objetivos

O objetivo do trabalho é quebrar o paradigma atual, desafiar as dificuldades existentes, e produzir um sistema que garante segurança no intercâmbio de mensagens SMS entre dispositivos celulares sem afetar a usabilidade do serviço. Além disto, o nível de segurança obtido deve ser equiparável ao nível de segurança de aplicações de segurança vigentes atualmente, como por exemplo uma transação bancária pela Internet pelo protocolo HTTPS.

### 2.1. Escopo

O que nosso sistema garante é....

Problemas como... etc etc etc... não são de nossa responsabilidade... etc etc etc...

### 2.2. Metodologia

### 2.3. Métricas

A seguir, definimos as métricas desejadas.

- Tempo de espera: Consiste nos tempos para cifrassinar e vericifrar uma mensagem. Baseando-se em aplicações já existentes e satisfazendo os requisitos de usabilidade de nosso projeto, estimamos que um intervalo de espera para processamento de uma mensagem de no máximo 5 segundos seja tolerável pelo usuário.
- Tamanho máximo da mensagem: Consiste da soma dos bytes úteis da mensagem com os bytes de controle do algoritmo. Implementações SMS baseadas em *Sun Wireless Messaging API (WMA)* podem dividir uma única mensagem em, no máximo, 3 segmentos. Recomenda-se que as aplicações SMS utilizem mensagens com menos de 399 bytes binários de modo a não comprometer sua portabilidade [Ortiz 2002]. Desse modo, estabelecemos um tamanho máximo de 399 bytes para as mensagens transmitidas, sendo este espaço compartilhado entre os dados de controle do algoritmo criptográfico utilizado e a mensagem criptografada em si.
- Tamanho das chaves privada/pública e da assinatura: Devido às limitações de espaço de armazenamento das mensagens, estabeleceu-se que a assinatura de uma mensagem, bem como a chave privada do usuário, não deveriam exceder 200 bits. No entanto, essa restrição não deveria comprometer os requisitos de segurança do sistema.

Sabendo que um certificado digital típico ocupa entre 2KB e 4KB, nota-se aqui que uma solução baseada em infra-estrutura convencional de chaves públicas inviabilizaria completamente o sistema: antes de se enviar uma mensagem SMS segura para algum usuário, seria necessário receber o certificado desse usuário particionado em 15 a 30 mensagens SMS, além de enviar em resposta outro certificado em mais 15 a 30 mensagens SMS. Esse esforço precisaria ser efetuado novamente para cada novo destinatário

a quem determinado usuário desejasse enviar mensagens, ou em cada caso de renovação ou revogação de certificado. Some-se a isto o espaço ocupado por uma única assinatura convencional, tipicamente de 128 bytes por estar baseada no algoritmo RSA com 1024 bits; este *overhead* seria duplicado com o requisito de cifrar e assinar a mensagem, isto é, tomaria 256 bytes do espaço disponível.

Por outro lado, a manutenção de um diretório confiável de chaves públicas, típico de sistemas de criptografia convencionais, seria impraticável em uma rede de telefonia celular. Uma solução tecnológica baseada em alternativas à criptografia convencional é, portanto, imprescindível.

Sendo assim, foi considerado o uso de criptografia com assinatura baseada em identidades, de acordo com o conceito proposto inicialmente por Shamir [Shamir 1984]. Aprofundando-se na especificação, percebeu-se ainda que a chave pública do usuário poderia ser estabelecida essencialmente a partir de sua identificação única no sistema, ou seja, seu próprio número de celular. Desse modo, a criptografia baseada em identidades com emparelhamentos bilineares parecia atender aos requisitos do nosso aplicativo e foi inicialmente adotada na solução do projeto.

## 3. Discussão

### 3.1. Preliminares teóricas

### 3.2. Alternativas existentes

### 3.3. Revisão literatura

## 4. MIOLO

## 5. Modelos

## 6. Resultados

## 7. Conclusão

### 7.1. Analisar resultados

### 7.2. Possíveis desenvolvimentos futuros

## 8. Referências

## Referências


Enck, W., Traynor, P., McDaniel, P., and Porta, T. L. (2005). Exploiting open functionality in sms-capable cellular networks. In *Proceedings of the 12th ACM conference on Computer and communications security*, pages 393–404, New York, NY, USA. ACM Press.

Ng, Y. L. (2006). Short message service (sms) security solution for mobile devices.

Ortiz, C. (2002). The wireless messaging api. Sun Developer Network (SDN) article. `http://developers.sun.com/mobility/midp/articles/wma/index.html`.

Shamir, A. (1984). Identity based cryptosystems and signature schemes. In *Advances in Cryptology – Crypto'84*, volume 0196 of *Lecture Notes in Computer Science*, pages 47–53. Springer.