Criptografia de chave pública

Segurança de dados – MSI

Prof. Daniel Saad Nogueira Nunes

Criptografia de Chave Pública

- A criptografia de chave pública, proposta publicamente por Diffie e Hellman em 1976 é o primeiro avanço verdadeiramente revolucionário na criptografia em milhares de anos.
- Algoritmos de chave pública são baseados em funções matemáticas em vez de em simples operações sobre sequências de bits, como as usadas em algoritmos criptográficos simétricos.

Criptografia de Chave Pública

- A criptografia de chave pública é **assimétrica**, pois envolve a utilização de duas chaves separadas, em contraste com a criptografia simétrica, que utiliza somente uma chave.
- A utilização de duas chaves tem profundas consequências nas áreas de confidencialidade, distribuição de chave e autenticação.

Criptografia de Chave Pública

- Existem alguns mitos referentes à criptografia de chave pública:
  - Ela é mais segura do que a criptografia simétrica.
  - Tornou a criptografia simétrica obsoleta.

Criptografia de Chave Pública

Mito #1: Criptografia de Chave Pública é mais Segura

- A criptografia de chave pública não é mais resistente à criptoanálise do que a criptografia simétrica.
- A segurança de qualquer esquema de criptografia depende:
  - Tamanho da chave.
  - Esforço computacional na quebra de uma cifra.
- Não há nada na criptografia simétrica, nem na de chave pública, que torne uma superior à outra neste quesito.

Criptografia de Chave Pública

Mito #2: Tornou a Criptografia Simétrica Obsoleta

- Em razão do alto custo computacional dos esquemas de criptografia de chave pública, é improvável que a criptografia simétrica seja abandonada em um futuro próximo.
- Os mecanismos para distribuição de chaves não são mais simples nem mais eficientes do que os exigidos pela criptografia simétrica.

Criptografia de Chave Pública

Elementos da Criptografia de Chave Pública

- Texto às claras: é a mensagem ou dados legíveis passados para o algoritmo como entrada.
- Algoritmo de cifração: executa várias transformações no texto às claras.
- Chave pública e privada: é um par de chaves que foi selecionado de modo que, se uma é usada para cifrar, a outra é usada para decifrar.
  - As transformações utilizadas pelo algoritmo de cifração dependem da chave pública ou privada que é passada como entrada.

Criptografia de Chave Pública

Elementos da Criptografia de Chave Pública

- Texto cifrado: mensagem embaralhada e ininteligível produzida como saída. Ela depende do texto às claras e da chave. Para dada mensagem, duas chaves diferentes produzirão textos cifrados diferentes.
- Algoritmo de decifração: aceita o texto cifrado e a chave correspondente, e produz o texto às claras original.

Uma Anedota

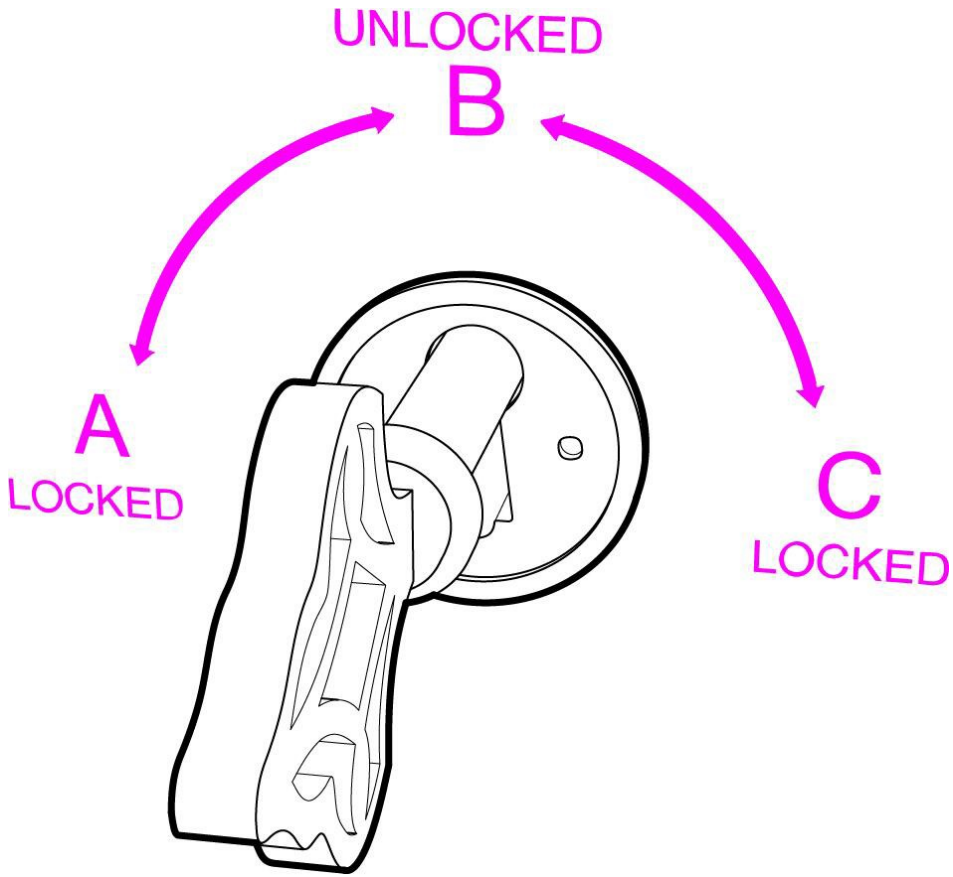


Figura: https://medium.com/@vrypan/explaining-public-key-cryptography-to-non-geeks-f0994b3c2d5

Criptografia de Chave Pública

- Como o nome sugere, a chave pública do par torna-se pública para outros usarem, enquanto a chave privada é de conhecimento apenas de seu proprietário.
- Um algoritmo criptográfico de chave pública de uso geral depende de uma chave para a cifração e de uma chave diferente, mas relacionada, para a decifração.

Criptografia de Chave Pública

Etapas Essenciais

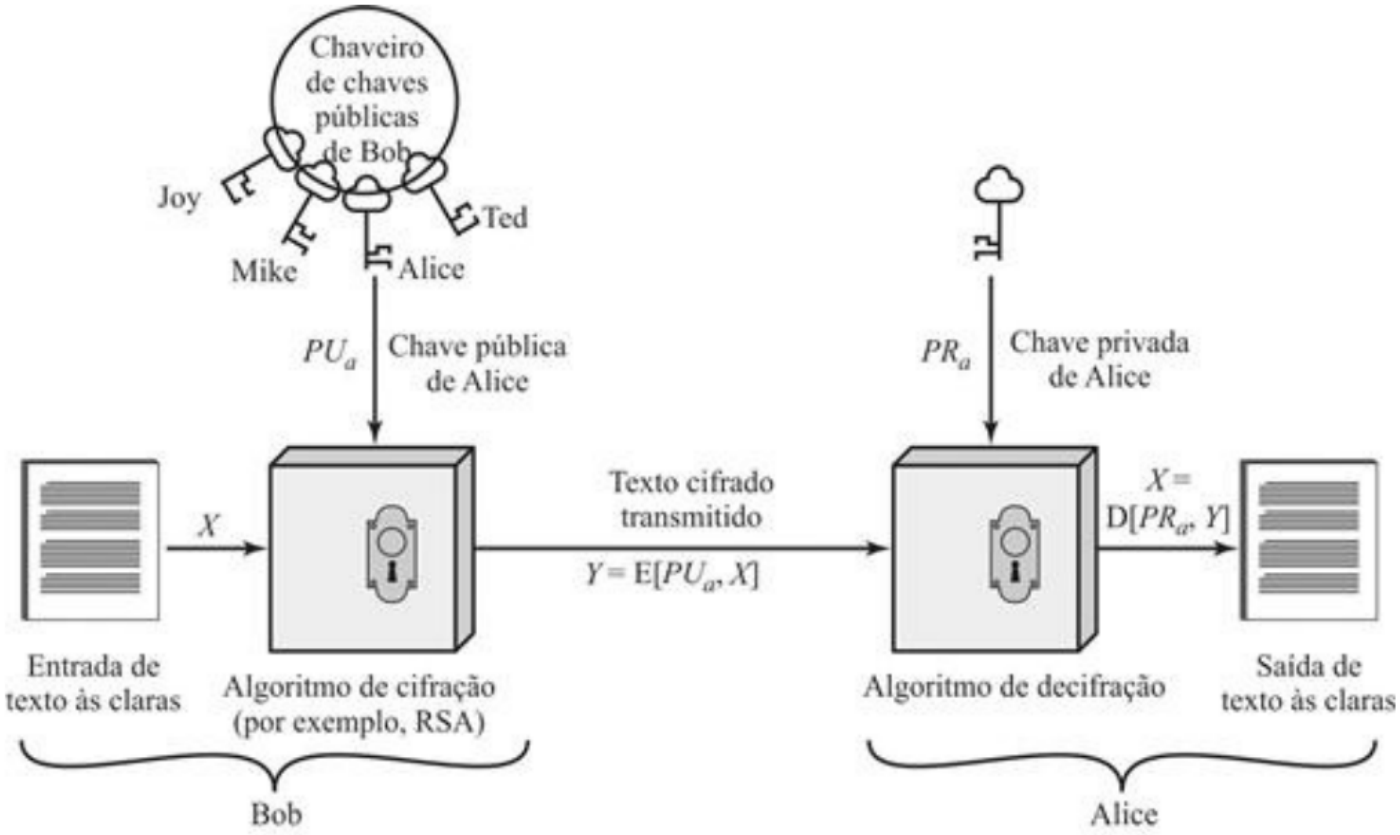
- Cada usuário gera um par de chaves a ser usado para a cifração e decifração de mensagens.
- Cada usuário coloca uma das duas chaves em um registro público ou outro arquivo acessível. Esta é a chave pública. A chave mantida é a privada. Um usuário pode ter domínio de várias chaves públicas de outros usuários.
- Se Bob desejar enviar uma mensagem privada a Alice, ele cifra a mensagem usando a chave pública de Alice.
- Quando Alice recebe a mensagem, ela a decifra usando a sua chave privada.

Criptografia de Chave Pública

Etapas Essenciais

- Nenhum outro destinatário pode decifrar a mensagem porque somente Alice sabe qual é a chave privada de Alice.
- **Confidencialidade!**

Criptografia de Chave Pública

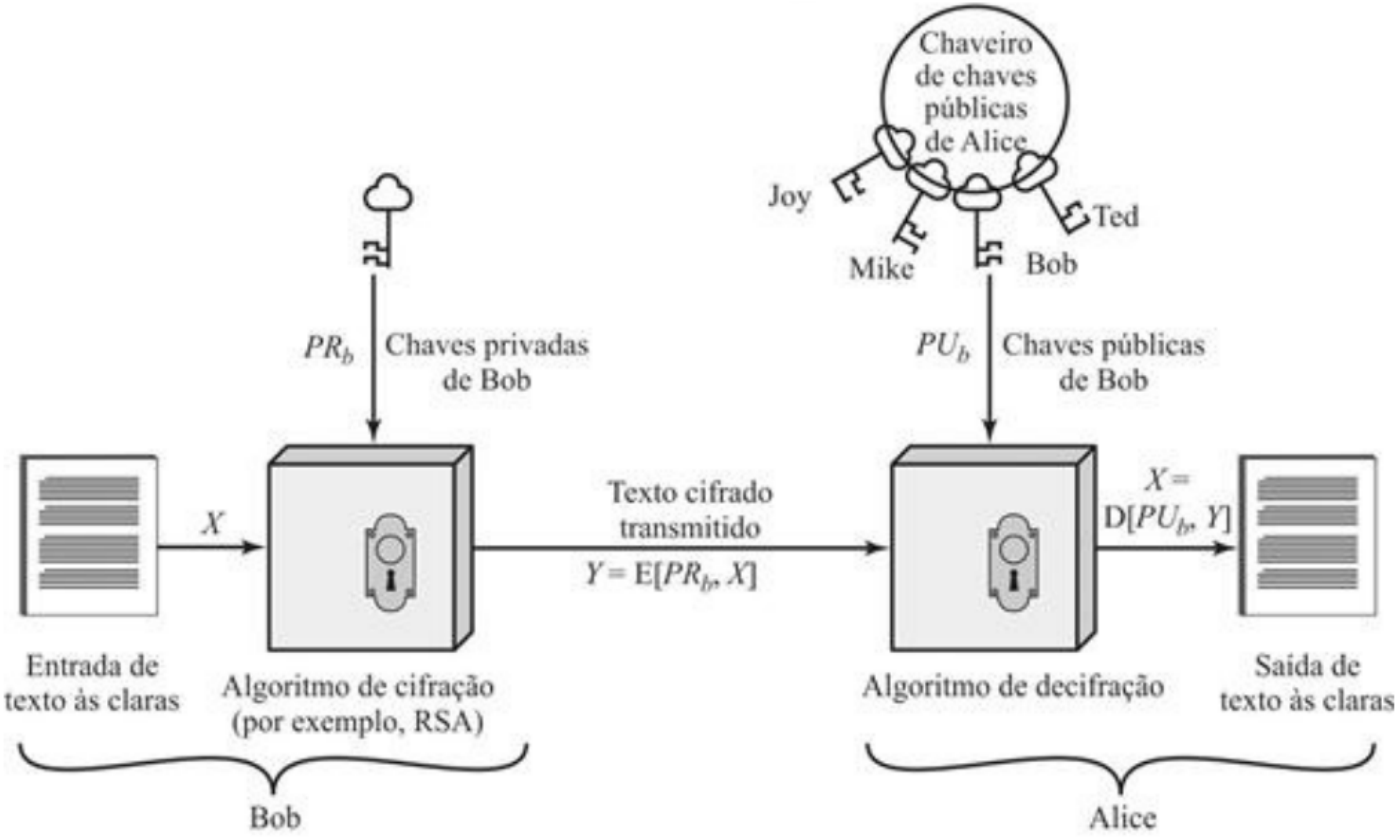


(a) Cifração com chave pública

Criptografia de Chave Pública

- Outro modo de utilizar a criptografia de chave pública é Alice cifrar o texto com sua chave privada w enviar o texto cifrado.
- Qualquer usuário com a chave pública pode decifrar o texto.
- Mas só por que ela veio da Alice.
- **Autenticidade!**

Criptografia de Chave Pública



(b) Cifração com chave privada

Aplicações para Criptossistemas de Chave Pública

- Dependendo do objetivo, o remetente utiliza a chave pública ou a chave privada.
- Classificamos a utilização de criptossistemas de chave pública em três categorias:
  - Assinatura digital.
  - Distribuição de chave simétrica.
  - Cifração de chaves secretas.

Aplicações para Criptossistemas de Chave Pública

Algoritmo	Assinatura Digital	Distribuição de chave simétrica	Cifração de chaves secretas
RSA	Sim	Sim	Sim
Diffie-Hellman	Não	Sim	Não
DSS	Sim	Não	Não
Curvas Elípticas	Sim	Sim	Sim

Requisitos para Criptografia de Chave Pública

- Para serem viáveis, os criptossistemas de chave pública devem cumprir alguns requisitos.

Requisitos para Criptografia de Chave Pública

Requisitos

- É computacionalmente fácil para uma entidade B gerar um par $(\mathrm{PU}_b, \mathrm{PR}_b)$. A chave pública e privada.
- É computacionalmente fácil para um remetente A, que conheça a chave pública e a mensagem a ser cifrada, M, gerar o texto cifrado correspondente:

$$C = E(\mathrm{PU}_b, M)$$

Requisitos para Criptografia de Chave Pública

Requisitos

- É computacionalmente fácil para o destinatário B decifrar o texto cifrado resultante usando a chave privada para recuperar a mensagem original:

$$M = D(\mathrm{PR_b}, \mathrm{C}) = D[\mathrm{PR}_b, E(\mathrm{PU}_b, M)]$$

Requisitos para Criptografia de Chave Pública

Requisitos

- É computacionalmente inexequível para um oponente que conheça a chave pública, PU_b e um texto cifrado, C, recuperar a mensagem original, M.

Requisitos para Criptografia de Chave Pública

Requisitos

- Qualquer das duas chaves relacionadas pode ser usada para a cifração, sendo a outra usada para a decifração:

$$M = D[\mathrm{PU}_b, E(\mathrm{PR}_b, M)] = D[\mathrm{PR}_b, E(\mathrm{PU}_b, M)]$$

Algoritmos Criptográficos Assimétricos

- Examinaremos agora brevemente os algoritmos criptográficos assiméricos mais amplamente utilizados.

Algoritmos Criptográficos Assimétricos

RSA

- Proposto por Ron Rivest, Adi Shamir e Len Adleman e publicado em 78.
- Cifra de bloco no qualo texto às claras e o texto cifrado são inteiros entre 0 e $n - 1$.
- Quebrável com chaves pequenas.
- Chaves de 1024 bits ou mais são utilizadas.
  - Mais de 300 dígitos.

Algoritmos Criptográficos Assimétricos

Acordo de Chaves Diffie-Hellman

- Proposto por Diffie e Hellman em 76.
- Denominado de troca de chaves ou acordo de chaves de Diffie-Hellman.
- Permite que dois usuários cheguem a um acordo seguro sobre um segredo compartilhado.
- Este segredo pode ser utilizado posteriormente para criptografia simétrica.
- Limitado apenas à troca das chaves.

Algoritmos Criptográficos Assimétricos

DSS

- DSS: Digital Signature Standard;
- Usa o SHA-1 e apresenta uma nova técnica de assinatura digital:
  - DSA: Digital Signature ALgorithm
- Provê apenas assinatura digital.
- Diferentemente do RSA, ele não pode ser usado para cifração ou troca de chaves.

Algoritmos Criptográficos Assimétricos

Criptografia de Curvas Elípticas

- Maioria dos produtos e padrões utilizam RSA.
- Para ser seguro, RSA passou a utilizar vários bits, o que ocasiona maior poder de processamento.
- A criptografia de curvas elípticas (ECC), propõe oferecer uma segurança igual a do RSA para um tamanho em bits muito menor, o que reduz o processamento.
- Suas fraquezas ainda não foi provadas extensivamente como no RSA. O nível de confiança ainda não é tão alto.

Assinaturas Digitais e Gerenciamento de Chaves

- Algoritmos de chave pública são usados em uma variedade de aplicações, tais como:
  - Assinatura Digital.
  - Gerenciamento e distribuição de chaves.

Assinaturas Digitais e Gerenciamento de Chaves

- Em relação ao gerenciamento, há no mínimo três aspectos distintos:
  - Distribuição de chaves públicas de maneira segura.
  - Utilização de criptografia de chave pública para distribuir chaves secretas.
  - Utilização de criptografia de chaves temporárias para cifração de mensagens.

Assinaturas Digitais e Gerenciamento de Chaves

- Examinaremos primeiro a assinatura digital.
- Seguiremos após para o gerenciamento de chaves.

Assinatura Digital

- Já vimos como a criptografia de chave pública pode ser usada para autenticação.
- Suponha que Bob queira enviar uma mensagem a Alice.
- Embora não seja importante mantê-la em segredo, ele quer ter certeza de que Alice saiba que a mensagem vem realmente dele.

Assinatura Digital

- Para isso Bob utiliza uma hash segura, como SHA-512, para gerar um valor de hash para a mensagem.
- Ele cifra o código de hash com a sua chave privada criado uma **assinatura digital**.
- Bob envia a mensagem com a assinatura anexada.

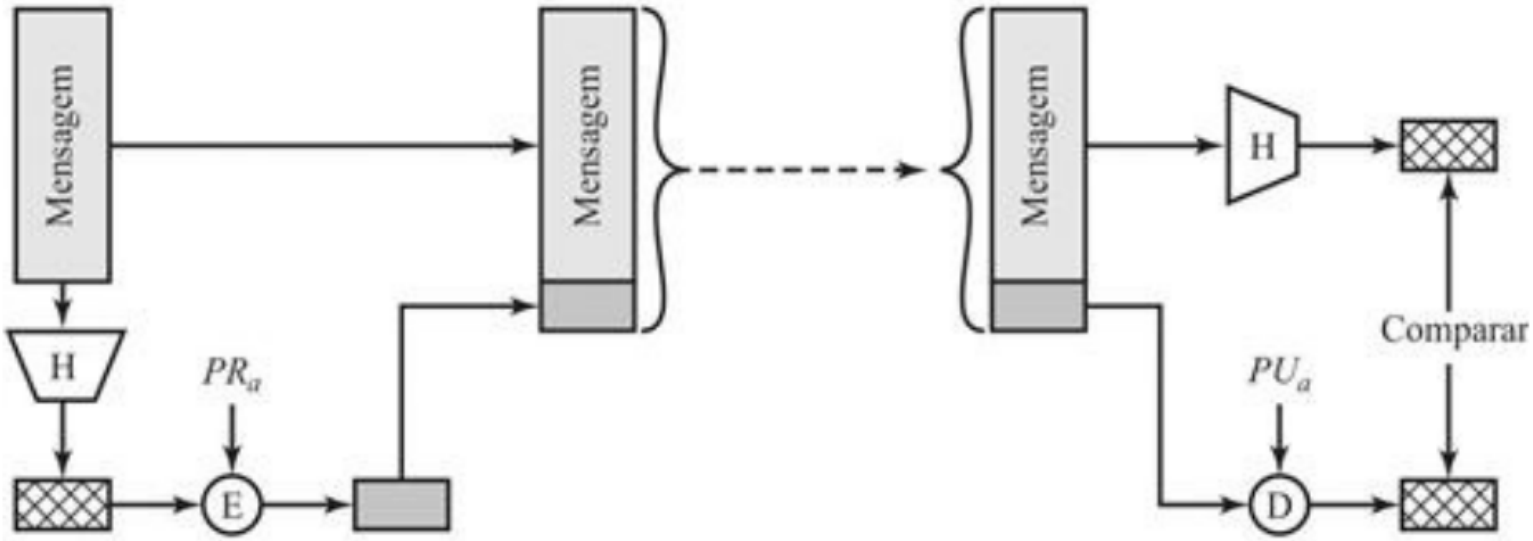
Assinatura Digital

- Quando Alice recebe a mensagem mais a assinatura ela calcular um valor do hash da mensagem.
- Decifra a assinatura digital usando a chave pública de Bob.
- Compara os valores de hash.

Assinatura Digital

- Como ninguém tem a chave privade de Bob, ninguém, além dele, poderia ter criado um texto cifrado que seria decifrado com a chave pública de Bob.
- É impossível também alterar a mensagem ser ter acesso à chave privada de Bob (função hash é segura).
- A mensagem está autenticada em termos de origem.
- Também temos integridade de dados.

Assinatura Digital



(b) Usando criptografia de chave pública

Certificados de Chave Pública

- A particularidade da criptografia de chave pública, é a chave pública.
- Problema: um adversário poderia fingir ser alguém e anunciar uma chave pública fazendo se passar por outra pessoa.
- Solução: certificado de chave pública.

Certificados de Chave Pública

Certificado de Chave Pública

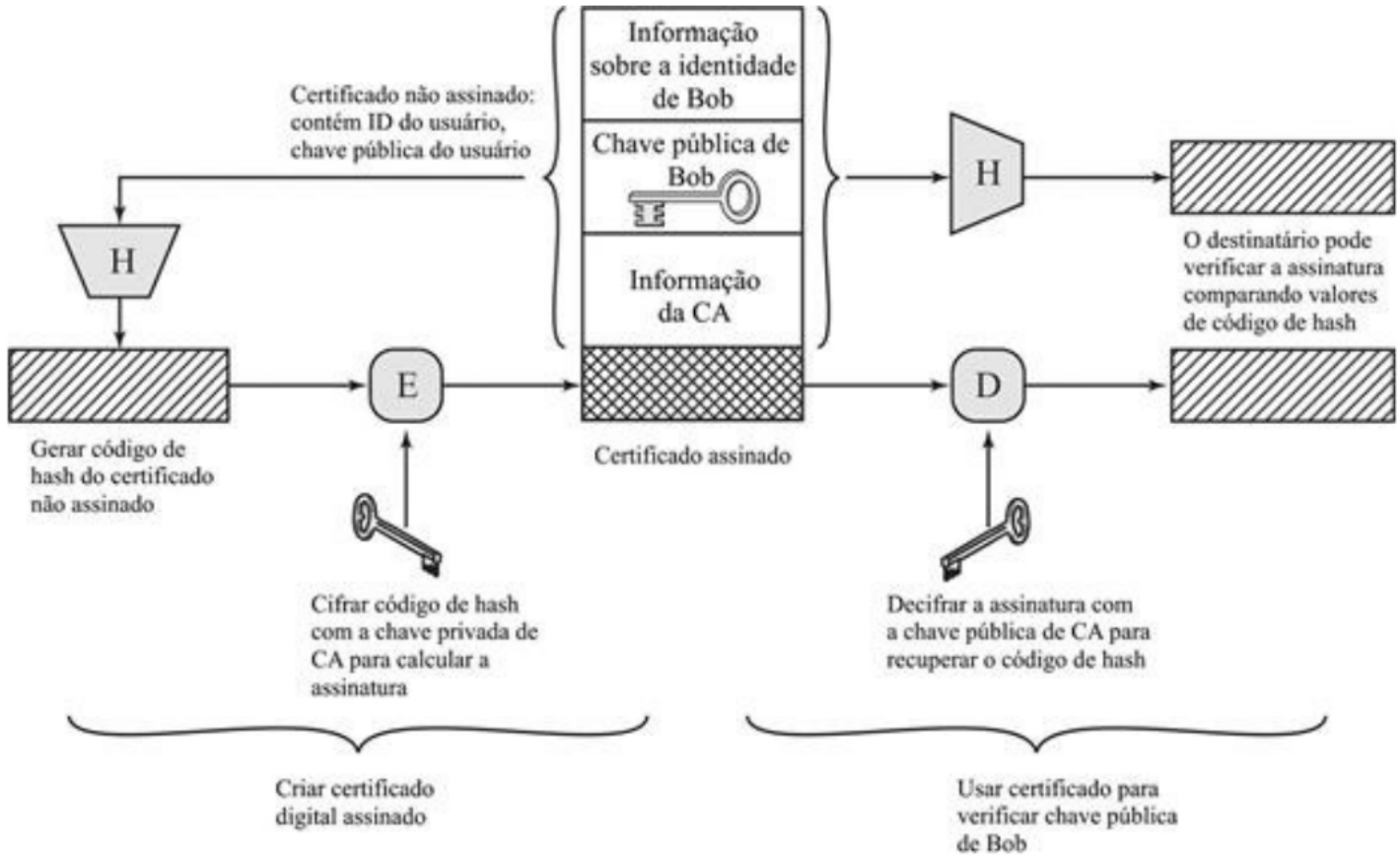
- Consiste de uma chave pública mais um ID de usuário proprietário da chave, assinados por uma terceira entidade confiável.
- Também inclui informações sobre a terceira entidade mais uma indicação do período de validade do certificado.
- Geralmente a terceira entidade é uma Autoridade Certificadora (CA), na qual a comunidade de usuários confia.

Certificados de Chave Pública

Certificado de Chave Pública

- Um usuário pode apresentar a sua chave pública à autoridade de modo seguro e obter um certificado assinado pela CA.
- Então ele pode publicar o certificado.
- Quem precisar da chave pública deste usuário pode obter o certificado e verificar se ele é válido por meio da assinatura confiável anexada.

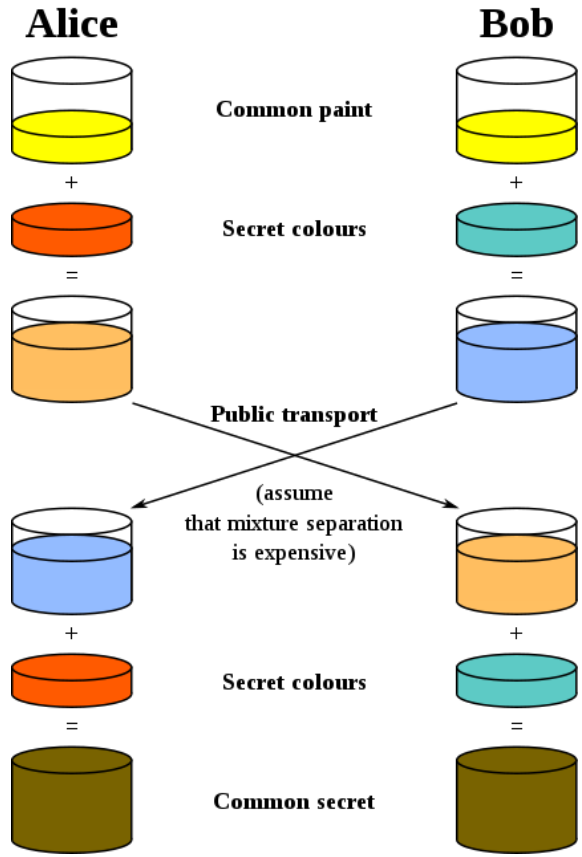
Certificados de Chave Pública



Troca de Chave Simétrica Usando Criptografia de Chave Pública

- Na criptografia simétrica um requisito fundamental é que as duas entidades comunicantes compartilhem uma chave secreta.
- No entanto como os dois podem acordar a chave secreta de maneira segura?
- Utilizando um mecanismo de troca de chaves baseado em criptografia de chave pública.
- Diffie-Hellman.
- Baseado em exponenciação modular.

Troca de Chaves Simétricas



Envelopes Digitais

- Envelopes digitais protegem chaves siméricas.
- Protege uma mensagem sem antes exigir que o remetente e o destinatário tenham a mesma chave secreta.

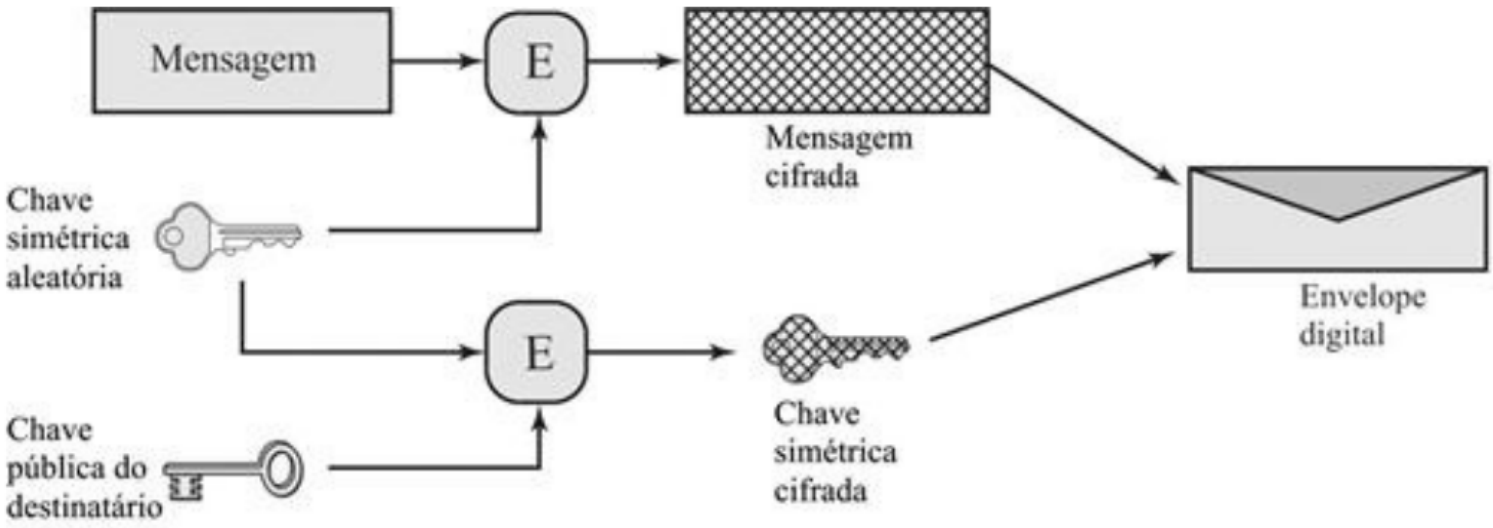
Envelopes Digitais

- Bob prepara uma mensagem.
- Gera uma chave simétrica aleatória que será usada somente desta vez.
- Cifra a mensagem usando criptografia simétrica com a chave secreta de uso único.
- Cifra a chave secreta de uso único usando criptografia de chave pública com a chave pública de alice.
- Anexa a chave secreta de uso único, agora cifrada, à mensagem cifrada e a envia a Alice.

Envelopes Digitais

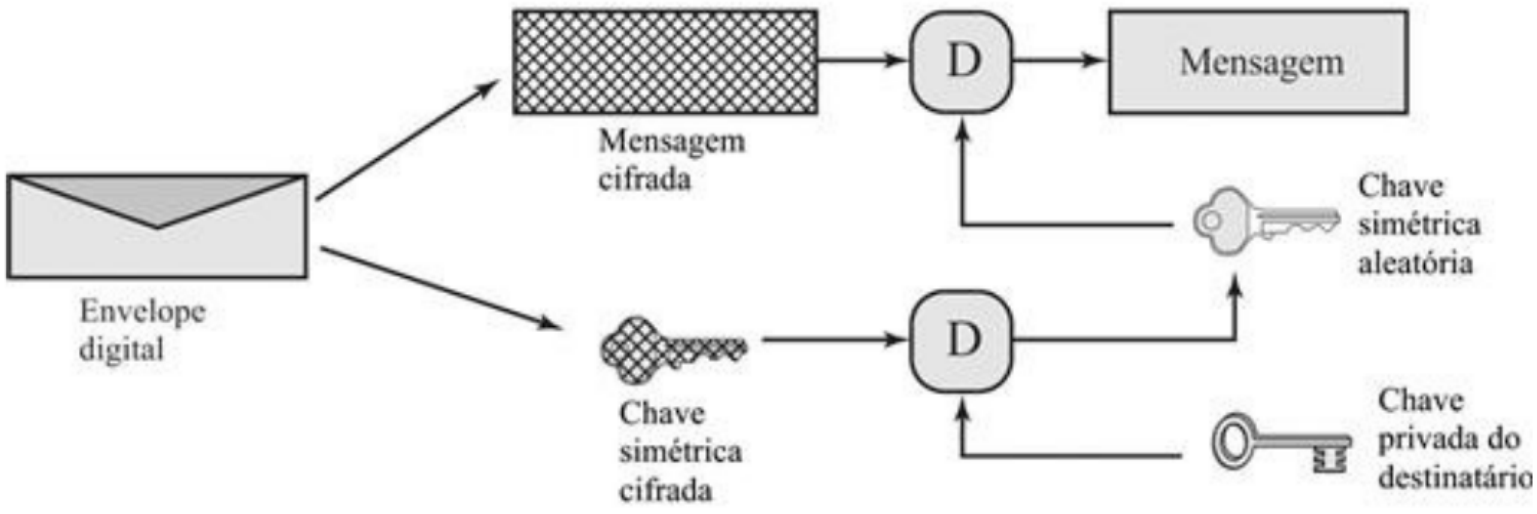
- Somente Alice conseguirá decifrar a chave de uso único e, portanto, recuperar a mensagem original.
- Se Bob obtiver a chave pública de Alice por meio do certificado de chave pública de Alice, ele terá certeza que essa é uma chave válida.

Envelopes Digitais



(a) Criação de um envelope digital

Envelopes Digitais



(b) Abertura de um envelope digital