Palestra 02/06 - Criptografia

Sabrina Araújo da Silva - nºUSP 12566182

Objetivo 1

Esconder informações de terceiros.

Exemplos:

- Calcular senha de conta corrente
- "Pescar" senha de cartão de crédito

Objetivo 2

"Assinar" criptograficamente documento digital com chave particular vinculada à chave pública.

Criptografia

- Técnicas de proteção de informação sigilosa
- Autenticação do remetente e destinatário de documentos eletrônicos: assinatura digital/criptográfica
- Proteção de integridade de banco de dados

CA - Certificate Authority ("cartório")

1. Cadastramento
2. Chave pública P
3. Chave pública P assinada pela CA, e a chave da CA para verificação da assinatura

Como saber se aquela chave pública é de fato do legítimo dono?

-> A chave deve ser assinada por uma autoridade idônea

Criptografia de chave pública

Sistema criptográfico que usa chaves públicas que podem ser amplamente disseminadas e chaves privadas que são conhecidas apenas pelo proprietário.

RSA (Rivest-Shamir-Adleman)

A chave de encriptação é pública e é diferente da chave de decriptação que é privada. Foi o primeiro algoritmo a possibilitar criptografia e assinatura digital.

AES (advanced encryption standard)

AES é um algoritmo de chave simétrica, o que significa que a mesma chave é usada para criptografar e descriptografar os dados.