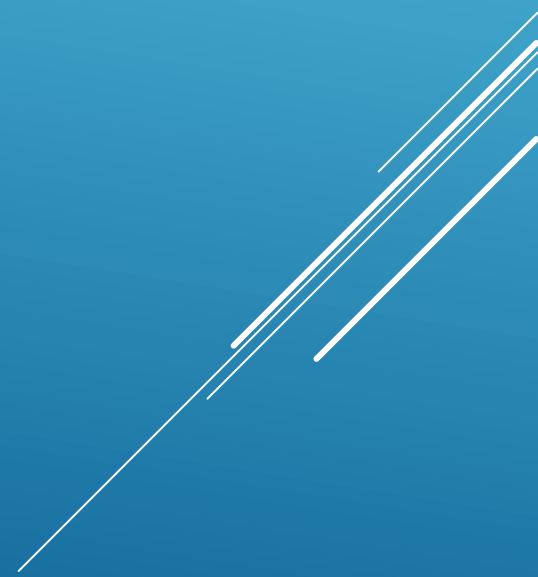


# AGENDA

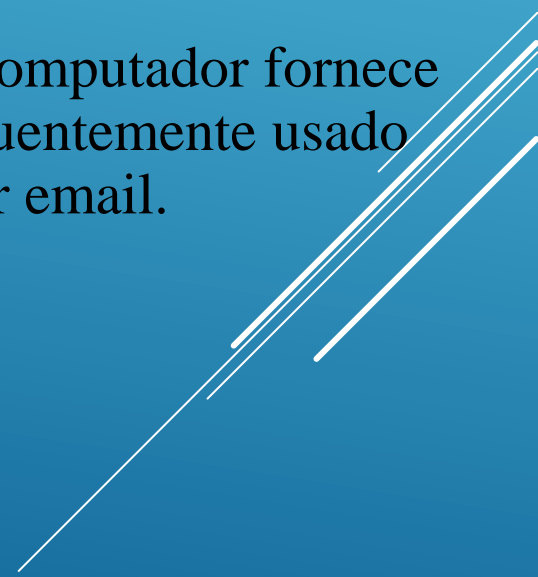
- Algoritmos Assimétricos;
- Assinatura Digital;
- Certificado Digital;
- Autoridades certificadoras.



# ALGORITMOS ASSIMÉTRICOS

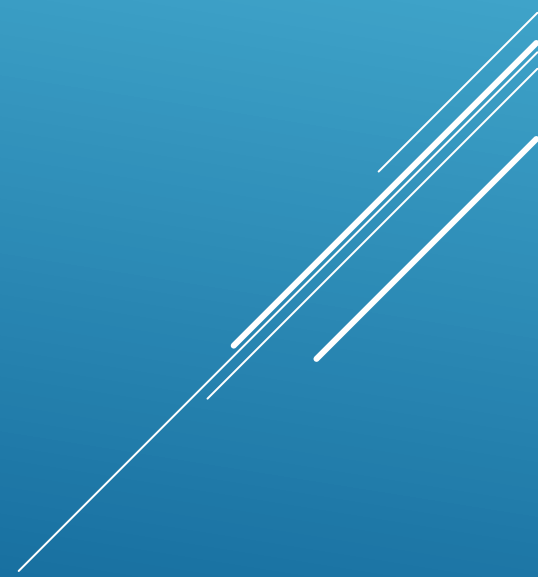
- Algoritmos assimétricos usam uma chave pública e uma chave privada. Os algoritmos assimétricos alcançam confidencialidade, autenticação e integridade usando esse processo.
- Como nenhuma das partes possui um segredo compartilhado, é necessário usar comprimentos de chave muito longos. A criptografia assimétrica pode usar comprimentos de chave entre 512 e 4.096 bits.
- Comprimentos de chave maiores ou iguais a 1.024 bits podem ser confiáveis, enquanto comprimentos menores são considerados não confiáveis.

# ALGORITMOS ASSIMÉTRICOS

- Exemplos de protocolos que usam algoritmos de chave assimétrica:
    - Troca de chaves na Internet (IKE) - este é um componente fundamental das VPNs IPsec.
    - Secure Socket Layer (SSL) - agora é implementado como TLS (Transport Layer Security) padrão da IETF.
    - Shell Seguro (SSH) - Este protocolo fornece uma conexão de acesso remoto seguro a dispositivos de rede.
    - Pretty Good Privacy (PGP) - Este programa de computador fornece privacidade e autenticação criptográficas. É frequentemente usado para aumentar a segurança das comunicações por email.
- 
- Several white diagonal lines of varying lengths and thicknesses are drawn across the bottom right corner of the slide, creating a modern, abstract graphic element.

# ALGORITMOS ASSIMÉTRICOS

- Os algoritmos assimétricos são substancialmente mais lentos que os algoritmos simétricos. Seu design é baseado em problemas computacionais, como fatorar números extremamente grandes ou calcular logaritmos discretos de números extremamente grandes.
- Por serem lentos, algoritmos assimétricos geralmente são usados em mecanismos criptográficos de baixo volume, como assinaturas digitais e troca de chaves.



# ALGORITMOS ASSIMÉTRICOS

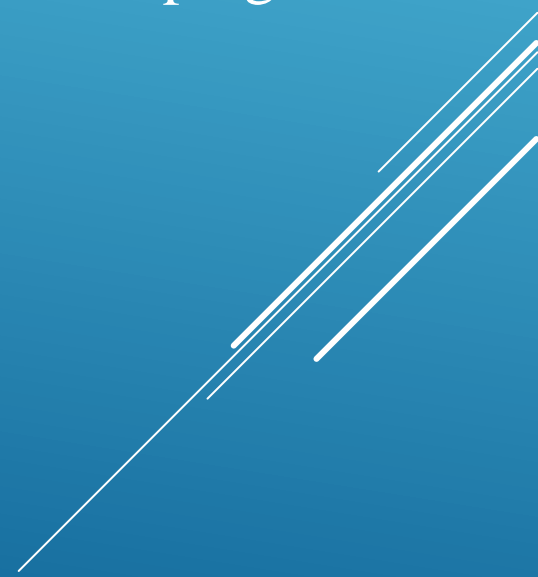
Algoritmos de Criptografia Assimétrica	Tamanho da chave	Descrição
<b>Diffie-Hellman (DH)</b>	512, 1024, 2048, 3072, 4096	O algoritmo Diffie-Hellman permite que os dispositivos compartilhem da mesma chave.
<b>Digital Signature Standard (DSS) Digital Signature Algorithm (DSA)</b>	512 - 1024	O DSS especifica o DSA como o algoritmo para assinaturas digitais. DSA é um algoritmo de chave pública baseado no esquema de assinatura ElGamal. A velocidade de criação de assinaturas é semelhante à RSA, mas é 10 a 40 vezes mais lenta para verificação.
<b>Rivest, Shamir, and Adleman encryption algorithms (RSA)</b>	512 to 2048	O RSA é para criptografia de chave pública que se baseia na dificuldade atual de fatorar números muito grandes. É o primeiro algoritmo conhecido usado para assinatura e criptografia. É amplamente utilizado em protocolos de comércio eletrônico e acredita-se que seja seguro dadas as chaves suficientemente longas e o uso de implementações atualizadas.
<b>ElGamal</b>	512 - 1024	Um algoritmo de criptografia de chave assimétrica para criptografia de chave pública que é baseado no acordo-chave Diffie-Hellman. Uma desvantagem do sistema ElGamal é que a mensagem criptografada se torna muito grande, cerca de duas vezes o tamanho da mensagem original e por isso é usada apenas para pequenas mensagens, como chaves secretas.
<b>Elliptical curve techniques</b>	160	A criptografia de curva elíptica pode ser usada para adaptar muitos algoritmos criptográficos, como Diffie-Hellman ou ElGamal. A principal vantagem da criptografia da curva elíptica é que as chaves são muito menores.

# ALGORITMO DIFFIE-HELMANN

- Diffie-Hellman (DH) é um algoritmo matemático assimétrico em que dois computadores geram uma chave secreta compartilhada idêntica sem ter se comunicado antes. A nova chave compartilhada nunca é realmente trocada entre o remetente e o destinatário.
- Aqui estão três exemplos de casos em que o DH é comumente usado:
  - Os dados são trocados usando uma VPN IPsec.
  - Os dados são criptografados na internet usando SSL ou TLS.
  - Os dados SSH são trocados.

# ALGORITMO DIFFIE-HELMANN

- A segurança DH usa números incrivelmente grandes em seus cálculos.
- Infelizmente, os sistemas de chave assimétrica são extremamente lentos para qualquer tipo de criptografia em massa. Portanto, é comum criptografar a maior parte do tráfego usando um algoritmo simétrico, como 3DES ou AES e, em seguida, usar o algoritmo DH para criar chaves que serão usadas pelo algoritmo de criptografia.





# ALGORITMO DIFFIE-HELMANN (HTTPS)

```
Cipher Suite: TLS_AES_128_GCM_SHA256 (0x1301)
Cipher Suite: TLS_AES_256_GCM_SHA384 (0x1302)
Cipher Suite: TLS_CHACHA20_POLY1305_SHA256 (0x1303)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_128_GCM_SHA256 (0xc02b)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_GCM_SHA256 (0xc02f)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_AES_256_GCM_SHA384 (0xc02c)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384 (0xc030)
Cipher Suite: TLS_ECDHE_ECDSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca9)
Cipher Suite: TLS_ECDHE_RSA_WITH_CHACHA20_POLY1305_SHA256 (0xcca8)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_128_CBC_SHA (0xc013)
Cipher Suite: TLS_ECDHE_RSA_WITH_AES_256_CBC_SHA (0xc014)
Cipher Suite: TLS_RSA_WITH_AES_128_GCM_SHA256 (0x009c)
Cipher Suite: TLS_RSA_WITH_AES_256_GCM_SHA384 (0x009d)
Cipher Suite: TLS_RSA_WITH_AES_128_CBC_SHA (0x002f)
Cipher Suite: TLS_RSA_WITH_AES_256_CBC_SHA (0x0035)
Cipher Suite: TLS_RSA_WITH_3DES_EDE_CBC_SHA (0x000a)
```

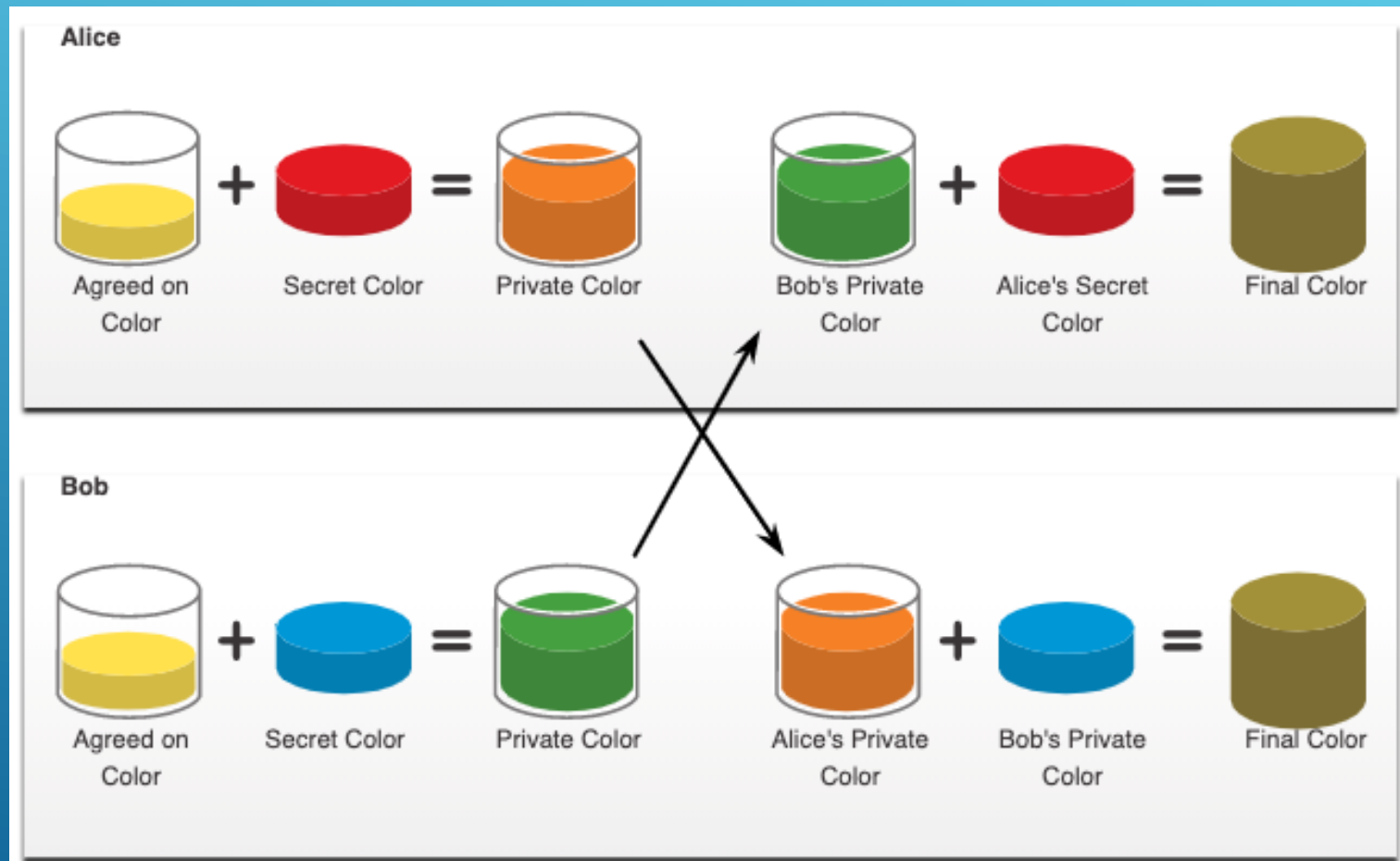


# ALGORITMO DIFFIE-HELMANN (SSH)

```
Wireshark · Follow TCP Stream (tcp.stream eq 0) · eth1

SSH-2.0-OpenSSH_8.0p1 Debian-3
SSH-2.0-OpenSSH_4.7p1 Debian-8ubuntu1
....
...u...=P][... .K...~diffie-hellman-group-exchange-sha256,diffie-hellman-
group-exchange-sha1,diffie-hellman-group14-sha1,diffie-hellman-group1-
sha1...ssh-rsa,ssh-dss...aes128-cbc,3des-cbc,blowfish-cbc,cast128-
cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-cbc,rijndael-
cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr...aes128-cbc,3des-
cbc,blowfish-cbc,cast128-cbc,arcfour128,arcfour256,arcfour,aes192-cbc,aes256-
cbc,rijndael-cbc@lysator.liu.se,aes128-ctr,aes192-ctr,aes256-ctr...ihmac-
md5,hmac-sha1,umac-64@openssh.com,hmac-ripemd160,hmac-
ripemd160@openssh.com,hmac-sha1-96,hmac-md5-96...ihmac-md5,hmac-
sha1,umac-64@openssh.com,hmac-ripemd160,hmac-ripemd160@openssh.com,hmac-
sha1-96,hmac-
md5-96...none,zlib@openssh.com...none,zlib@openssh.com.....
....l.....;E....<.....
curve25519-sha256,curve25519-sha256@libssh.org,ecdh-sha2-nistp256,ecdh-sha2-
nistp384,ecdh-sha2-nistp521,diffie-hellman-group-exchange-sha256,diffie-
hellman-group16-sha512,diffie-hellman-group18-sha512,diffie-hellman-group14-
sha256,diffie-hellman-group14-sha1,ext-info-c...frsa-sha2-512-cert-
v01@openssh.com,rsa-sha2-256-cert-v01@openssh.com,ssh-rsa-cert-
v01@openssh.com,rsa-sha2-512,rsa-sha2-256,ssh-rsa,ecdsa-sha2-nistp256-cert-
```

# ALGORITMO DIFFIE-HELMANN



# ALGORITMO DIFFIE-HELMANN

- A troca de chaves DH começa com Alice e Bob concordando com uma cor comum arbitrária que não precisa ser mantida em segredo (amarelo).
- Em seguida, Alice e Bob selecionarão uma cor secreta. Alice escolheu vermelho enquanto Bob escolheu azul. Essas cores secretas nunca serão compartilhadas com ninguém. A cor secreta representa a chave privada secreta escolhida de cada parte.
- Alice e Bob agora misturam a cor comum compartilhada (amarelo) com sua respectiva cor secreta para produzir uma cor particular.
- Alice envia sua cor particular (laranja) para Bob e Bob envia sua cor particular (verde) para Alice.
- Alice e Bob misturam a cor que receberam com a sua cor secreta original. O resultado é o marrom que é idêntica à mistura final de cores do outro (representa a chave secreta compartilhada).

# ALGORITMO DIFFIE-HELMANN

- Algoritmo para ser usado na distribuição de chaves (sistema de distribuição de chave pública)
  - $g^x \pmod n$
- Onde:  $g$  (a base) precisa ser menor do que  $n$  (o módulo), onde  $n$  é um número primo, e  $g$  precisa ser maior do que 1
- Para obter as chaves, Alice e Bob podem trocar informações abertamente, sem a mínima preocupação com alguém que esteja presente ou que eventualmente esteja interceptando estas informações. Em apenas 4 etapas, os dois terão uma chave secreta.

# ALGORITMO DIFFIE-HELMANN

- **1. A escolha da base e do módulo (público)**
  - Inicialmente Alice e Bob escolhem dois números grandes, um para a base  $g$  e um para o módulo  $n$ , obedecendo as restrições citadas. Esta escolha não necessariamente envolve apenas os dois, mais pessoas podem participar do grupo de usuários. Para facilitar, será usado um exemplo com números pequenos e apenas com Alice e Bob.
  - $g = 7$  e  $n = 11$

# ALGORITMO DIFFIE-HELMANN

## ■ 2. A escolha dos expoentes

- Depois, na privacidade da sua casa, Bob escolhe um expoente  $x$  bem grande. Este número Bob mantém cuidadosamente em segredo. Alice faz a mesma coisa e também mantém sua escolha em segredo. De posse dos seus expoentes, os dois calculam o resultado da função:

- Alice
- -----
- $x = 6$  (segredo)
- $A = 7^6 \pmod{11}$
- $A = 117649 \pmod{11}$
- $A = 4$

- Bob
- -----
- $y = 3$  (segredo)
- $B = 7^3 \pmod{11}$
- $B = 343 \pmod{11}$
- $B = 2$

# ALGORITMO DIFFIE-HELMANN

## ■ 3. A troca de resultados

- No dia seguinte, os dois se encontram novamente no intervalo das aulas. Alice entrega o resultado obtido ( $A=4$ ) para Bob e este entrega o resultado que obteve ( $B=2$ ) para Alice. Mais uma vez, nenhum dos dois está preocupado que alguém tome conhecimento destes números.



# ALGORITMO DIFFIE-HELMANN

## ■ 4. O cálculo da chave secreta

- Com o resultado obtido pelo outro, Bob e Alice voltam a fazer cálculos em particular. Usam a mesma função só que, desta vez, a base usada por Alice é o resultado obtido por Bob e a base usada por Bob é o resultado obtido por Alice. Os expoentes continuam sendo os previamente escolhidos:

■ Alice

■ -----

■  $x = 6$

■  $B' = 2^6 \pmod{11}$

■  $B' = 64 \pmod{11}$

■  $B' = k = 9$  (chave secreta)

Bob

-----

$y = 3$

$A' = 4^3 \pmod{11}$

$A' = 64 \pmod{11}$

$A' = k = 9$  (chave secreta)

- Ambos chegaram ao mesmo resultado e agora possuem uma chave secreta em comum.

# ALGORITMO DIFFIE-HELMANN

## ■ Considerações

- A chave secreta nada mais é do que  $g^{xy} \pmod{n}$ . Para confirmar, basta fazer os cálculos:
- $k = g^{xy} \pmod{n} = 7^{6 \times 3} \pmod{11} = 7^{18} \pmod{11} = 1.628.413.597.910.449 \pmod{11} = 9$

Alice				Bob		
Secreto	Público	Calcula	Envia	Calcula	Público	Secreto
a	p, g		p, g →			b
a	p, g, A	$g^a \pmod{p} = A$	A →		p, g	b
a	p, g, A		← B	$g^b \pmod{p} = B$	p, g, A, B	b
a, <b>s</b>	p, g, A, B	$B^a \pmod{p} = s$		$A^b \pmod{p} = s$	p, g, A, B	b, <b>s</b>

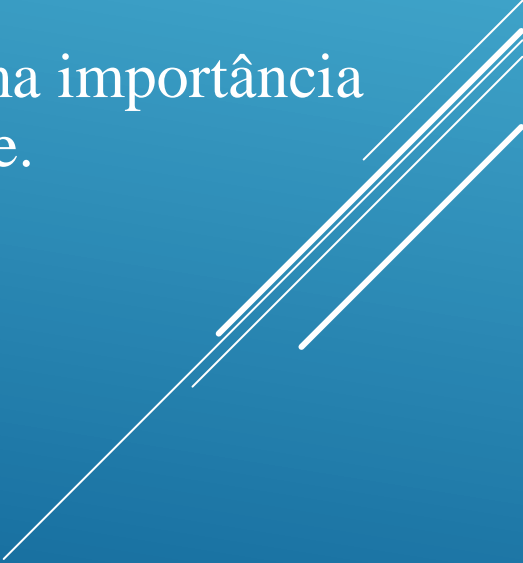
# ALGORITMO DIFFIE-HELMANN EXTENDIDO

- O protocolo de troca de chaves pode ser facilmente estendido para atender três ou mais pessoas. Se João, Maria e Onofre quiserem gerar uma chave secreta, o procedimento é o seguinte:
  - 1. Maria escolhe um inteiro grande qualquer  $x$  e calcula  $X = g^x \pmod{n}$
  - 2. João escolhe um inteiro grande qualquer  $y$  e calcula  $Y = g^y \pmod{n}$
  - 3. Onofre escolhe um inteiro grande qualquer  $z$  e calcula  $Z = g^z \pmod{n}$
  - 4. Maria envia  $X$  para João, João envia  $Y$  para Onofre e Onofre envia  $Z$  para Maria.
  - 5. Maria calcula  $Z' = Z^x \pmod{n}$
  - 6. João calcula  $X' = X^y \pmod{n}$
  - 7. Onofre calcula  $Y' = Y^z \pmod{n}$
  - 8. Maria envia  $Z'$  para João, João envia  $X'$  para Onofre e Onofre envia  $Y'$  para Maria.
  - 9. Maria calcula  $k = Y'^x \pmod{n}$
  - 10. João calcula  $k = Z'^y \pmod{n}$
  - 11. Onofre calcula  $k = X'^z \pmod{n}$

# ALGORITMO DIFFIE-HELMANN EXTENDIDO

- A chave secreta  $k$  é igual a  $g^{xyz} \pmod{n}$  e este protocolo pode ser facilmente estendido para quatro ou mais pessoas.

# ASSINATURA DIGITAL

- As assinaturas digitais oferecem a mesma funcionalidade que as assinaturas manuscritas para documentos eletrônicos.
  - Uma assinatura digital é usada para determinar se alguém edita um documento depois que o usuário o assina.
  - Uma assinatura digital é um método matemático usado para verificar a autenticidade e integridade de uma mensagem, documento digital ou software.
  - Em muitos países, assinaturas digitais têm a mesma importância jurídica que um documento assinado manualmente.
  - As assinaturas digitais também fornecem repúdio.
- 

# ASSINATURA DIGITAL

## ■ Aplicações

- Verificar se uma mensagem realmente foi enviada pelo remetente declarado.
- Usadas para **datar documentos**: uma pessoa de confiança **assina** o documento, a data e a hora com sua chave secreta, atestando que o documento existia no momento indicado.
- Testemunhar (ou **certificar**) que determinada chave pública pertence a uma determinada pessoa. Isto é feito assinando-se a combinação da chave e a informação sobre o proprietário através de chave de confiança.
- A assinatura digital de terceiros de confiança (proprietários de chaves de confiança), a chave pública e a informação a respeito de seu proprietário são geralmente chamadas de **certificados**.

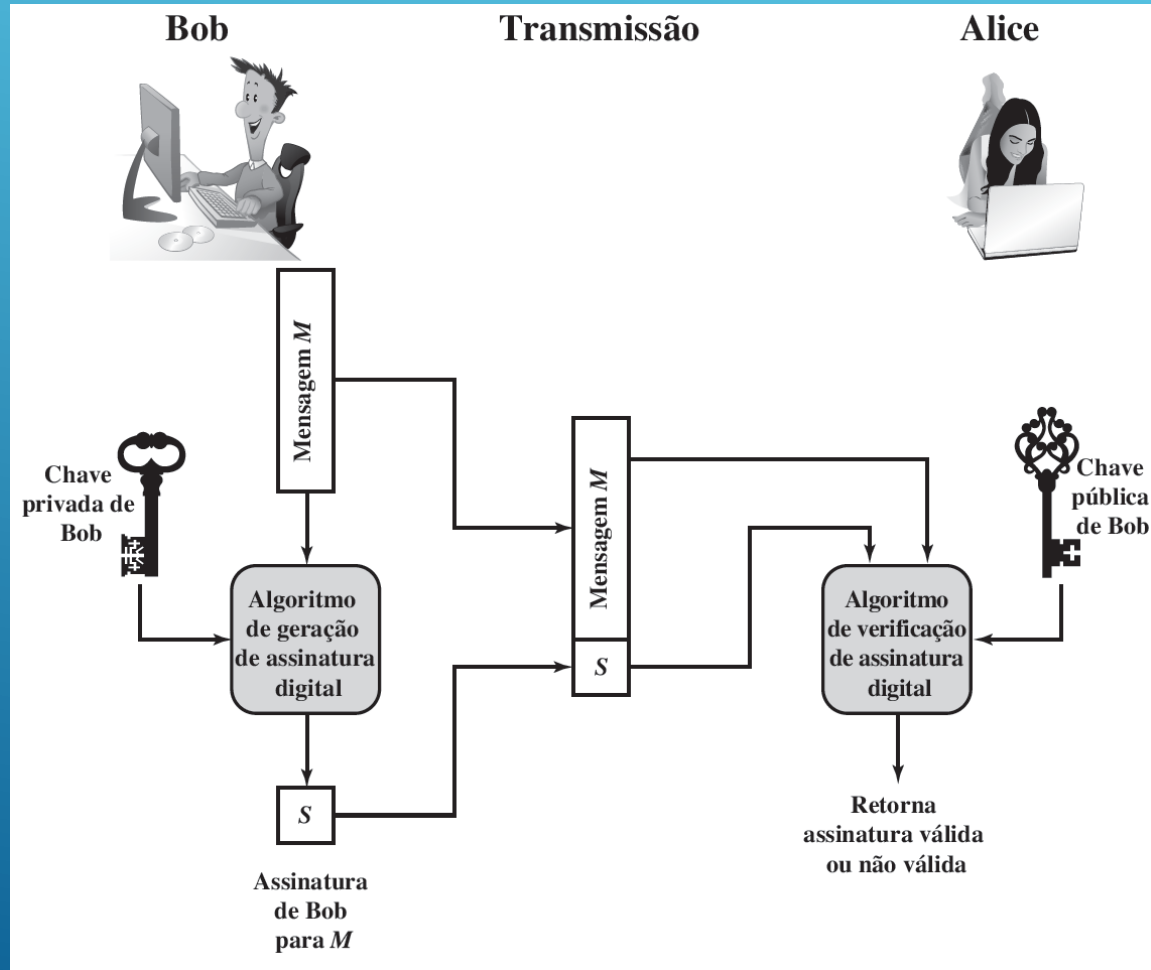
# ASSINATURA DIGITAL

- **Formas possíveis para implementar assinaturas digitais.**
  - Funções de hash (MD5, SHA);
  - Algoritmos de chave assimétrica (DSA, RSA, ElGamal, Curva Elíptica)



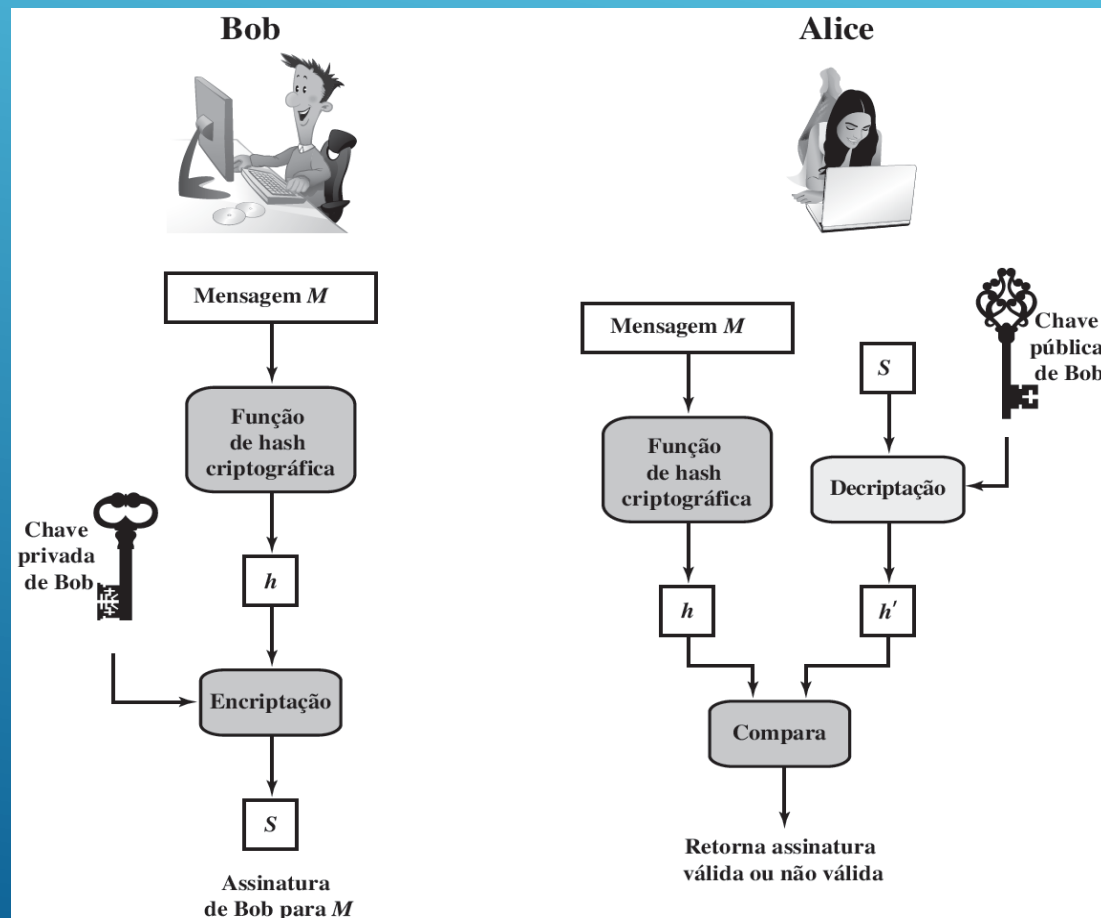
# ASSINATURA DIGITAL

- Modelo genérico do processo de assinatura digital:



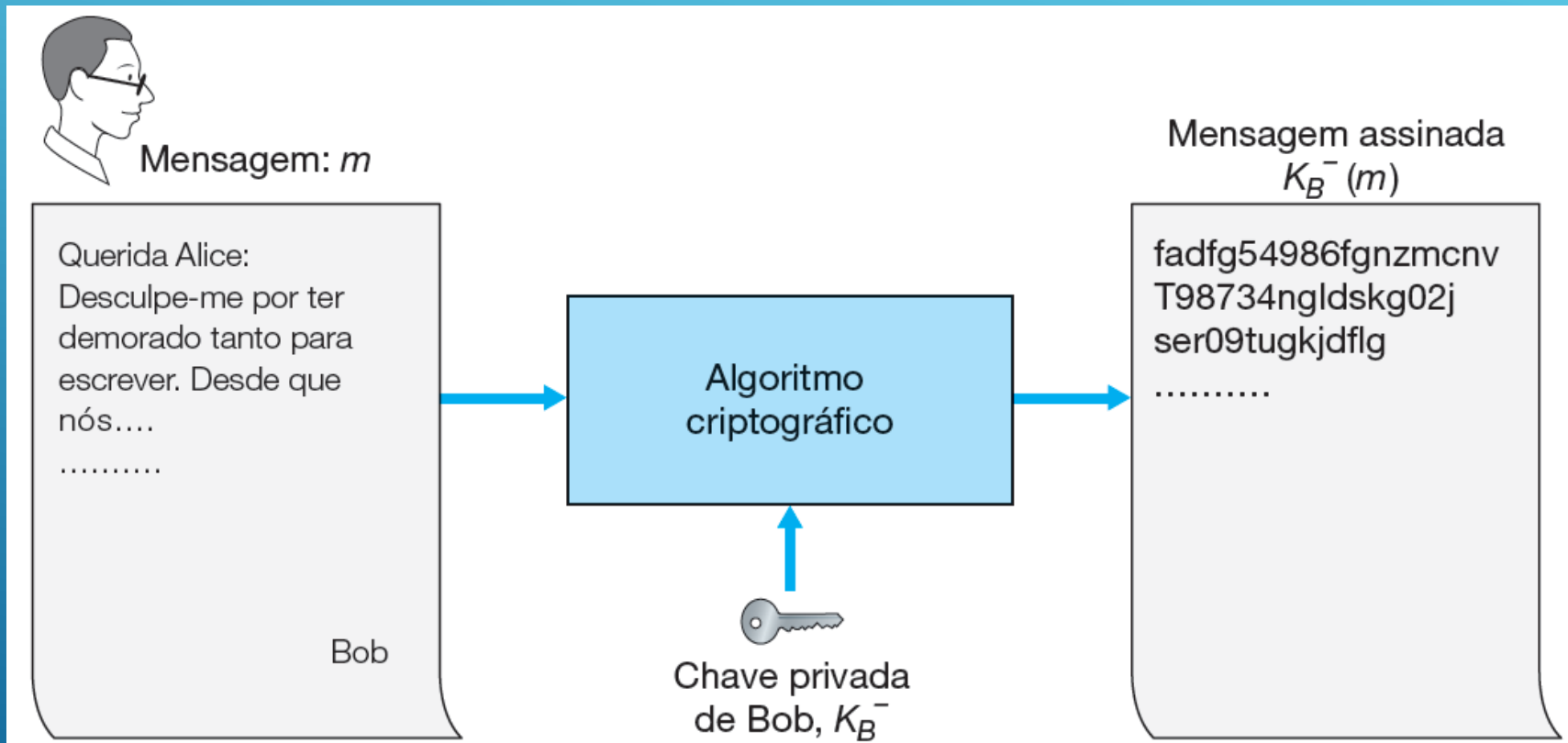
# ASSINATURA DIGITAL

- Representação simplificada dos elementos essenciais do processo de assinatura digital:



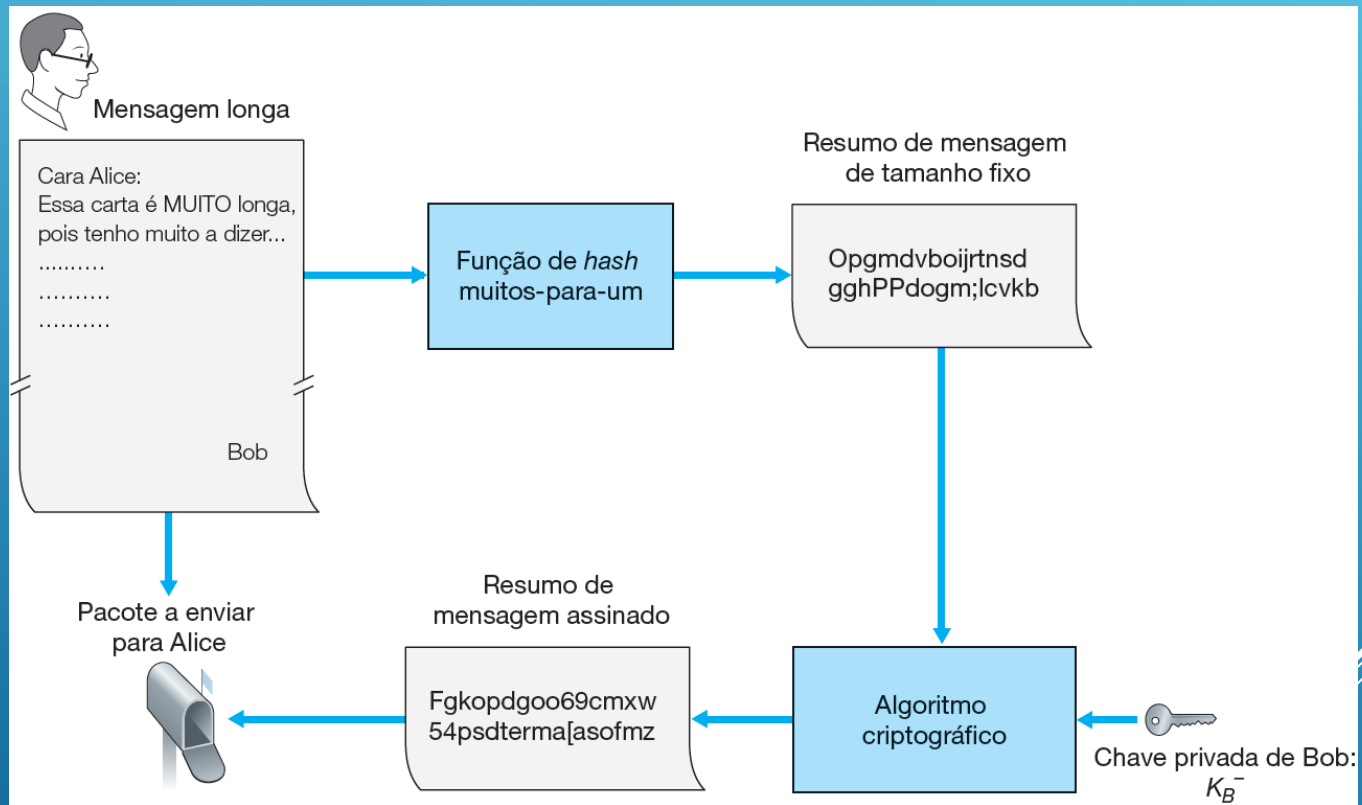
# ASSINATURA DIGITAL

- Criando uma assinatura digital para um documento



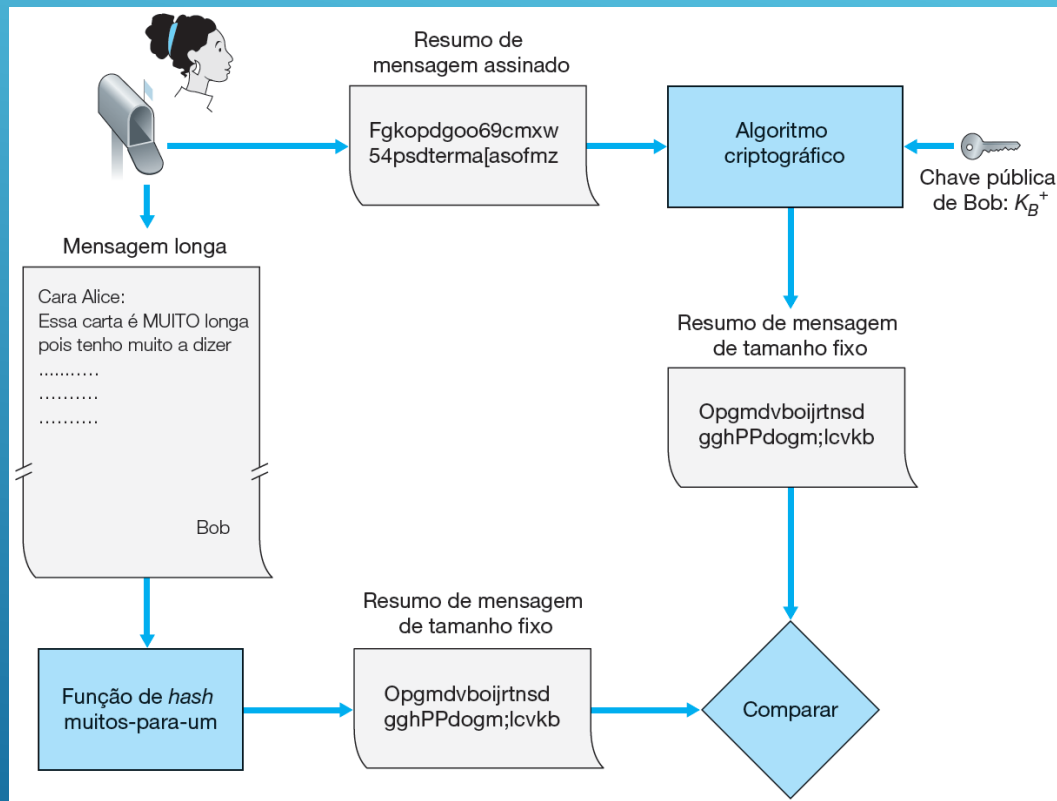
# ASSINATURA DIGITAL

- Enviando uma mensagem assinada digitalmente



# ASSINATURA DIGITAL

## ■ Verificando uma mensagem assinada



# CRIPTOGRAFIA (ALGORITMO RSA)

## ■ Geração de chaves:

1. Encontre dois números primos grandes  $p$ ,  $q$ .  
(ex., 1024 bits cada um)
2. Calcule  $n = pq$ ,  $z = (p-1)(q-1)$
3. Escolha  $e$  (com  $e < n$ ) que não tem fatores primos em comum com  $z$ . ( $e$ ,  $z$  são “primos entre si”).
4. Escolha  $d$  tal que  $ed-1$  é exatamente divisível por  $z$ .  
(em outras palavras:  $ed \bmod z = 1$  ).
5. Chave *Pública* é  $(n, e)$ . Chave *Privada* é  $(n, d)$ .

# CRIPTOGRAFIA (ALGORITMO RSA)

0. Dado  $(n,e)$  e  $(n,d)$  como calculados antes

1. Para criptografar o padrão de bits,  $m$ , calcule

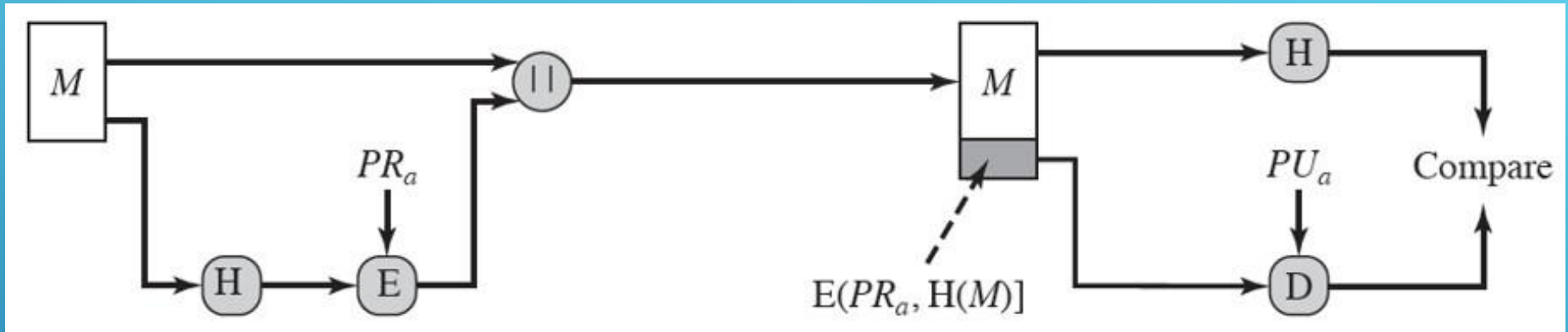
$$c = m^e \bmod n \quad (\text{i.e., resto quando } m^e \text{ é dividido por } n)$$

2. Para decriptografar o padrão de bits recebidos,  $c$ ,  
calcule

$$m = c^d \bmod n \quad (\text{i.e., resto quando } c^d \text{ é dividido } n)$$



# ASSINATURA DIGITAL (ALGORITMO RSA)



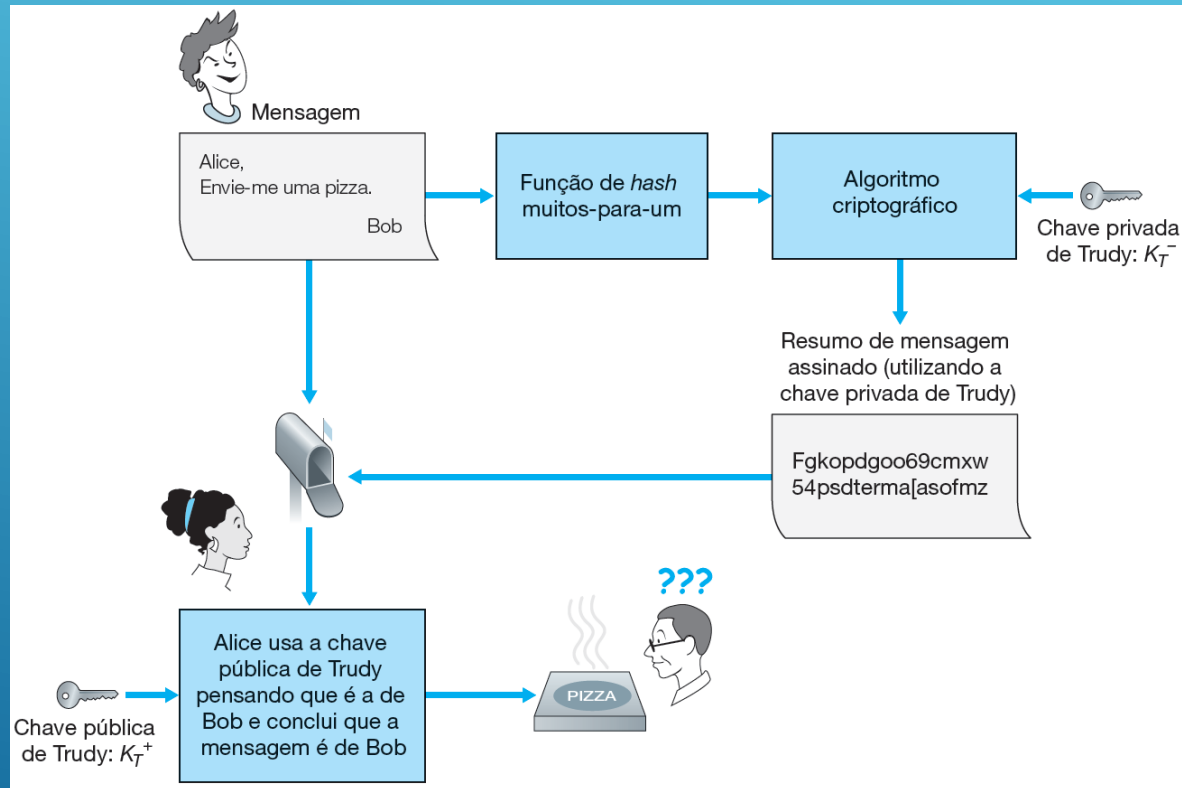
- Quer-se assinar uma mensagem  $m$ . A assinatura  $s$  será:
  - $s = m^d \bmod n$
- Para verificar a assinatura, faz-se:
  - $m' = s^e \bmod n$
- Se  $m=m'$  então a assinatura  $s$  deve ser considerada válida. Para um inimigo forjar uma assinatura, é necessário saber o valor de  $d$ . Isso é equivalente a quebrar o RSA (que por sua vez é tão difícil quanto fatorar  $n$ ).

# ASSINATURA DIGITAL

- Uma aplicação importante de assinaturas digitais é a **certificação de chaves públicas**.
- A vinculação de uma chave pública a uma entidade particular é feita, em geral, por uma **Autoridade Certificadora (CA)**, cuja tarefa é validar identidades e emitir certificados.
- Tão logo verifique a identidade da entidade, a CA cria um certificado que vincula a chave pública da entidade à identidade verificada.

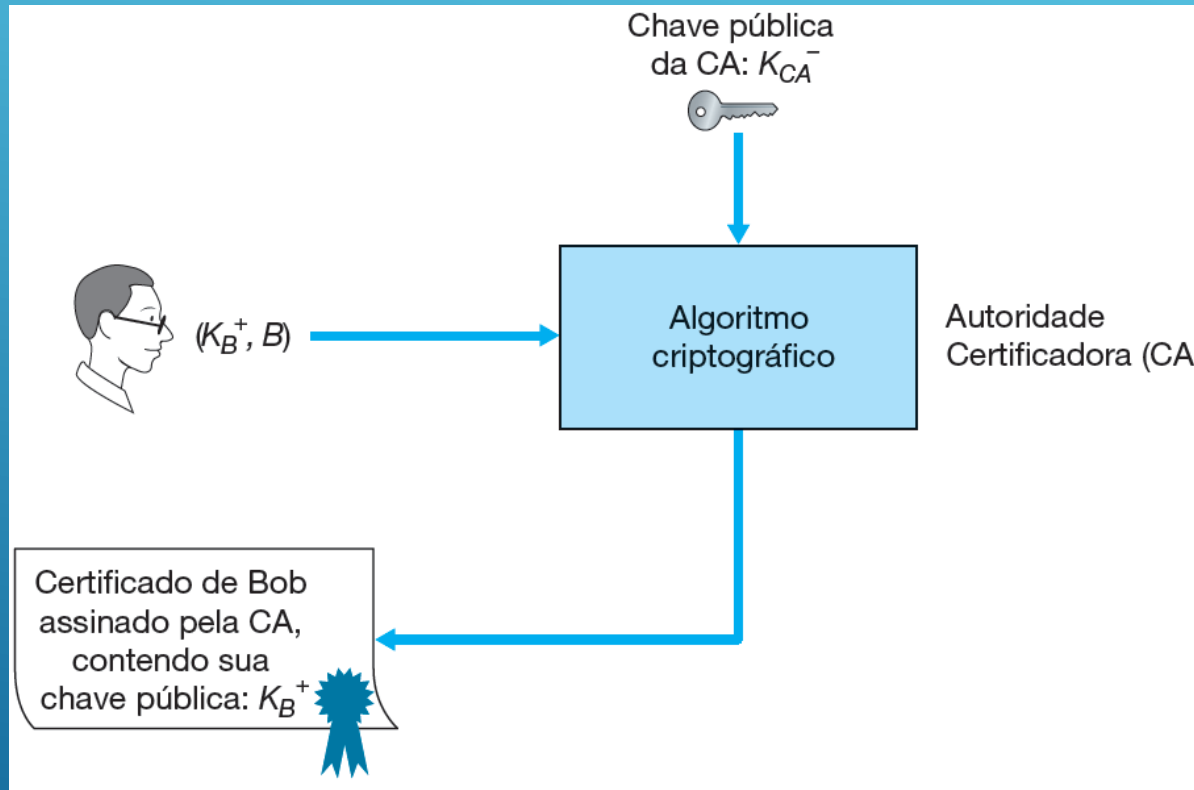
# ASSINATURA DIGITAL

- Trudy se passa por Bob usando criptografia de chaves públicas



# ASSINATURA DIGITAL

- Bob obtém sua chave pública certificada pela CA



# CERTIFICADO DIGITAL

- O **Certificado Digital** é a identidade digital da pessoa física e jurídica no meio eletrônico. Ele garante **autenticidade, confidencialidade, integridade** e **não repúdio** nas operações que são realizadas por meio dele, atribuindo validade jurídica.

**Existem 2 tipos de Certificado Digital:**

**Certificado A1** - é emitido e armazenado no **computador** ou no **dispositivo móvel** (smartphone ou tablet). Tem validade de 1 ano.



**Certificado A3** - é emitido e armazenado em mídia criptográfica (**Cartão, Token ou Nuvem**). Tem validade de 1 a 5 anos.



# CERTIFICADO DIGITAL

## ■ Aplicações:



Para Pessoas Físicas e Jurídicas



Para Servidores/Sites



Certificado Digital  
e-CPF



Certificado Digital  
e-CNPJ



Certificado Digital  
NF-e | NFC-e



Certificado Digital  
OAB



Certificado Digital  
para celular: mobileID



Certificado Digital na  
nuvem: remotedID



Certificado SSL

# CERTIFICADO DIGITAL

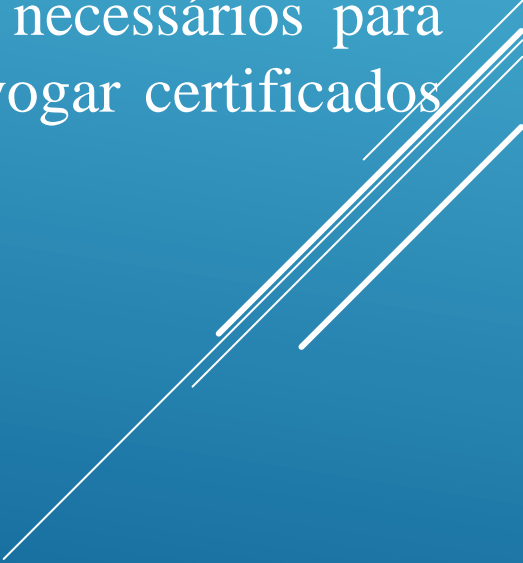
## ■ Aplicações:

- Governo Federal (ComprasNet, sistemas de diárias e passagens, INPI, receita federal, Siscomex, nota fiscal eletrônica)
- Governo estadual e municipal (Semasa, Eletropaulo, Detran)
- Sistema jurídico (STJ, diário da justiça on-line, cartório eletrônico)
- Outras iniciativas (carteiras de identidade profissionais, e-mail, micro e pequenas empresas).

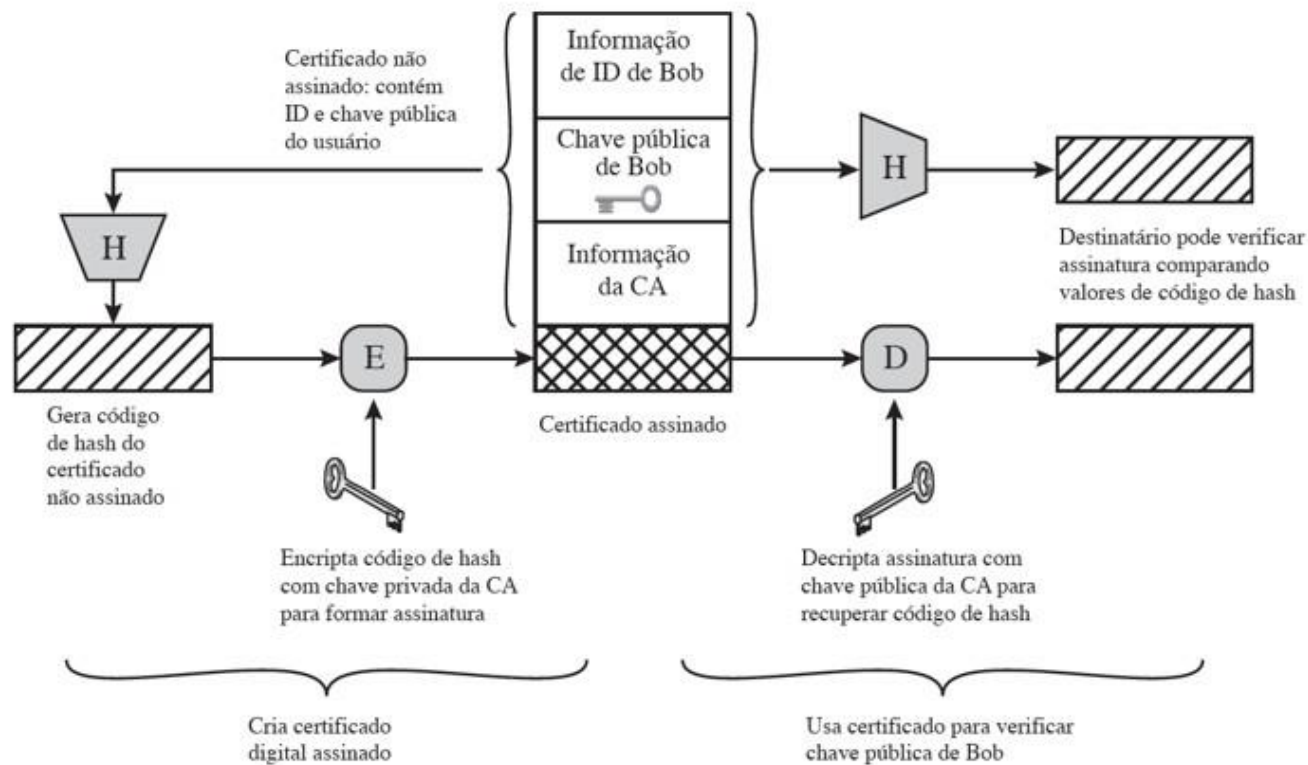




# CERTIFICADO DIGITAL

- Certificado digital deve seguir uma estrutura padrão para que qualquer entidade pode ler e entender, independentemente do emitente.
  - O X.509 é o padrão para a construção de certificados digitais para infra-estrutura de chave pública (PKI) usada para gerenciar certificados digitais.
  - PKI são as políticas, funções e procedimentos necessários para criar, gerenciar, distribuir, usar, armazenar e revogar certificados digitais.
- 

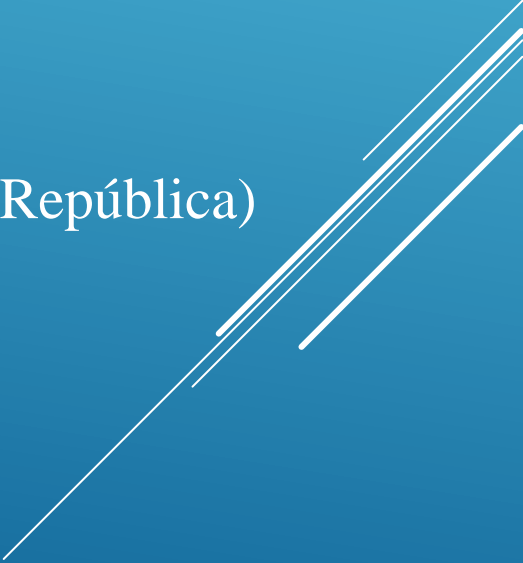
# USO DO CERTIFICADO DE CHAVE PÚBLICA (X.509)



# AUTORIDADES CERTIFICADORAS

- Para que possa ser aceito e utilizado por pessoas, empresas e governos, os certificados digitais precisam ser emitidos por entidades apropriadas. Sendo assim, o primeiro passo é procurar uma *Autoridade Certificadora* (AC) ou uma *Autoridade de Registro* (AR) para obter um certificado digital.
- Uma AC tem a função de associar uma identidade a uma chave e "inserir" esses dados em um certificado digital. Para tanto, o solicitante deve fornecer documentos que comprovem sua identificação. Já uma AR tem uma função intermediária, já ela pode solicitar certificados digitais a uma AC, mas não pode emitir esse documento diretamente.

# AUTORIDADES CERTIFICADORAS

- A ICP-Brasil (Infra-estrutura de Chaves Públicas) possuem nove ACs credenciadas:
    - Serpro
    - CEF
    - Serasa
    - Receita federal
    - Certisign
    - Imprensa Oficial
    - AC-JUS (Autoridade Certificadora da Justiça)
    - ACPR (Autoridade Certificadora da Presidência da República)
    - Casa da Moeda do Brasil
- 
- Several white lines of varying lengths and angles are drawn in the bottom right corner of the slide, creating a modern, abstract graphic element.

# AUTORIDADES CERTIFICADORAS

- São essas instituições que devem ser procuradas por quem deseja obter certificado digital legalmente reconhecido no Brasil. Note que cada uma dessas entidades pode ter critérios distintos para a emissão de certificados, o que inclusive resulta em preços diferentes, portanto, é conveniente ao interessado saber qual AC é mais adequada às suas atividades. Essas entidades podem ter ACs "secundárias" ou ARs ligadas a elas.



# AUTORIDADES CERTIFICADORAS

## ■ Aplicações:



Para Pessoas Físicas e Jurídicas



Para Servidores/Sites



Certificado Digital  
e-CPF



Certificado Digital  
e-CNPJ



Certificado Digital  
NF-e | NFC-e



Certificado Digital  
OAB



Certificado Digital  
para celular: mobileID



Certificado Digital na  
nuvem: remoteID



Certificado SSL

# AUTORIDADES CERTIFICADORAS

## ■ Aplicações:

- Governo Federal (ComprasNet, sistemas de diárias e passagens, INPI, receita federal, Siscomex, nota fiscal eletrônica)
- Governo estadual e municipal (Semasa, Eletropaulo, Detran)
- Sistema jurídico (STJ, diário da justiça on-line, cartório eletrônico)
- Outras iniciativas (carteiras de identidade profissionais, e-mail, micro e pequenas empresas).



# BIBLIOGRAFIA

## ■ Bibliografia:

- STALLINGS, W. Criptografia e Segurança de Redes - Princípios e Práticas - 6ed., Pearson, 2015.
- KUROSE, James F; ROSS, Keith W. Redes de computadores e a internet: uma abordagem Top-Down. 6. ed. São Paulo: Pearson, c2014.
- ITI. Instituto Nacional de Tecnologia da Informação. <<http://www.iti.gov.br/icp-brasil>>. Acesso em: 16.08.2024.
- Notas de Aula