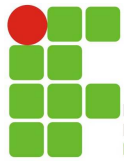
Segurança de Redes

Curso Superior de Tecnologia em Redes de Computadores
Prof. Macêdo Firmino

Aula 08
Assinatura e Certificado Digital

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

"Esse é o singelo segredo da felicidade. Faça o que fizer, não deixe que o passado interfira, não deixe que o futuro incomode. Porque o passado já não existe, e o futuro ainda não chegou." (Osho)



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

O que Aprenderemos?

- Entender o que é uma assinatura digital.
- Compreender quais as propriedades que a assinatura garante.
- Aprender como funciona o processo de assinatura digital.
- Entender como as chaves públicas são distribuidas.
- Compreender a finalidade das autoridade de certificação e do cetificado digital.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Assinatura Digital

Para garantir a integridade e autenticidade das mensagens foi mostrado o método MAC (Código de Autenticação de Mensagens) que trata da função hash com chave simétrica. Entretanto, com a utilização de chaves simétricas surge o problema de distribuição das chaves. Visando solucionar esta problemática temo o conceito de assinatura digital.

A assinatura digital é método usado para garantir a autenticação, irretratabilidade (ou não-repúdio) e integridade dos dados, utilizando algoritmos de criptografia de chave pública com função Hash. Como a chave pública pode ser divulgada livremente, este método não apresenta o problema de distribuição de chave presente no método MAC.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

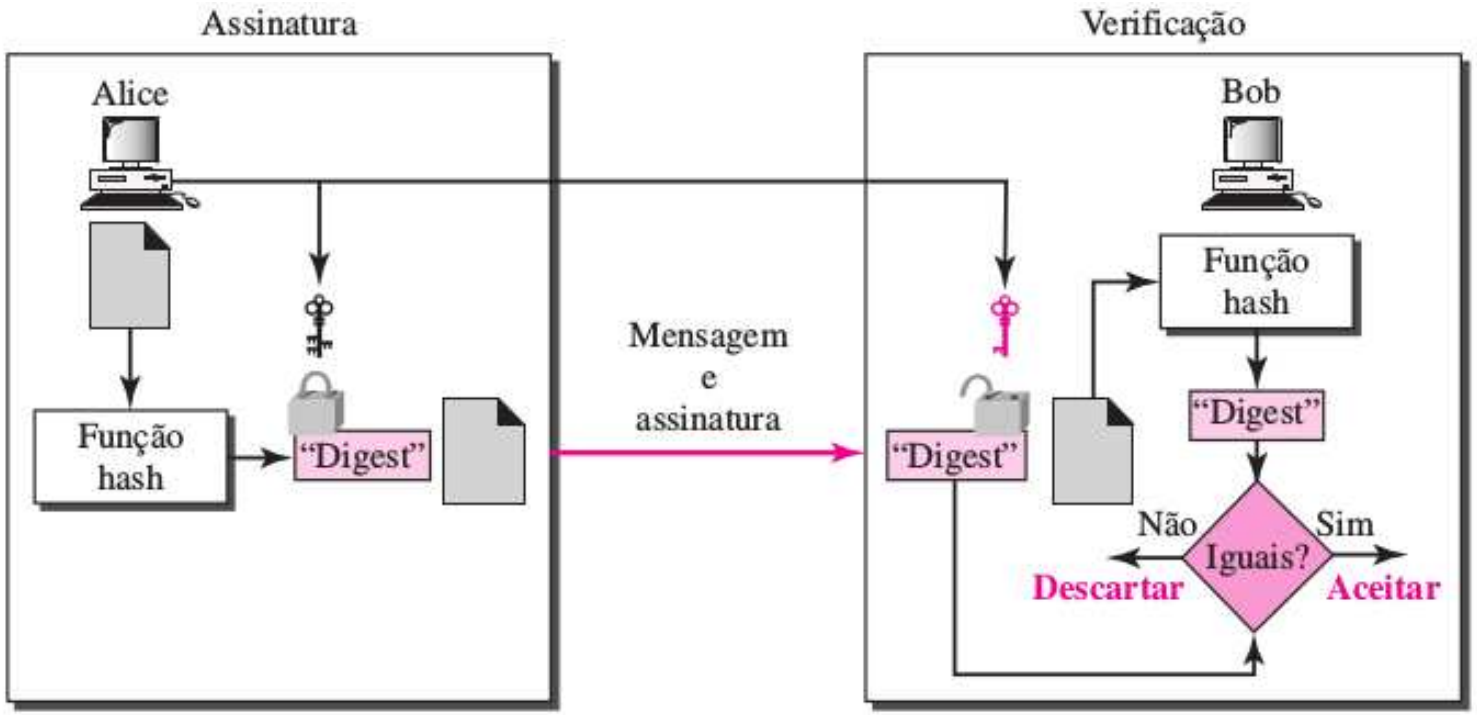
Assinatura Digital

Um sistema de assinatura digital não oferece comunicação confidencial. Se for necessária confidencialidade, a mensagem e a assinatura devem ser criptografadas por meio de um criptossistema de chave pública ou simétrica.

Cada assinatura é única para os dados assinados e para as chaves utilizadas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Assinatura Digital – Funcionamento



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Assinatura Digital – Funcionamento

O transmissor escreve mensagem, calcula hash da mensagem, assina o hash com sua chave privada (assinatura digital), envia a assinatura e a mensagem original para o receptor. O Receptor separa a assinatura da mensagem original, utiliza chave pública do transmissor para verificar a assinatura e calcula o hash local da mensagem recebida. O resultado da verificação da assinatura corresponde ao hash da memsagem calculado pelo emissor. Caso os dois hashes sejam iguais, a mensagem foi enviada por alguma pessoa proprietária da chave privada, e não foi modificada na transmissão.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Assinatura Digital x Criptografia Assimétrica

Devemos fazer uma distinção entre chaves públicas e privadas usadas em assinatura digital e chaves públicas e privadas usadas para fins de criptografia (confidencialidade). Em um criptossistema, utilizamos as chaves públicas e privadas do receptor; na assinatura digital, usamos a chave pública e privada do emissor. Em outras palavras, o emissor usa a chave pública do receptor para criptografar; o receptor utiliza sua própria chave privada para decriptografar. Na assinatura digital, o emissor utiliza sua chave privada; o receptor usa a chave pública do emissor.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Assinatura Digital – Algoritmos

Na assinatura digital poderá ser utilizado qualquer dos algoritmos de hash. Entretanto, os mais utilziados são os algoritmos da família SHA-1 e SHA-2. Poderá ser utilizado quaisquer dois algoritmos de chave públicas apresentados no criptografia. Entretanto, o algoritmo mais utilizado é o RSA, Curva Elíptica e Elgamal e o DSS (*Digital Signature Standard*).

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

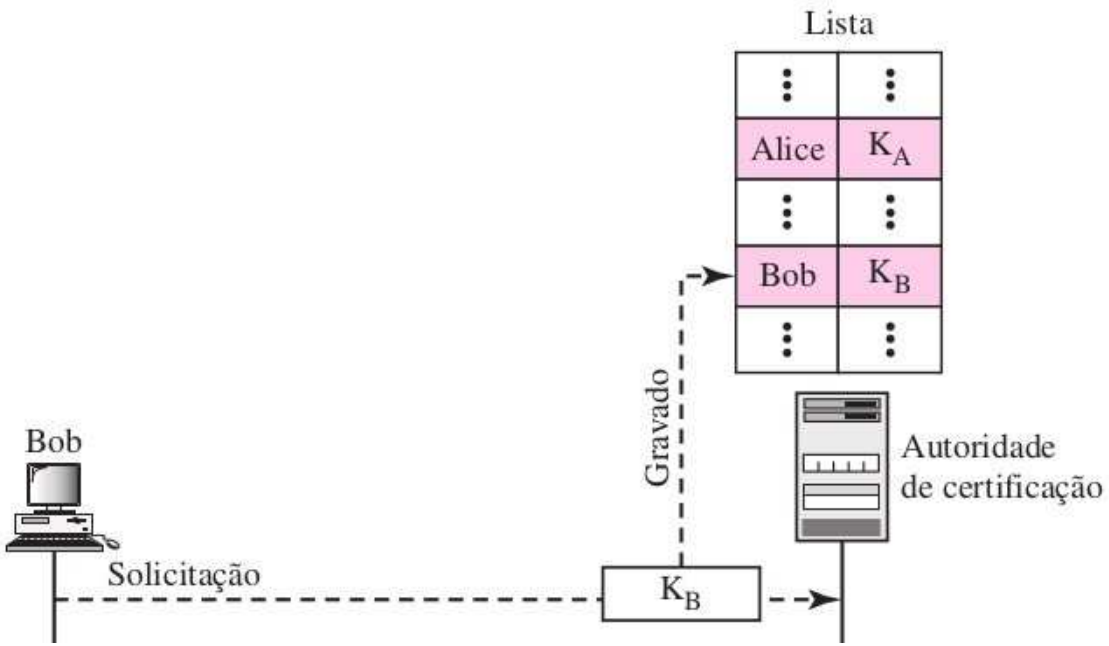
Distribuição de Chaves Públicas

Como obter uma chave pública? E como saber se a chave pública é realmente de uma determinada entidade? As chaves públicas podem ser distribuídas através de Autoridade de Certificação. Estas autoridades retem uma lista de chaves públicas. Cada usuário pode escolher uma chave pública/privada, manter a privada e entregar a pública para inserção na lista. A autoridade de certificação requer que cada usuário se registre e prove sua identidade.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Distribuição de Chaves Públicas

Uma CA (Autoridade de Certificação) é uma organizações nacionais ou internacionais que vinculam uma chave pública a uma entidade e emite um certificado, análogas aos cartórios que verificam assinaturas normais.



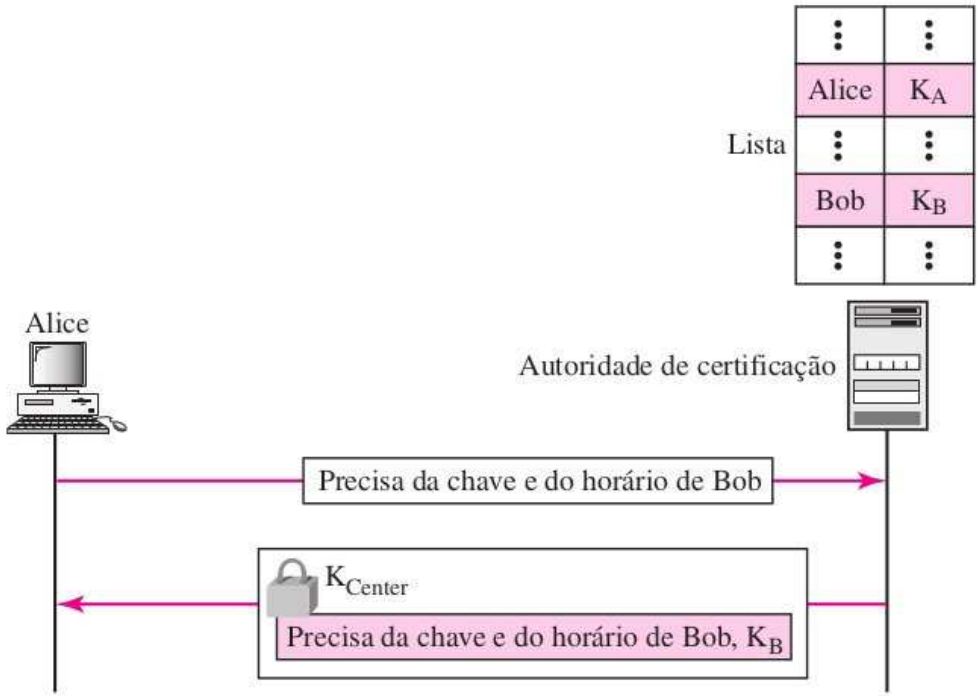
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Distribuição de Chaves Públicas

A CA verifica a identificação de uma entidade (usando documentação comprobatória, tais como , cpf, cnpj, documentos com imagem e biométria). Então, pode solicitar a chave pública da entidade e gravá-la no certificado. Para impedir que o próprio certificado seja falsificado, a CA assina o certificado com sua chave privada. Agora, qualquer um pode baixar o certificado assinado e usar a chave pública da autoridade de certificação para extrair a chave pública de Bob.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Se Alice precisar conhecer a chave pública de Bob, ela poderá enviar uma solicitação para a autoridade de certificação, inclusive o nome de Bob e um registro de horas. A autoridade de certificação responde com a chave pública de Bob, a solicitação original e o registro de horas assinado com a chave privada do centro. Alice usa a chave pública da autoridade de certificação, conhecida por todos, para decriptografar a mensagem e extrair a chave pública de Bob.



INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Entidade Certificadora

A CA mais importante do Brasil é a AC-Raiz Brasileira. Ela existe desde 2001, após a criação da Infraestrutura de Chaves Públicas Brasileira (ICP Brasil). A AC-Raiz é quem autoriza que outras ACs funcionem, descentralizando a emissão de certificados. São exemplos de ACs brasileiras: Serpro, Caixa Econômica Federal, Receita Federal, Certisign, Casa da Moeda, Ministério das Relações Exteriores.

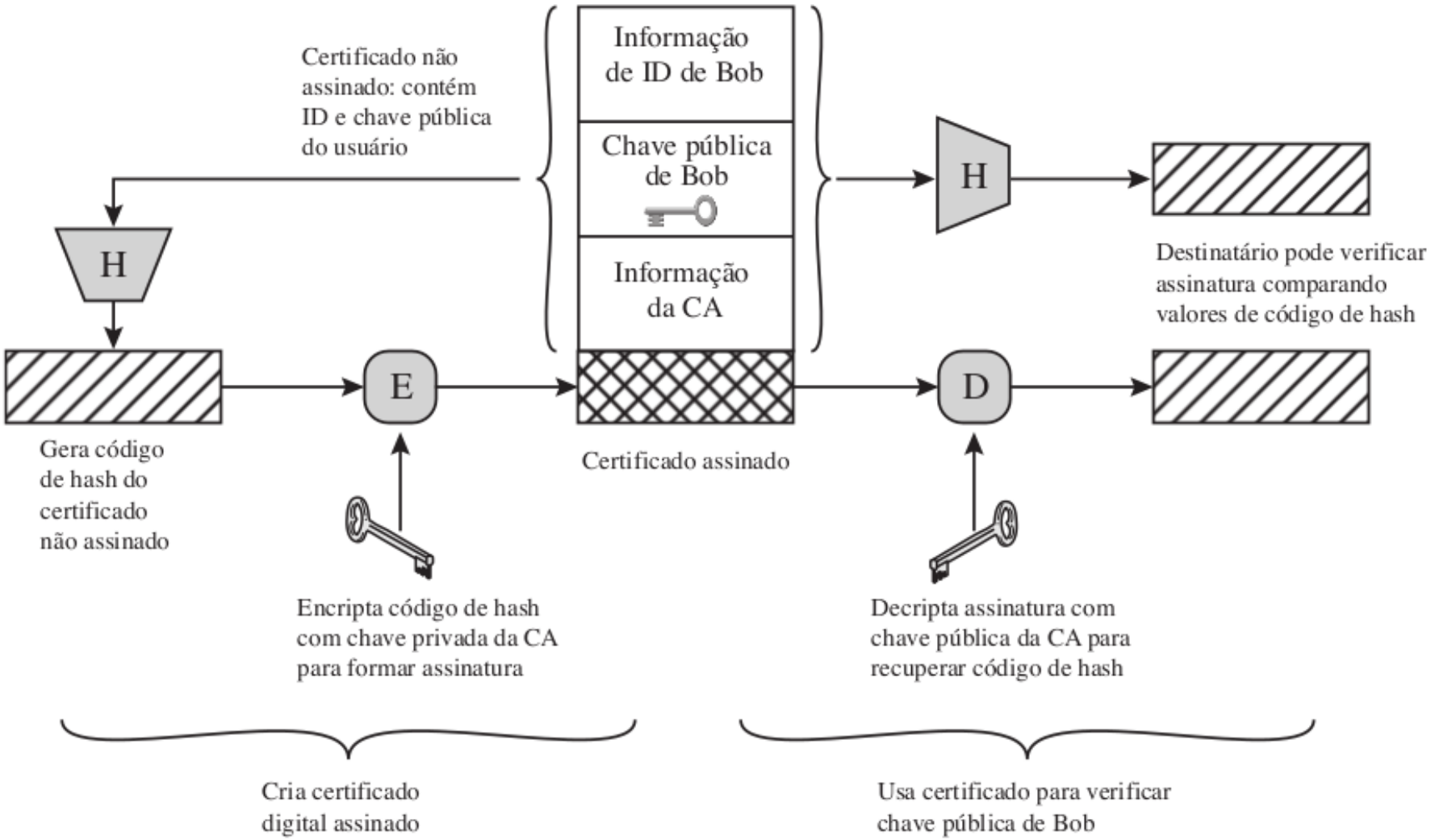
INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Certificado Digital

O ITU desenvolveu um padrão internacional para certificados denominado X.509. Nele define os campos de um certificado, os principais são:

- Version: define a versão do X.509 do certificado. O número da versão iniciou em 0; a atual é versão 2;
- Serial number: um número atribuído a cada certificado;
- Signature: identifica o algoritmo e parâmetros usado para assinar o certificado;
- Issuer: identifica a autoridade de certificação;
- Period of validity: define o primeiro e o último momento em que o certificado é válido;
- Subject: define a entidade a qual a chave pública pertence;
- Subject's public key: define a chave pública do sujeito.

Certificado Digital



EDUCAÇAO, CIENCIA E TECNOLOGIA
RIO GRANDE DO NORTE

Certificado Digital

Quando você tenta acessar um site utilizando conexão segura, normalmente seu navegador já realiza verificações. Caso as verificações falhem, o navegador emite alertas.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Certificado Digital

- Em geral, alertas são emitidos em situações como:
  - O certificado está fora do prazo de validade;
  - O navegador não identificou a cadeia de certificação ;
  - O endereço do site não confere com o descrito no certificado;
  - O certificado foi revogado.

INSTITUTO FEDERAL DE EDUCAÇÃO, CIÊNCIA E TECNOLOGIA RIO GRANDE DO NORTE

Dúvidas

INSTITUTO FEDERAL DE
EDUCAÇÃO, CIÊNCIA E TECNOLOGIA
RIO GRANDE DO NORTE