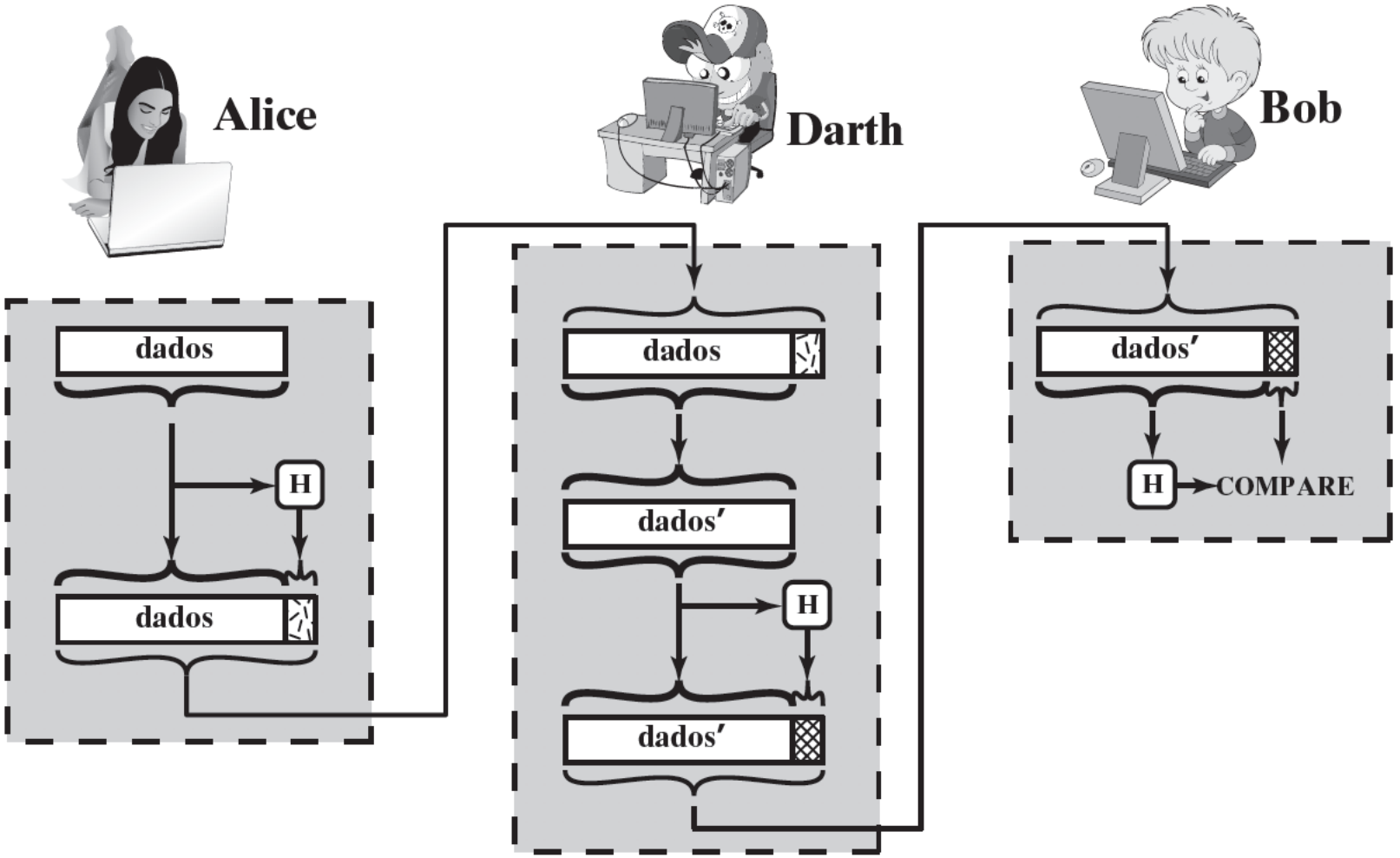
Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

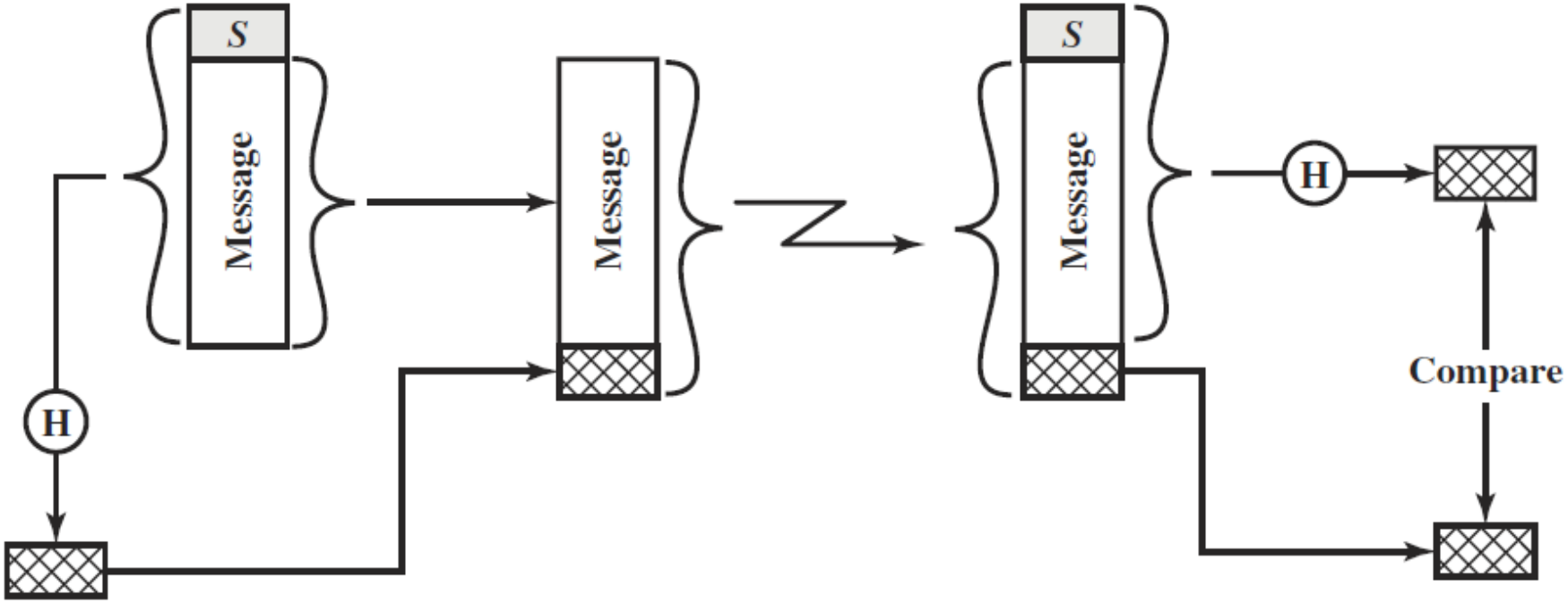
Aula anterior

Segurança da Informação– GBC083

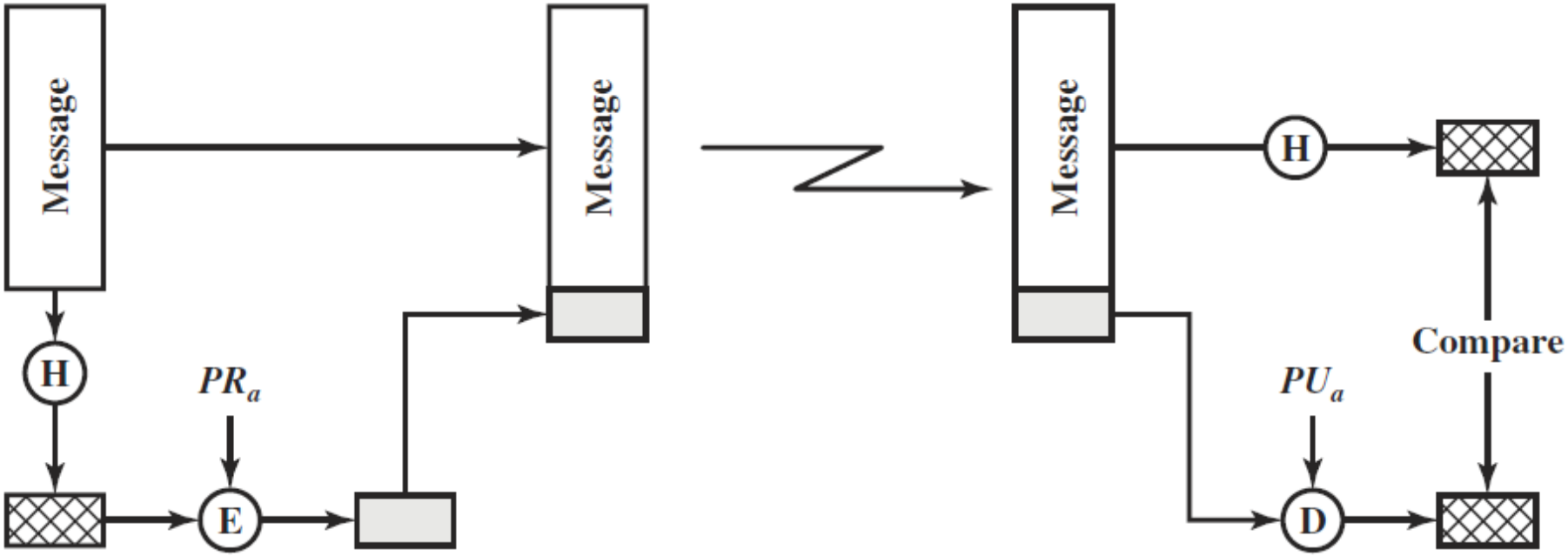
Integridade de mensagens – Problemas…



Autenticação usando a função hash - 2



Assinatura digital – Funcionamento básico



Divulgação de chaves públicas

- A natureza das chave públicas faz com que seja importante divulgá-las amplamente.

- Indivíduos podem anunciar suas chaves livremente:
  - **Problema**: como garantir que aquela chave pública realmente pertence a uma determinada entidade?
  - Veremos na próxima aula – certificados e infraestrutura de chaves pública (ICP).

Infraestrutura de chaves públicas

Segurança da Informação– GBC083

Principais questões associadas ao Tópico 13

1. O que é um certificado digital?
   - Qual a relação entre assinatura digital e certificado digital?
2. Quem irá gerenciar os certificados? Quem são as autoridades certificadoras e de registro (AC e AR)?
3. Qual é o processo para verificação de um certificado digital?

Certificados digitais – Pergunta 1

- Assinatura digital procurar resolver o problema em situações onde somente a autenticação não é suficiente;
  - Não existe confiança mútua entre emissor e receptor.

- As seguintes características são desejáveis:
  1. Verificar o **autor** da assinatura;
  2. **Autenticar** o conteúdo no momento da assinatura;
  3. Ser verificável por **terceiros**, para resolver disputas.

Certificados digitais – Pergunta 1

- A natureza das chave públicas faz com que seja importante divulgá-las amplamente.

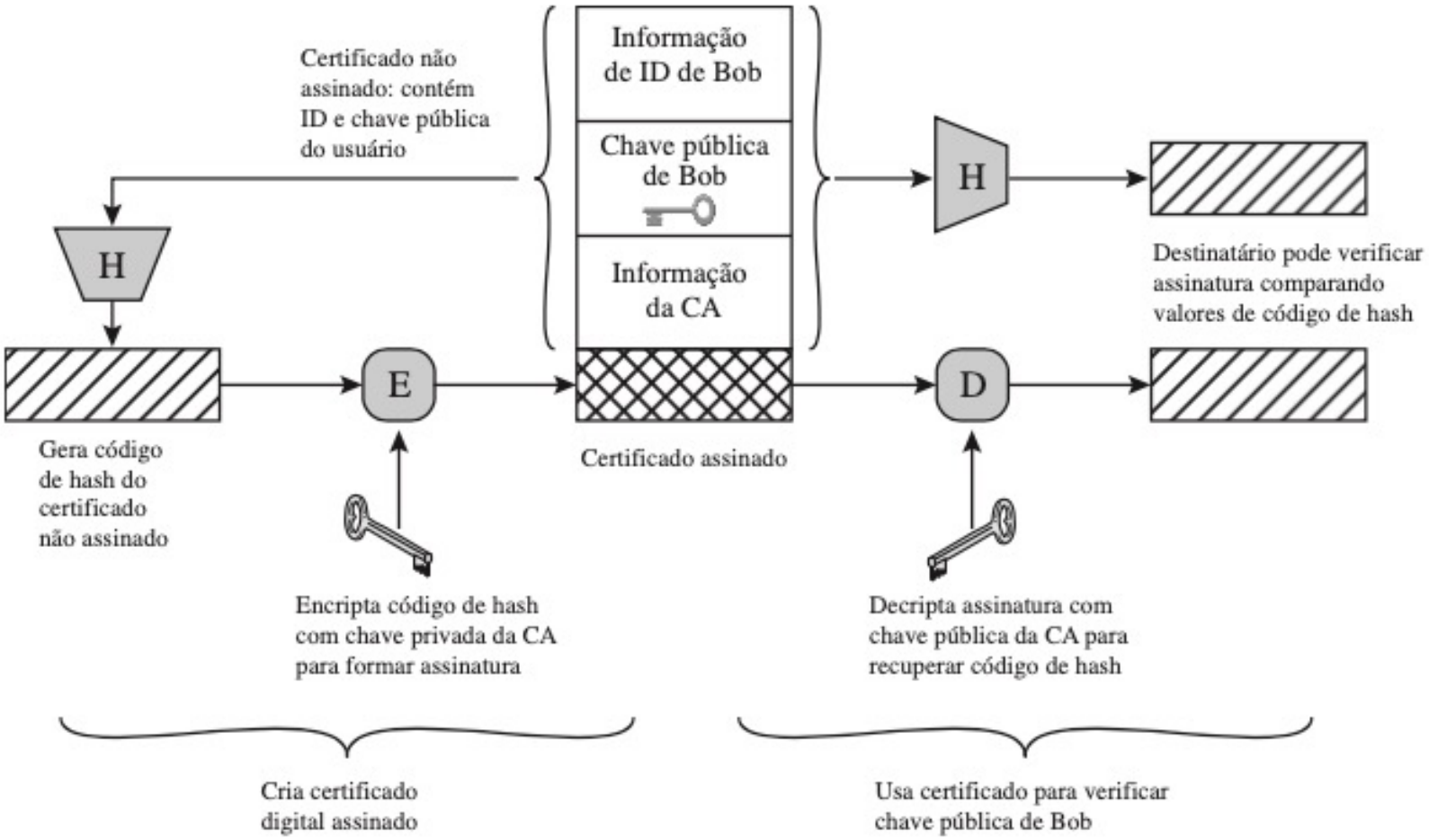
- Indivíduos podem anunciar suas chaves livremente:
  - **Problema**: como garantir que aquela chave pública realmente pertence a uma determinada entidade?

Certificados digitais – Pergunta 1

- Certificados digitais utilizam a criptografia de chave pública (criptografia assimétrica).

- Definição rápida de certificado digital:
  - Chave pública de um usuário ou sistema que é assinada digitalmente por uma autoridade certificadora (AC) usando a chave privada dela.

Certificados digitais – Pergunta 1



Certificados digitais – Pergunta 1

- Usando a ideia de certificados digitais junto de terceiros confiáveis (Autoridades Certificadoras), é possível verificar se uma determinada chave pública realmente pertence aquela pessoa/sistema;

- Vamos ver um exemplo – acessar o site da Amazon pela primeira vez.

Quem irá gerenciar os certificados – Pergunta 2

- As Autoridades Certificadoras (AC) têm a função de criar, manter e controlar todos os certificados que elas emitem;

- Elas devem, inclusive, invalidar certificados expirados ou comprometidos;

- O gerenciamento de certificados digitais e o papel de uma AC são assuntos complexos e delicados.
  - Ambos são analisados dentro do assunto conhecido como Infraestrutura de chaves pública – PKI.

Quem irá gerenciar os certificados – Pergunta 2

- PKI: Public Key Infrastructure;

- É uma união de pessoas, organizações, hardware, software, políticas e procedimentos para prover a infraestrutura necessária ao uso adequado de certificados digitais baseados em chaves públicas;
  - Exemplo: ICP-Brasil - https://www.iti.gov.br/icp-brasil

- Uma PKI oferece confiabilidade nas transações que utilizam certificado digital.

Quem irá gerenciar os certificados – Pergunta 2

- ICP-Brasil é uma cadeia hierárquica de confiança que viabiliza a emissão de certificados digitais para identificação virtual do cidadão;

- O modelo adotado pelo Brasil foi o de certificação com raiz única;
  - Desempenha o papel de Autoridade Certificadora Raiz – AC-Raiz;
  - Também tem o papel de credenciar e descredenciar os demais participantes da cadeia, supervisionar e fazer auditoria dos processos.

Quem irá gerenciar os certificados – Pergunta 2

Quem irá gerenciar os certificados – Pergunta 2

- Autoridades certificadoras são empresas. Elas cobram pela emissão e gerenciamento dos certificados. Um projeto bem interessante, *Let's Encrypt*, possui como objetivo fornecer certificados de graça para quem quiser. E aí? Tudo bem com isso? Algum problema?

Quem irá gerenciar os certificados – Pergunta 2

Qual o problema dos certificados grátis?

- Como é o processo de verificação? Quem assina? O que acontece se um agente malicioso gera um certificado desses e disponibiliza um site que não armazena corretamente os seus dados pessoais? Trecho do site: *"Our services are free and easy to use so that* ***every website*** *can deploy HTTPS."*

https://securityboulevard.com/2019/01/lets-encrypt-are-enabling-the-bad-guys-and-why-they-should/

Qual é o processo para verificação de um certificado digital? – Pergunta 3

Suponha que Alice e Bob irão se comunicar utilizando a infraestrutura de chaves públicas. Como seria o passo a passo, desde a criação das chaves/certificado até a verificação do mesmo?

Qual é o processo para verificação de um certificado digital? – Pergunta 3

1. Bob solicita a criação de um par de chaves para a AC;

2. AC verifica a identidade de Bob e, se tudo estiver correto, ela irá gerar um par de chaves (PU_{bob}, PRI_{bob});

3. A AC então irá assinar a chave pública de Bob que ela acabou de gerar fazendo o seguinte: gerar o hash de PU_{bob} - $H(PU_{bob})$ e cifrar esse hash com a sua chave privada (AC) resultando: $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

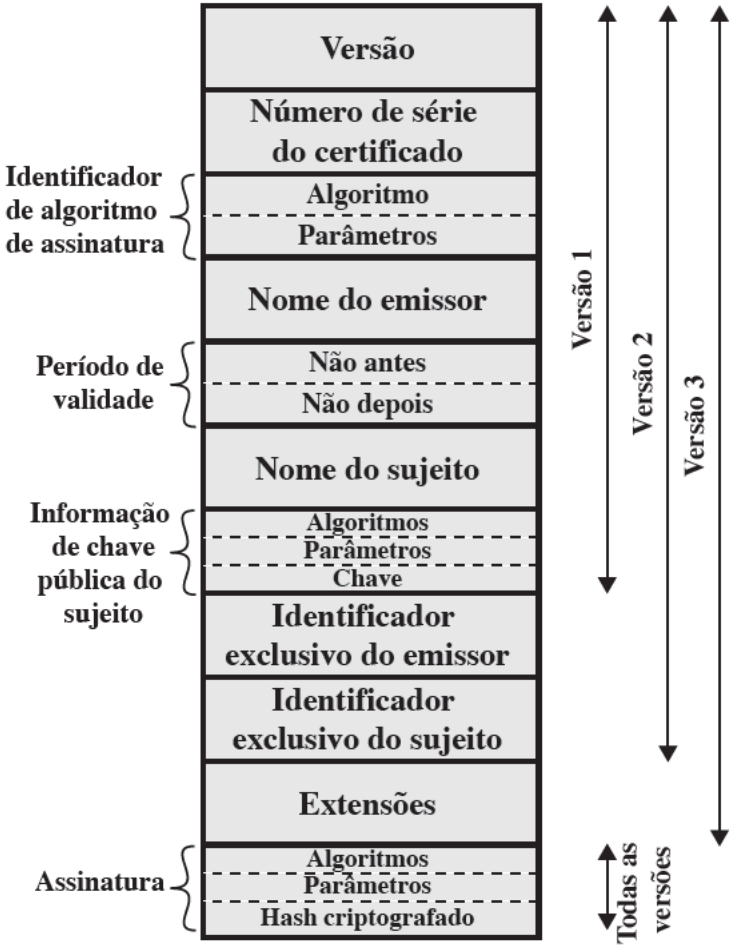
4. A AC envia para Bob o seu par de chaves (PU_{bob}, PRI_{bob}) e a assinatura de sua chave pública $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

Qual é o processo para verificação de um certificado digital? – Pergunta 3

5. Em seu navegador, Alice já possui a chave pública da AC - PU_{ac}. Quando Bob tentar conversar com a Alice pela primeira vez, ele irá enviar a sua chave pública PU_{bob} juntamente com o seu certificado $Cert_{bob} = E(PRI_{ac}, H(PU_{bob}))$;

6. Alice recebe PU_{bob} || $Cert_{bob}$. Primeiramente, ela irá calcular o hash de PU_{bob} -> $H(PU_{bob})$* e guardar o resultado. Depois irá usar a chave pública da AC que está instalada no seu navegador para decifrar $Cert_{bob}$ fazendo o seguinte: $D(Cert_{bob}, PU_{ac})$. O resultado dessa operação será $H(PU_{bob})$**. Se $H(PU_{bob})$* = $H(PU_{bob})$**, a chave foi conferida e Alice pode confiar que realmente veio de Bob, pelo intermédio de um terceiro que ambos confiam..

Qual é o processo para verificação de um certificado digital? – Pergunta 3



(a) Certificado X.509

Qual é o processo para verificação de um certificado digital? – Pergunta 3

Alice irá comprar na loja eletrônica de Bob. Suponha que Alice instalou em seu navegador o certificado da AC raiz. Considere que o certificado de Bob foi obtido com a AC intermediária e que a AC raiz assinou o certificado da AC intermediária.

Nesse cenário, o que deverá ser feito para que Alice verifique o certificado de Bob? Explique e mostre cada um dos passos.

Roteiro de estudos

1. Leitura das seções 14.4, 14.5 e 14.6. do livro "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudar os "slides completos";
3. Estudo da vídeo-aula referente ao tópico 13;
4. Abrir diferentes navegadores e procurar pelos certificados instalados neles – qual algoritmo foi usado para assinar? Qual o tamanho da chave? Quem é a AC?
5. Resolução dos TP-5.e TP-6.