Segurança da Informação– GBC083

Prof. Rodrigo Sanches Miani – FACOM/UFU

Integridade, autenticação e não-repúdio

Prof. Rodrigo Sanches Miani – FACOM/UFU

Tópicos da aula

1. Motivação
2. Verificação de integridade usando funções de hash
3. Autenticação usando funções de hash
   - MAC – Código de autenticação de mensagem
4. Não repúdio usando funções de hash

Motivação

Segurança da Informação– GBC083

Motivação

- Suponha que Alice e Bob estão usando o modelo híbrido de criptografia para trocar mensagens com confidencialidade;
- Alice e Bob não confiam inteiramente no canal e gostariam de verificar se as mensagens que receberam são realmente iguais as mensagens que foram enviadas;
- O que fazer?

Motivação

A ideia consiste em materializar os seguintes passos:

1. Alice escreve a mensagem M;
2. Alice cria um pequeno bloco de verificação y com base na mensagem M, por exemplo, y = H(M);
3. Alice envia T = M || y;
4. Bob recebe T e separa M e y;
5. Bob precisa verificar que a mensagem M recém chegada é a mesma que foi escrita por Alice;
6. Bob usa o mesmo método de Alice para calcular o bloco de verificação – y* = H(M);
7. Se y = y* Bob confia que a mensagem que chegou é a mesma escrita por Alice.

Motivação

Quem é a função H? Qual é o seu formato? Porque ela pode ser usada dessa forma?

Motivação

Quem é a função H? Qual é o seu formato? Porque ela pode ser usada dessa forma?

Vimos na aula anterior que funções de hash criptográficas preenchem tais requisitos... Veremos como hoje!

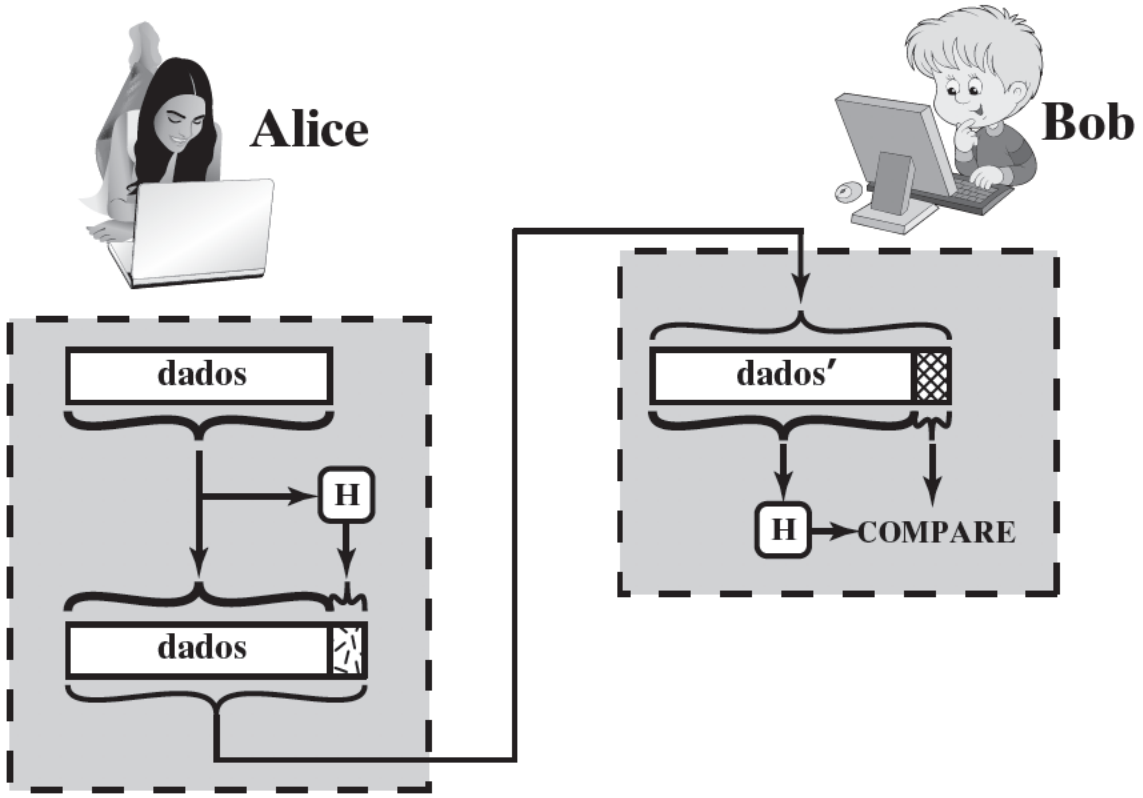
Verificação de integridade usando funções de hash

Segurança da Informação– GBC083

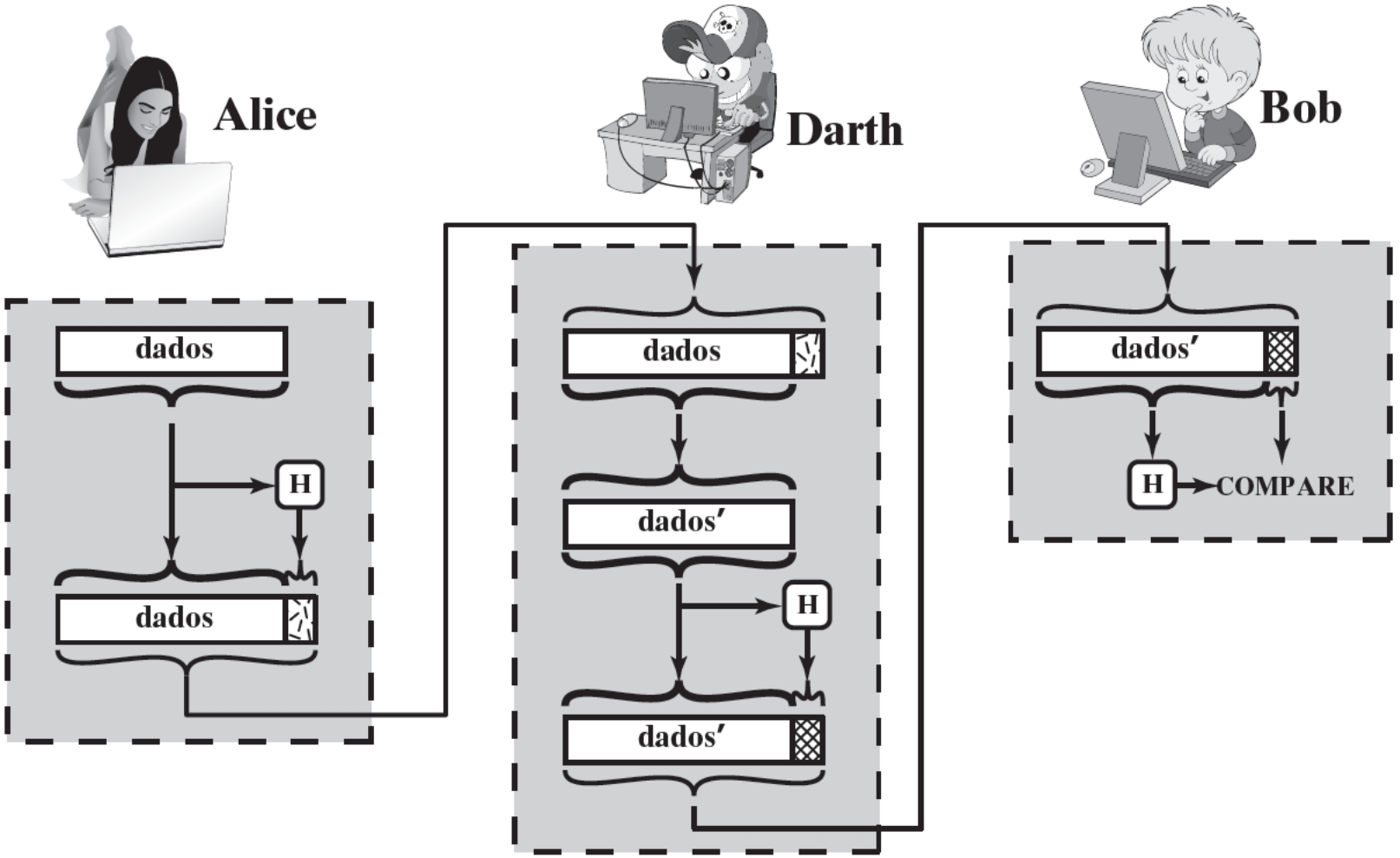
Integridade de mensagens

- Usando funções de Hash, como o destino pode garantir que a mensagem que acabou de chegar é íntegra?

Integridade de mensagens



Integridade de mensagens – Problemas…



Integridade de mensagens - Problemas

Como resolver o problema anterior?

Autenticação usando funções de hash

Segurança da Informação– GBC083

Autenticação de mensagens

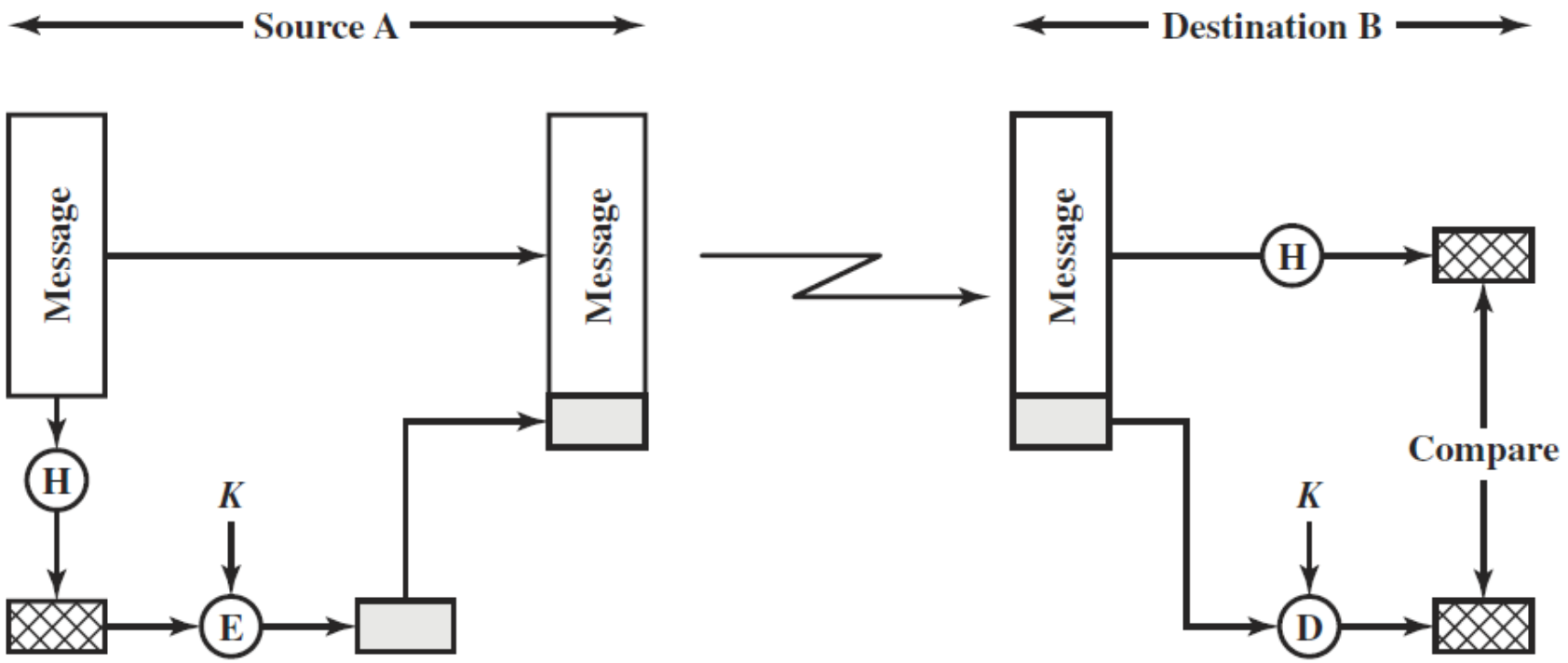
Definição (Stallings, 2008):

- É um mecanismo ou serviço usado para verificar a **integridade** de uma mensagem e que a **identidade** afirmada pelo emissor é válida.

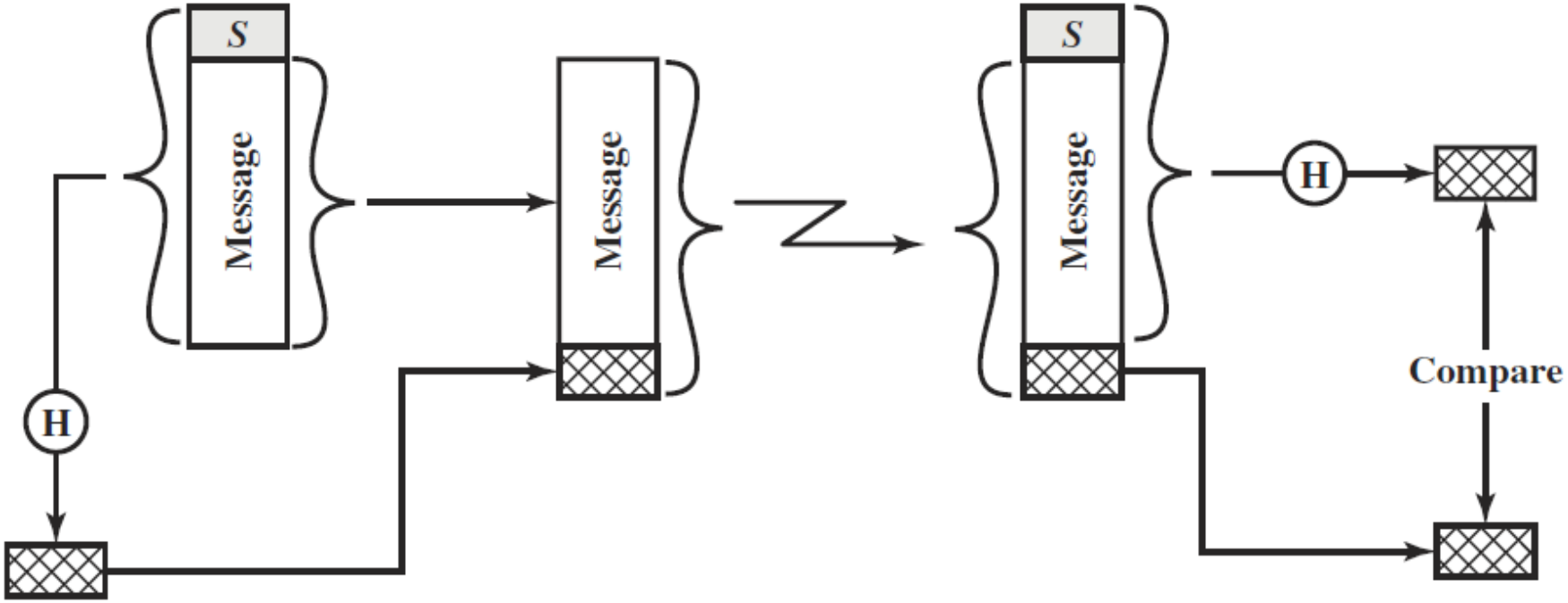
Autenticidade de mensagens

Usando funções de Hash, como o destino pode garantir que a mensagem que acabou de chegar é **autêntica**?

Autenticação usando função hash - 1



Autenticação usando a função hash - 2



Autenticação de mensagens

Porque os dois esquemas anteriores garantem a **autenticidade** das mensagens?

Garantia de autenticidade

- Um terceiro (Trudy) teria que ter acesso a chave secreta K para se passar pela Alice e criar o mesmo bloco de verificação;
  - Propriedades de função de hash criptográficas fortes dificultam o trabalho de Trudy... primeira imagem, segunda imagem e colisão;
  - Se o tamanho de K for suficientemente grande, é computacionalmente inviável para Trudy encontrar K.

Autenticação de mensagens - MAC

As técnicas de autenticação anteriores envolvem o uso de uma **chave secreta** para gerar um pequeno bloco de dados de tamanho fixo, conhecido como **soma de verificação criptográfica** ou MAC, que é anexada à mensagem;

Autenticação de mensagens - MAC

- Quando A tem uma mensagem para enviar a B, ele calcula o MAC como uma função da mensagem e da chave:
  - MAC = C(K,M), onde M é a mensagem, K é a chave, C é a função hash e MAC é o código gerado.

- Em nosso caso, quem poderia ser K e C?

Autenticação de mensagens - MAC

- Quando A tem uma mensagem para enviar a B, ele calcula o MAC como uma função da mensagem e da chave:
  - MAC = C(K,M), onde M é a mensagem, K é a chave, C é a função hash e MAC é o código gerado.

- Em nosso caso, quem poderia ser K e C?
  - K poderia ser a chave simétrica trocada pelos pares usando criptografia assimétrica;
  - C poderia ser a função de hash SHA-2;
  - Quando uma função de hash é usada para gerar um MAC ela é chamada de HMAC.

Não repúdio usando funções de hash

Segurança da Informação– GBC083

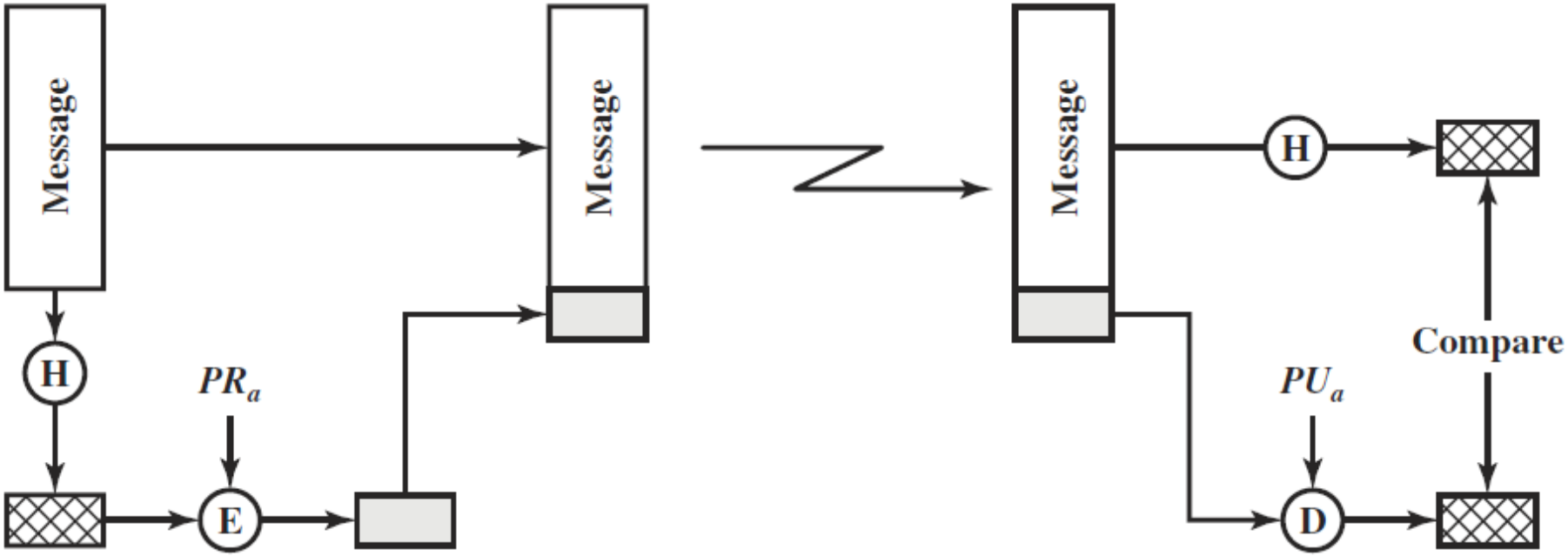
Assinatura digital – Motivações

- Suponha que Bob envie uma mensagem autenticada a Alice;

- Possíveis problemas:
  - Alice pode forjar uma mensagem diferente e alegar que veio de Bob;
  - Bob pode negar o envio da mensagem. Se Alice pode forjar a mensagem, não há como provar que Bob realmente a enviou.

- Em situações nas quais **não existe confiança mútua** entre emissor e destinatário, é necessário algo a mais que autenticação – não repúdio;

Assinatura digital – Funcionamento básico



Assinatura digital – Funcionamento básico

- Principal solução adotada envolve:
  - Uso de funções de hash;
  - Uso de criptografia assimétrica.

- Passos:
  - 1) O emissor aplica a função de hash na mensagem "M", o resultado será H(M);
  - 2) O emissor cifra o resultado do passo 1) usando a própria chave privada, o resultado será Kpr(H(M));
  - 3) O emissor envia a mensagem "M", concatenada com Kpr(H(M));
  - 4) O receptor recebe a mensagem e calcula o hash da mensagem "M", resultando H(M);
  - 5) O receptor decifra Kpr(H(M)) com a chave pública do emissor e compara o hash do passo 4);
  - 6) Se forem iguais, a mensagem está corretamente assinada pelo emissor.

Assinatura digital – Implicações

- É possível garantir autenticidade e integridade com o método anterior?

- Qual é a chave usada para gerar o MAC de um processo de assinatura digital?

Assinatura digital – Implicações

- É possível garantir autenticidade e integridade com o método anterior?
  - Sim! O uso da chave privada junto com o hash permite isso.

- Qual é a chave usada para gerar o MAC de um processo de assinatura digital?
  - Chave privada do emissor. Lembrando que MAC = $H(M, Kpr_e)$.

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).

Roteiro de estudos

1. Leitura das seções 12.1, 12.2,12.3 e 12.5 do livro "Criptografia e segurança de redes. Princípios e práticas". William Stallings;
2. Estudo da vídeo-aula referente ao tópico 12.