MAC499 - Trabalho de Formatura Supervisionado
César Seragiotto
orientador: Routo Terada

Criptografia Baseada Em Identidade

Em 1985, Adi Shamir sugeriu um esquema similar ao sistema postal, em que a chave de um usuário fosse função de sua identidade, evitando assim a necessidade de um diretório de chaves públicas, trocas de chaves ou uma autoridade superior que esteja sempre presente.

Criptografia utilizando resíduos quadráticos

O sistema possui uma autoridade que gera e divulga os parâmetros universais.

Assim, se um usuário deseja se registrar para ser capaz de receber dados codificados, ele envia sua identidade (p.ex. endereço de e-mail) para a autoridade, que lhe devolve uma chave privada.

Quando um outro usuário deseja enviar informação criptografada para outro, ele faz isso conhecendo a chave pública do destinatário e os parâmetros globais. Não há necessidade de nenhum diretório de chaves públicas.

O esquema de assinatura de Shamir

Uma autoridade confiável produz os parâmetros globais do sistema e uma chave mestra.

Um usuário, após apresentar sua identidade tem sua chave gerada. Esta chave é usada para assinar as mensagens enviadas. A autoridade não é mais necessária a partir daqui.

Na criptografia de chaves públicas no sentido habitual, para um usuário verificar a assinatura de outro usando sua chave pública deve-se verificar também a autenticidade desta. Torna-se inevitável a presença da autoridade certificadora.

É interessante perceber que neste esquema não há necessidade de se realizar uma apuração separada. A verificação da assinatura confirma (ou nega) duas coisas ao mesmo tempo:

- A assinatura foi criada pelo outro usuário usando sua chave privada, que está por trás de sua identidade;
- essa identidade foi certificada pela autoridade.