EN-3611

Segurança de Redes

Aula 04
Autenticação

Prof. João Henrique Kleinschmidt

Santo André, outubro de 2015

Resumos de mensagem (hash)

- Algoritmo Hash são usados quando a **autenticação é necessária**, mas **o sigilo, não**.

- **Resumo de mensagens** é um método de autenticação que **não exige a criptografia de um documento** (mensagem) **inteiro**.

- **Resumo de mensagens** é um método para **agilizar algoritmos de assinatura** digital.

Resumos de mensagem (hash)

- **Representante** de uma mensagem maior.
- **Verifica a integridade de dados**.
- O método se baseia numa **função *hash*** unidirecional que extrai um trecho qualquer do texto claro e a partir dele calcula uma ***string* de bits de tamanho fixo**.
- Essa função de hash, chamada de **resumo de mensagem**, geralmente representada por *MD (Message Digest),* tem quatro propriedades.

Resumos de mensagem

1. Se *P* for fornecido, o cálculo de *MD(P)* será muito fácil.
2. Se *MD(P)* for fornecido, será impossível encontrar *P*.
3. Dado *P*, ninguém pode encontrar *P'* tal que *MD(P') = MD(P).*
4. Uma mudança na entrada de até mesmo de 1 bit produz uma saída muito diferente.

Resumo de mensagem

- Duas funções ***hash*** amplamente usadas para aplicações práticas:

- **MD5** (Message Digest 5)
  - [Rivest, 1992]
  - 128-bit digest

- **SHA-1** (Secure Hash Algorithm)
  - [NIST,2002]
  - 160-bit digest

Resumo de mensagem

- **Mensagem 1**:
  Daniel, I sold **4** presses to Satomi. Ship immediately.
  (53 bytes)
- **Resumo SHA-1**:
  46 73 a5 85 89 ba 86 58 44 ac 5b e8 48 7a cd 12 63 f8 cl 5a
  (20 bytes)

- **Mensagem 2**:
  Daniel, I sold **5** presses to Satomi. Ship immediately.
  (53 bytes)
- **Resumo SHA-1**:
  2c db 78 38 87 7e d3 le 29 18 49 a0 61 b7 41 81 3c b6 90 7a
  (20 bytes)

Resumo de mensagem

- Mesmo que as mensagens tenham 53 bytes, os resumos têm apenas 20 bytes.
- Independentemente do que você forneça ao SHA-1, o resultado será sempre 20 bytes.
- Funções ***Hash*** são **3-10 vezes mais rápidas que criptografia simétrica**, que por sua vez **é bem mais rápida que criptografia de chave pública**.
- ***Hash*** significa desordem ou confusão

Verificando integridade

- Alice está enviando um contrato para Bob. A mensagem é sobre a venda de quatro computadores a Eva.
- Antes de Alice enviar a mensagem, **ela a resume**.
- Em seguida, Alice **envia os dados (contrato) e o resumo**.
- Quando Bob **tiver os dados**, **ele também os resume**.
- Se o resumo de Bob **corresponder** ao resumo recebido de Alice, ele saberá que **os dados (contrato) não foram alterados** em trânsito.
- Se Eva tivesse interceptado os dados e alterado a mensagem, **o resumo que** Bob **produziu não corresponderia ao resumo de** Alice.
- Bob saberia que **algo aconteceu** e não confiaria nos dados do contrato.
- **No entanto, "**Se Eva pudesse **alterar os dados,** ela também poderia **alterar o resumo enviado"**

Verificar integridade

- Mas **existem duas maneiras de evitar isso**:

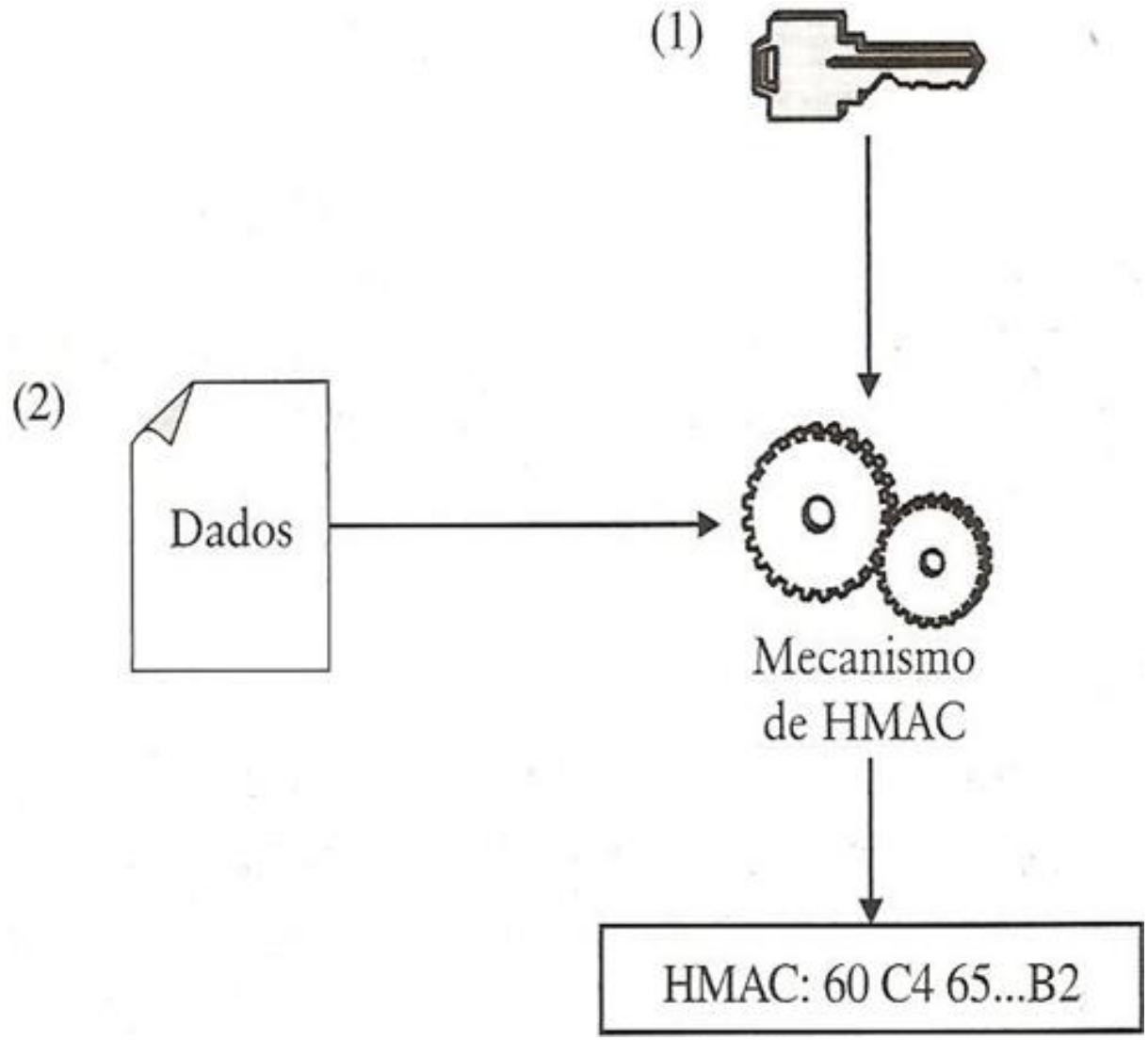
  - Uma maneira é utilizar um **MAC** (**Message Authentication Code**), ou seja, um **código de autenticação de mensagem**.

  - A outra, é utilizar uma **assinatura digital**.

HMAC

- ***Hash Message Authentication Code* –** baseado em resumo

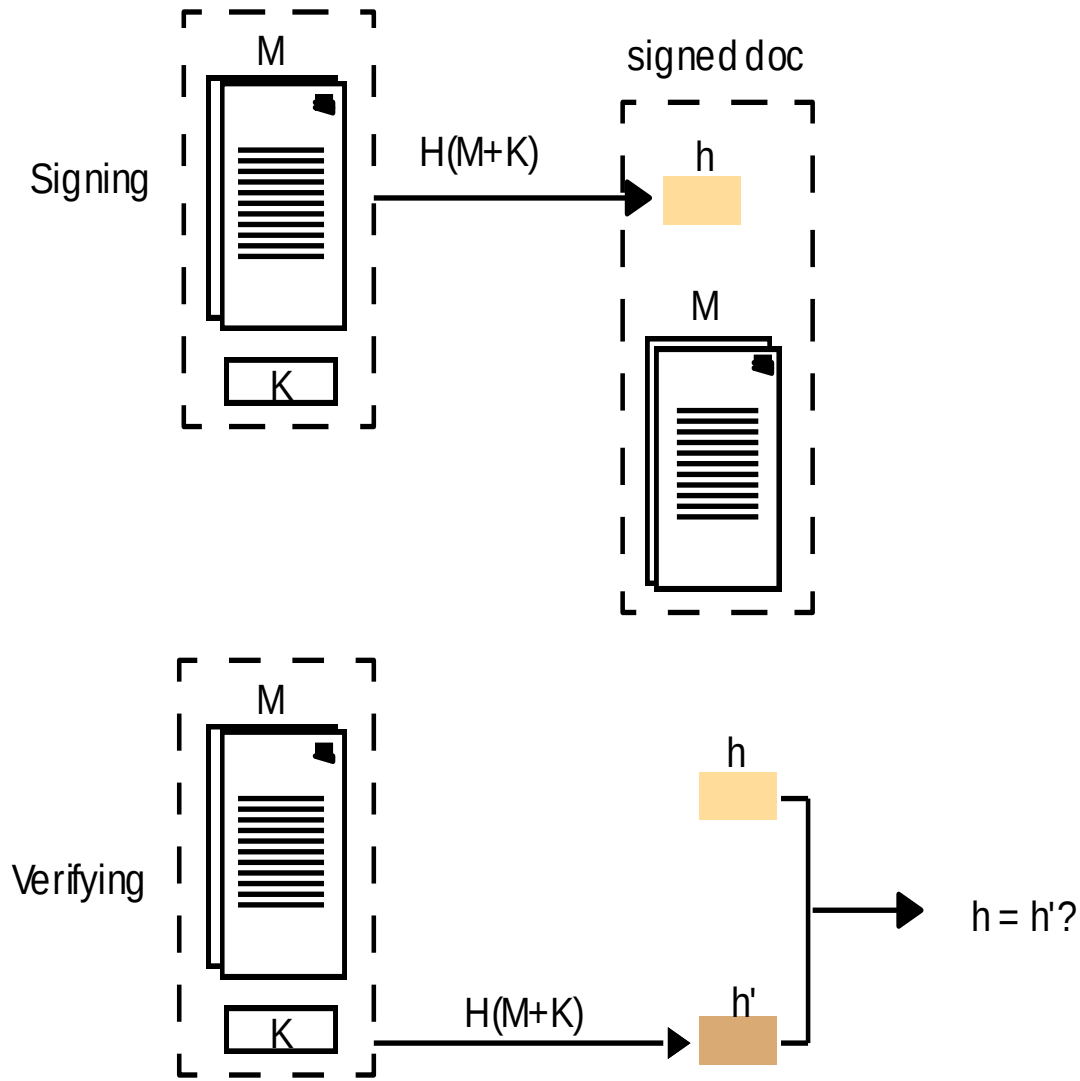
- Para detectar alterações nos dados, **HMAC utiliza uma chave.**
- Um **algoritmo de HMAC resume uma chave e os dados** (chave concatenada com os dados).
- Duas partes compartilham uma chave secreta. Fazem um resumo da chave junto com a mensagem.


(1)
(2)
Dados
Mecanismo
de HMAC
HMAC: 60 C4 65...B2

Verificando a integridade com MAC

1. **A** gera uma chave aleatória ***K*** e a **distribui usando canais seguros** para uma ou mais entidades, que precisam autenticar (verificar a integridade) mensagens recebidas de A.
2. O resumo ***h*** é um **MAC** (representa **M+K**). ***K*** não será comprometido pela revelação de ***h***, visto que a função ***h*** tem seu valor totalmente obscuro.
3. O receptor, **B**, concatena a chave secreta compartilhada, ***K,*** com o documento ***M*** e computa o resumo ***h' = h(M+K).*** A integridade de ***M*** é verificada se ***h = h'.***

Verificando a integridade com MAC



HMAC

- Suponha que Eva intercepte a transmissão e **mude a mensagem** original, tentando fazer com que Bob despache **5 computadores**, ao invés de **4**, substituindo a mensagem original de Alice.
- Depois de substituir a mensagem, ela a **envia a nova mensagem modificada e o HMAC da primeira**, ao Bob .
- Mas, então, Eva deveria alterar o HMAC. Não conseguirá, pois tem de descobrir qual valor de HMAC deveria ser o correto.
- Se Eva substituísse esse resumo, Bob ainda saberia que algo está errado.
- Se Eva não conseguiu substituir o resultado da HMAC, Bob **resumiria a chave e a mensagem, confirmando a fraude.**

Falhas de HMAC

- Bob pode saber que os dados vieram de Alice, **mas uma outra pessoa também poderia saber ?**

- Para verificar que os dados vieram de Alice, **o destinatário deve saber qual é a chave** para criar o resumo HMAC apropriado. Bob (o destinatário) sabe a chave secreta compartilhada, mas ninguém mais sabe.

- Bob poderia escrever uma mensagem falsa (passando o número de prensas para 8) e criar a HMAC correta.

Falhas de HMAC

- A **segunda desvantagem** de HMAC é que para uma outra pessoa, além de Alice ou Bob, verificar a HMAC, os correspondentes devem revelar a chave secreta.

- Agora, esse terceiro tem acesso à chave e também pode criar mensagens que parecem genuínas.

- Ou seja, a mensagem (o contrato) **pode ser falsificada** por Bob ou por essa terceira pessoa.

Assinaturas digitais

- A autenticidade de muitos documentos legais é determinada pela presença de uma assinatura autorizada.
- Isto não vale para as fotocópias.
- Para que os **sistemas de mensagens computacionais** possam **substituir o transporte físico de documentos** em papel e tinta, deve-se encontrar um **método que permita assinar os documentos de um modo que não possa ser forjado**.

Assinaturas digitais

- Necessita-se de um **sistema** através do qual **uma parte possa enviar uma mensagem "assinada" para outra** parte de forma que:

1. O receptor possa **verificar a identidade** alegada pelo transmissor.
2. Posteriormente, o transmissor **não possa repudiar** o conteúdo da mensagem.
3. O receptor não tenha a **possibilidade de forjar** ele mesmo a mensagem.

* Leis estão sendo aprovadas e adotadas, que declaram uma assinatura digital como uma maneira de associar juridicamente a assinatura de documentos.

Assinatura de Chave Pública

- A criptografia de chave pública ajuda a resolver o **problema da distribuição de chaves**.

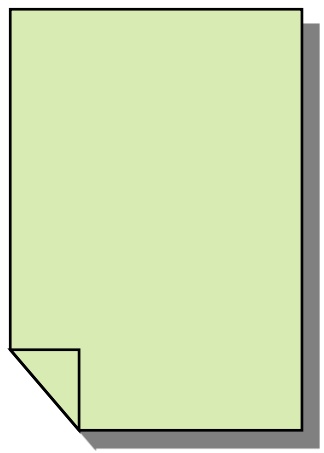
- Também resolve duas outras questões: autenticação e não-repúdio.

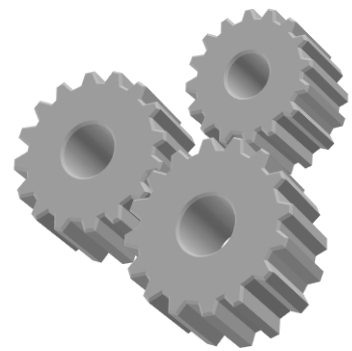
- Quando se usa o **RSA**, significa que qualquer texto simples que tenha sido encriptado com a **chave pública** pode ser descriptografado apenas com a **chave privada**.

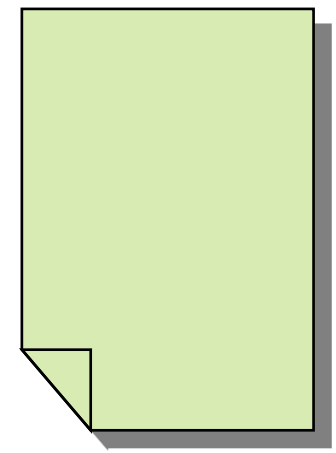
- O que aconteceria **se criptografássemos um texto simples com uma chave privada?** Isso é possível?

Assinatura digital

Chave Privada



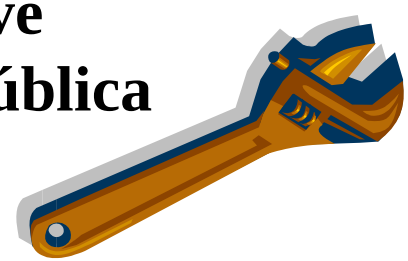


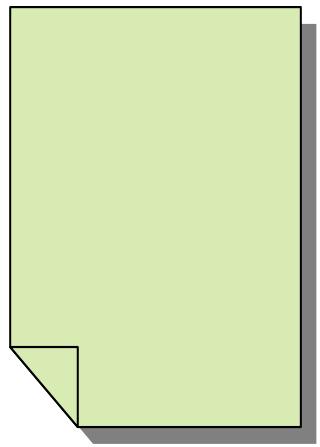


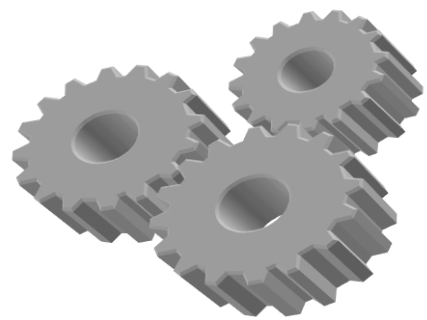
Criptografa (assina)

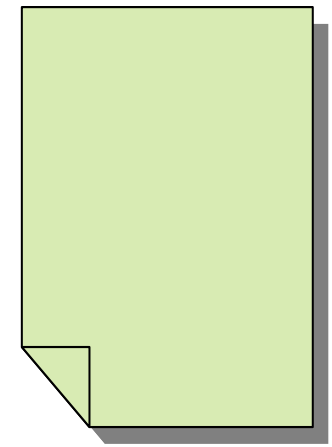
Assinatura digital

Chave Pública









Descriptografa (verifica assinatura)

Assinatura digital

- Duas suposições fundamentais:

  - que a chave seja segura e que apenas o proprietário da chave tenha acesso a ela (chaves devem ser protegidas)

  - a única forma de produzir uma assinatura é através da chave privada

- É possível mostrar que uma assinatura é única?

Assinatura digital

- Ninguém provou completamente a unicidade de uma assinatura **para qualquer esquema de assinatura**.
- **O que se pode afirmar?**
- **Cada fragmento** de dados **tem sua própria assinatura**.

- Nenhuma **única** assinatura digital é associada a uma pessoa ou a um par de chaves.

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

Assinatura digital

- Quando uma pessoa assina duas mensagens diferentes com **a mesma chave**, **as assinaturas serão diferentes**.
- Quando duas pessoas com chaves distintas assinam os mesmos dados, elas **produzirão assinaturas diferentes**.

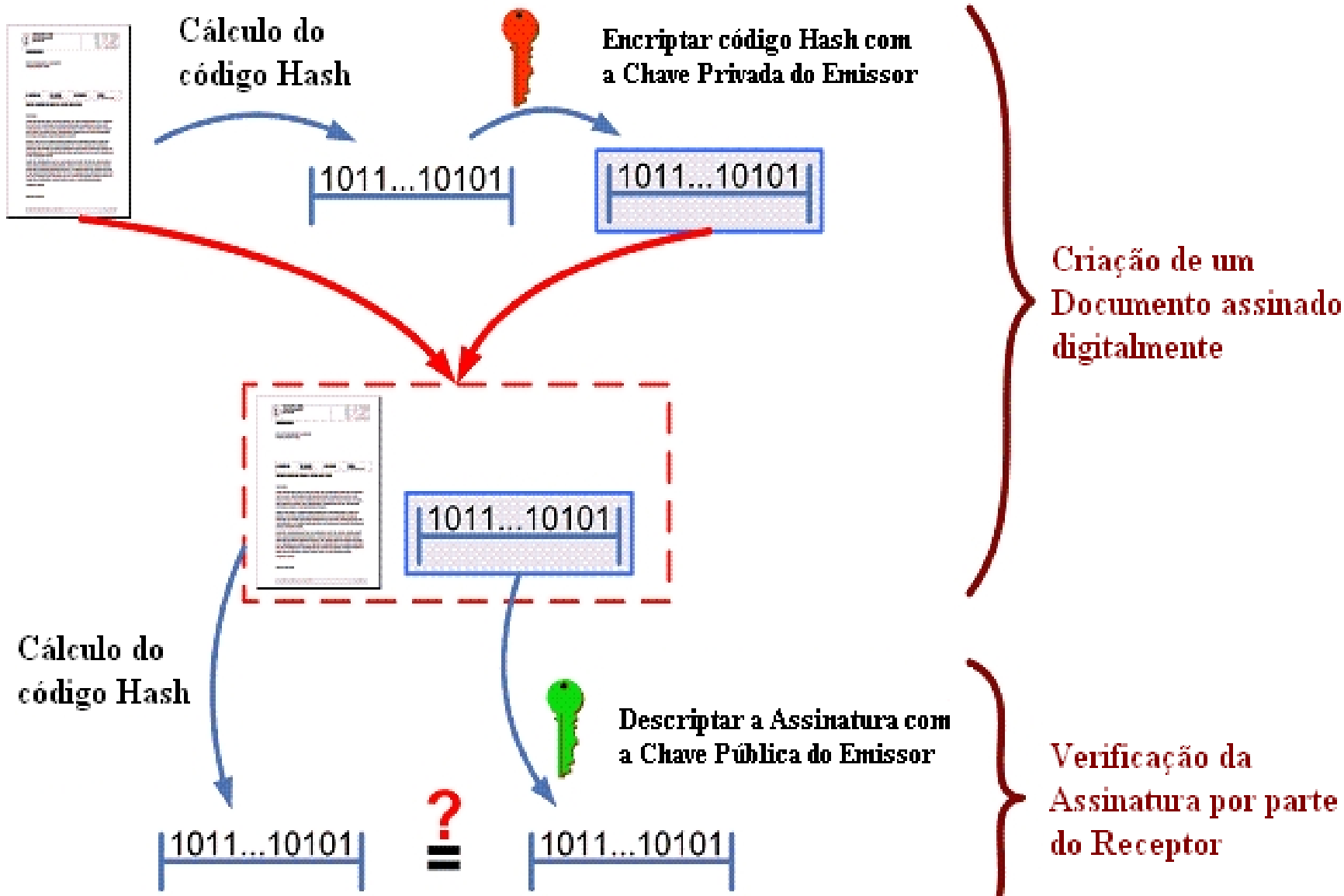
- Como resultado, **ninguém pode pegar uma assinatura válida e acrescentá-la à parte inferior de uma mensagem** que não originou a mesma.
- Algo que torna **a falsificação de uma assinatura** muito mais difícil.

Assinatura com chave pública

- O método para **A** assinar uma mensagem ***M*** e **B** verificar a assinatura é como segue:

1. **A** gera um par de chaves **(K_{pub}, K_{priv})**, e publica a chave K_{pub}, disponibilizando em um local bem conhecido.
2. Computa o resumo (hash) de ***M***, ***H(M)***, usando uma função *hash* segura e criptografa o resumo usando a chave privada K_{priv} para produzir a assinatura $S = \{ H(M) \}_{Kpriv}$.
3. **A** envia a mensagem assinada $[M]_k$ **= <M,S>** à **B**.
4. **B** decriptografa ***S*** usando K_{pub} e computa o resumo de ***M***, ***H(M)***. Se os resumos de **A** e de **B** correspondem, **a assinatura é válida**.

Criando e verificando a Assinatura Digital



Se o cálculo do código Hash não for igual ao resultado da assinatura descriptada, então o documento foi modificado após seu envio ou a assinatura não foi gerada com a Chave Privada so Emissor alegado

Resumo

- A **criptografia de chave simétrica** fornece privacidade sobre os dados sigilosos.
- A **criptografia de chave pública** resolve o problema da distribuição de chaves.
- **Resumo de mensagem** – seja com HMAC ou assinatura – assegura integridade.
- Uma **assinatura** oferece **autenticação e não-repúdio.**

Assinatura

- As assinaturas digitais, por si só, servem muito bem à verificação de uma quantidade limitada de pessoas, com as quais você está familiarizado.
- E se você receber uma mensagem de alguém que você não conheça ou de uma empresa desconhecida?
- O fato de a assinatura ter sido verificada não significa muita coisa. Afinal, qualquer pessoa pode obter um par de chaves e assinar uma mensagem, mas esta poderia estar se fazendo passar por outra.

Certificação

- Através de um sistema de certificados, é possível autenticar a identidade de alguém ou de uma empresa.

- A autenticação ocorre quando um terceiro, como uma empresa confiável, verifica e atesta a veracidade da identidade de uma entidade. Ex: Verisign, Certisign, SERPRO, CEF.