PCS2040 – Projeto de Formatura I

Aplicativo Seguro de SMS

Evolução da Especificação

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

Agenda

- Objetivo
- Requisitos Funcionais
- Requisitos Não Funcionais
- Estudo de viabilidade
- Próximos passos
- Referências

Objetivo

- **Implementar uma arquitetura que permita o envio de mensagens SMS de forma segura**
- Solução completa: criptografia nas mensagens, assinatura digital, geração e substituição de chaves
- Modelo de negócio: solução adaptável ao ambiente do cliente, seja ele final ou intermediário

Requisitos Funcionais

- Envio de mensagem encriptada de A para B
  - A encripta a mensagem com chave pública de B
  - B decripta a mensagem com sua chave privada
- Envio de mensagem assinada de A para B
  - A assina a mensagem com sua chave privada
  - B verifica a validade da mensagem com a chave pública de A

Requisitos Funcionais

- Assinatura digital de mensagens através do algoritmo BLS (Boneh, Lynn and Shacham).
- Operações realizadas sobre curvas elípticas
- Assinatura: hash e exponenciação modular
- Verificação: cálculo de uma função bilinear

Curvas Elípticas

- As operações são realizadas sobre curvas elípticas devidamente escolhidas.
- Uma curva elíptica em um espaço Fp, onde p é um número primo, obedece a uma equação do seguinte tipo:

$$Y^2 \bmod p = X^3 + aX + b \bmod p$$

Hash

- H(m) é o *hash* da mensagem m sobre uma curva elíptica E e Q é um ponto sobre tal curva.
- Par de chaves (s, V=s.Q), onde s é privada e V é pública
  - s.Q não é uma ”multiplicação” normal!

Assinatura

- A assinatura é feita calculando-se o Hash da mensagem m e multiplicando o resultado pela chave privada:

$$\sum \leftarrow s \cdot H(m)$$

Verificação

- Calcula-se:

$$e\left(H(m), V\right) \qquad e\left(\sum, Q\right)$$

- Aceita-se se os dois cálculos apresentarem o mesmo resultado
- Por quê?

Verificação

$$e\left(\sum, Q\right) = e\left(s \cdot H(m), V\right) = e\left(H(m), s \cdot Q\right) = e\left(H(m), V\right)$$

- obs: e(P,Q) é uma função bilinear

Requisitos Não-Funcionais

- Tempo de resposta – o tempo para assinar e cifrar ou decifrar e verificar uma mensagem menor que 5s;
- Tamanho da aplicação – limite de 200 kbytes; e
- Compatibilidade – o aplicativo deve ser compatível com qualquer celular que possua uma máquina virtual Java CLDC (Common Limited Device Configuration).

Estudo de viabilidade

- Além do estudo sobre os algoritmos que serão utilizados, foram feitos testes de benchmark em processadores de celulares para verificar a viabilidade do projeto.
- Benchmark: 100 operações de potenciação em números inteiros de 160 bits foram executadas em 5958ms em um celular Samsung SGH-E570 – 60 ms por operação.

Próximos Passos/Em andamento

- Estudo de algoritmos de cifrassinatura.
- Testes de viabilidade em outros celulares.
- Confecção de protótipo funcional básico
- Compltar especificação.
- Adequação da especificação à norma IEEE-830.

Referências

- Rivest, R.; Selected Topics in Cryptography, Lecture 26, 2004.
- Barreto, P. S. L. M.; Cifrassinatura BLMQ baseada em identidades.
- ECC CryptographyTutorial. http://www.certicom.com/index.php?action=ecc_tutorial,home. Acesso em 22 mar. 2008.

Dúvidas Senhores?