Projeto de Formatura – Turmas 2008

PCS - Departamento de Engenharia de Computação e Sistemas Digitais

Engenharia de Computação

Tema:

Sistema de SMS Seguro

SMS Seguro foi projetado para fornecer serviços de segurança nas transações via SMS. O sistema permite que usuários comuns, bancos e operadoras de celular trafeguem suas mensagens de modo a garantir autenticidade, integridade e confidencialidade.

Tecnologia

A adoção da Criptografia Baseada em Curvas Elípticas possibilitou o desenvolvimento de uma solução com chaves de tamanho reduzido e isenta de certificados, garantido velocidade e economia de banda nas transações em dispositivos móveis, ambiente de recursos tipicamente escassos.

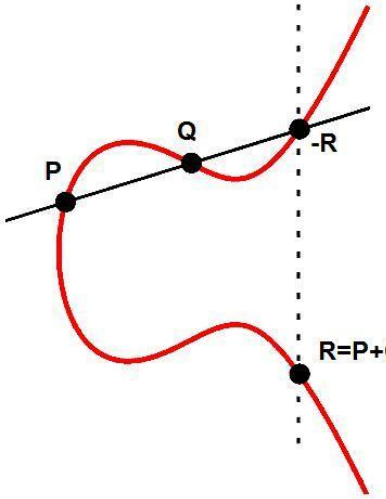

Fig 1. Soma de 2 pontos em uma curva elíptica.

Solução

No desenvolvimento do projeto foi gerado um novo protocolo de segurança denominado BDCPS, cujas letras referenciam os autores. Trata-se de nova técnica criptográfica mais eficiente e econômica que mescla o uso de criptografia baseada em identidades com técnicas convencionais. O sistema é implementado usando a linguagem de programação Java e executa em qualquer aparelho celular que possua ambiente Java ME.

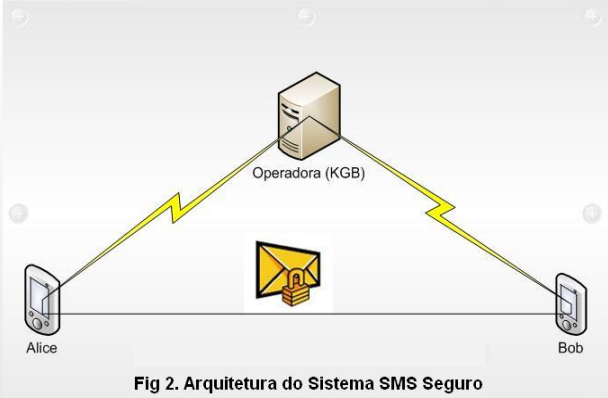

Fig 2. Arquitetura do Sistema SMS Seguro

Arquitetura

A arquitetura básica se constitui de: A) Uma autoridade de confiança denominada Key Generation Bureau que é responsável apenas por gerar uma parte da chave privada de um novo usuário que deseja usar o sistema. B) 2 ou mais dispositivos móveis que desejam se comunicar de forma segura. Na primeira conversa entre os usuários, Alice e Bob, ambos se autenticam sem a necessidade de consultar certificados e, a partir de então, podem conversar normalmente.

Integrantes: Eduardo de Souza Cruz <eduardo.cruz@poli.usp.br>
Geovandro Carlos C. F. Pereira <geovandro.pereira@poli.usp.br>
Rodrigo Rodrigues da Silva <rodrigo.silva1@poli.usp.br>

Professor Orientador: Paulo S. L. M. Barreto <pbarreto@larc.usp.br>