

# **Blockchain, Criptomoedas & Tecnologias Descentralizadas**

## **Criptografia assimétrica: Assinaturas digitais & distribuição de chaves**

**Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo**

# Objetivos

- Visão geral sobre mecanismos criptográficos assimétricos
  - Confidencialidade: **cifras assimétricas**
  - Integridade + Autenticidade + Irretratabilidade: **assinaturas digitais**

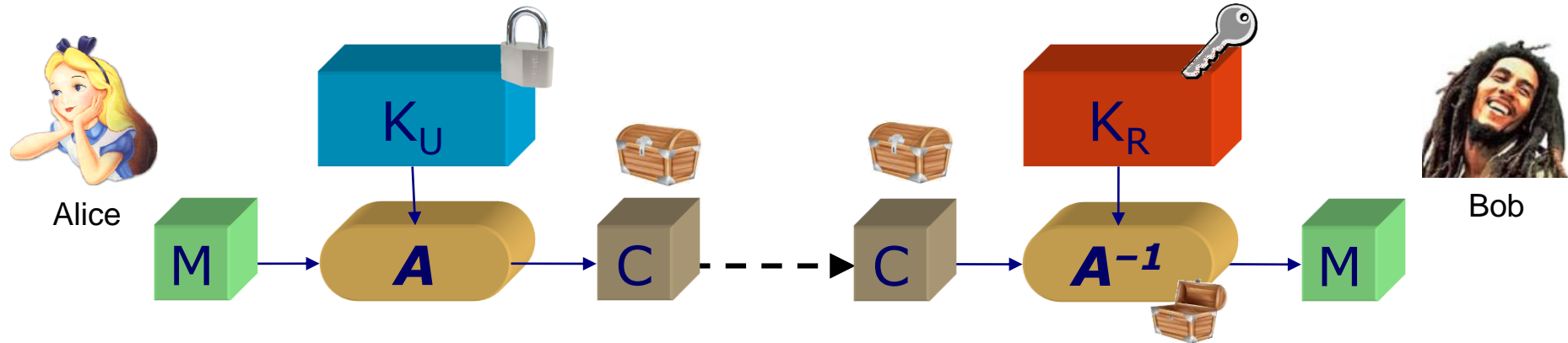
# Criptografia Assimétrica

- Duas chaves distintas
  - Chave **pública**  $K_U$ : divulgada abertamente
    - Analogia com o mundo real: um cadeado
  - Chave **privada**  $K_R$ : conhecida apenas pelo seu dono
    - Analogia com o mundo real: a chave do cadeado
  - Transformações **feitas usando uma chave** somente podem ser **invertidas com a outra chave**.
- Ambas as chaves são **geradas pelo seu dono**
  - Em um algoritmo seguro, deve ser inviável calcular a chave privada a partir da chave pública.
  - Para que **Alice** possa se comunicar com **Bob**, ambos devem obter, de alguma forma, a chave pública do outro.



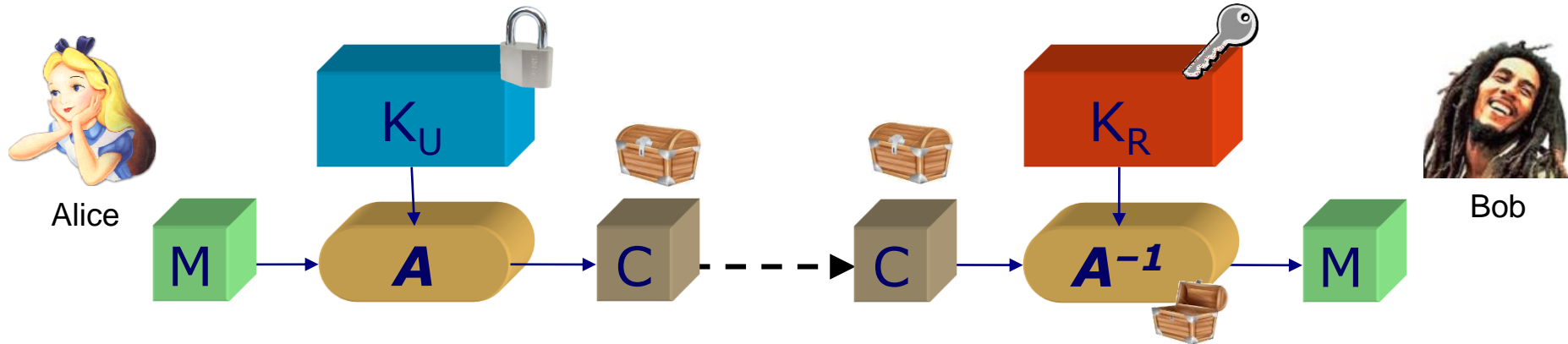
# Criptografia Assimétrica

- Usar chave pública do destinatário: qual serviço?



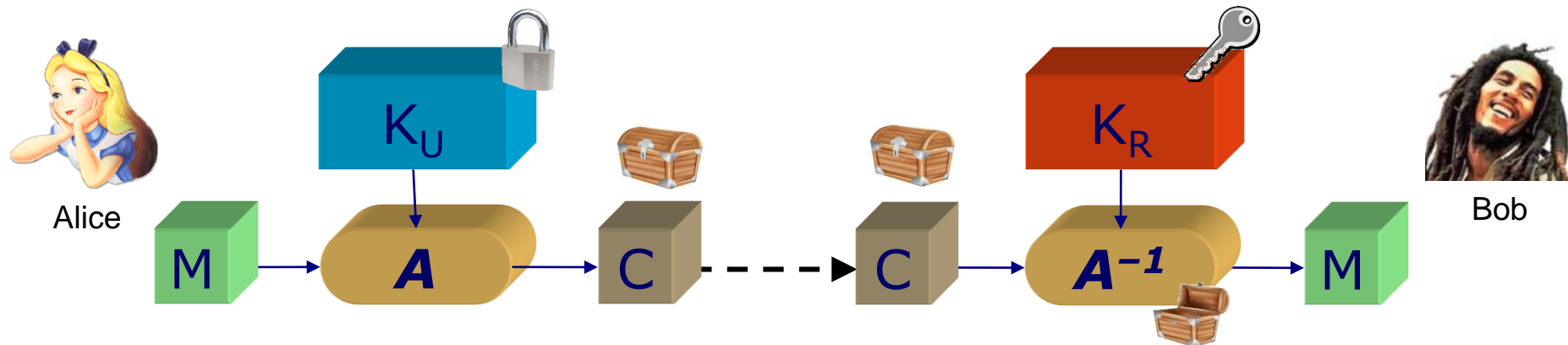
# Criptografia Assimétrica

- Cifração: confidencialidade

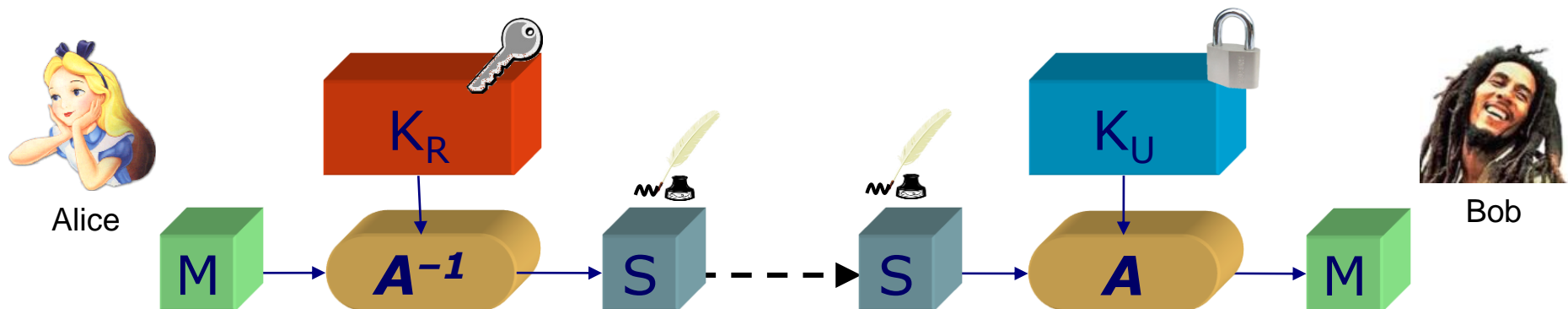


# Criptografia Assimétrica

- Cifração: confidencialidade

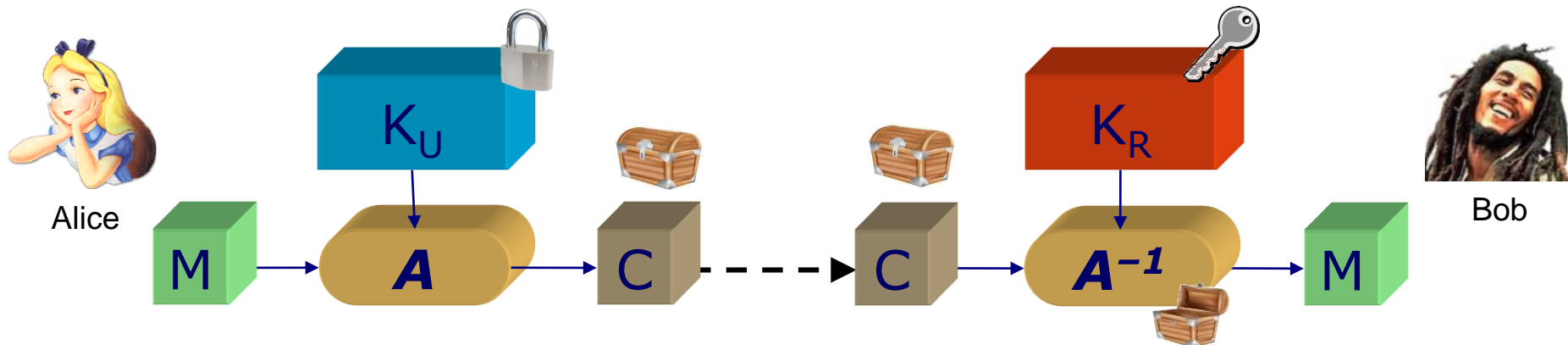


- Remetente usa sua chave privada: qual serviço?

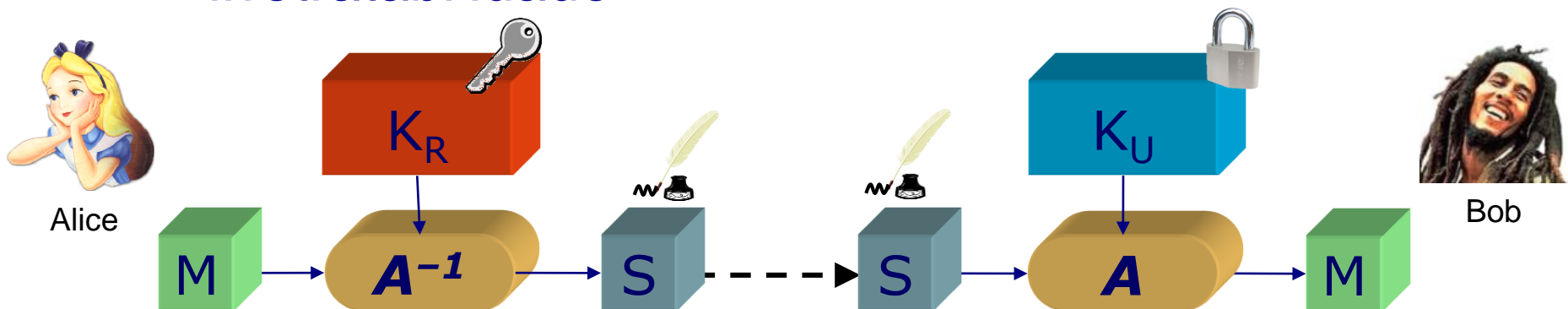


# Criptografia Assimétrica

- Cifração: confidencialidade

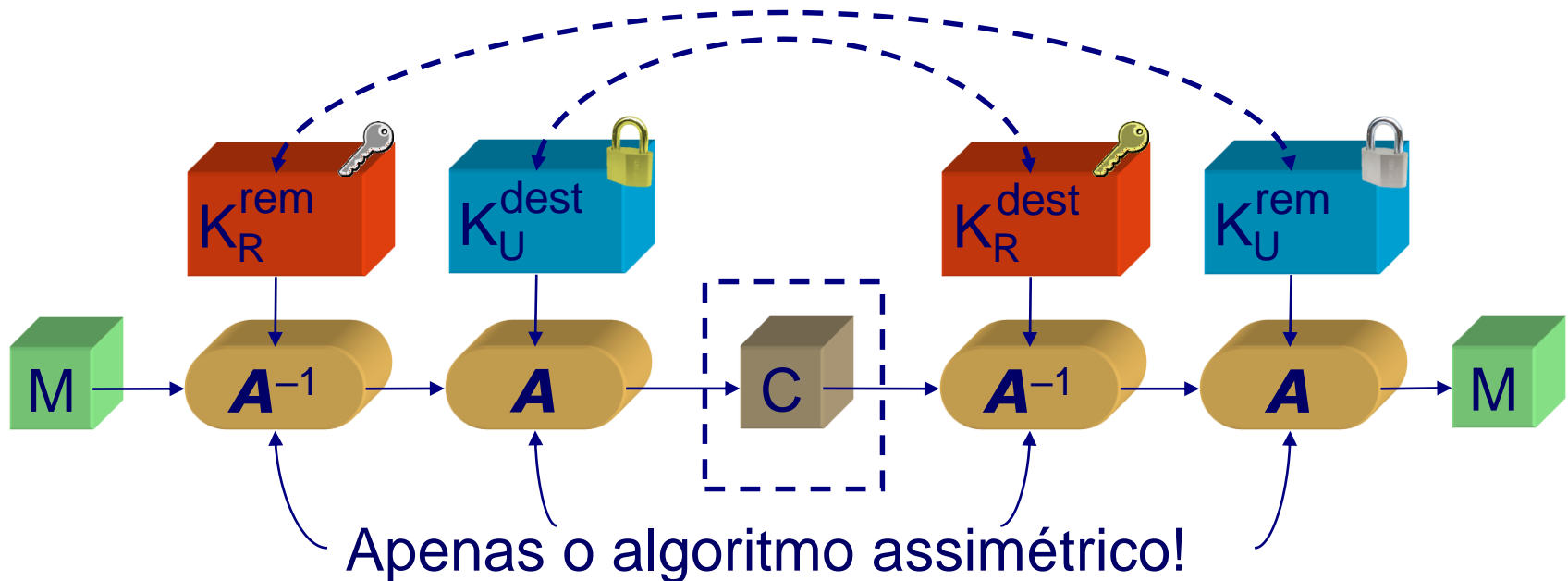


- Assinatura digital: integridade, autenticidade e irretratabilidade



# Envelope criptográfico assimétrico

- É possível obter confidencialidade, integridade, autenticidade e irretratabilidade aplicando-se apenas criptografia assimétrica sobre o conteúdo completo da mensagem.





# Criptografia assimétrica + simétrica

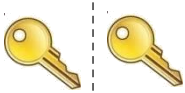
- Algoritmos **assimétricos** costumam ser **combinados com simétricos** por razões de **desempenho**:

- Algoritmos simétricos costumam ser ~1000 vezes mais rápidos do que assimétricos

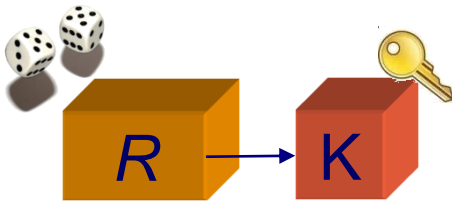
- Exemplos comuns:

- **Estabelecimento de chaves simétricas**: usadas por cifras simétricas e algoritmos de MAC

- **Assinatura digital do hash** da mensagem ao invés da mensagem em si: menor quantidade de dados processados pelo algoritmo assimétrico

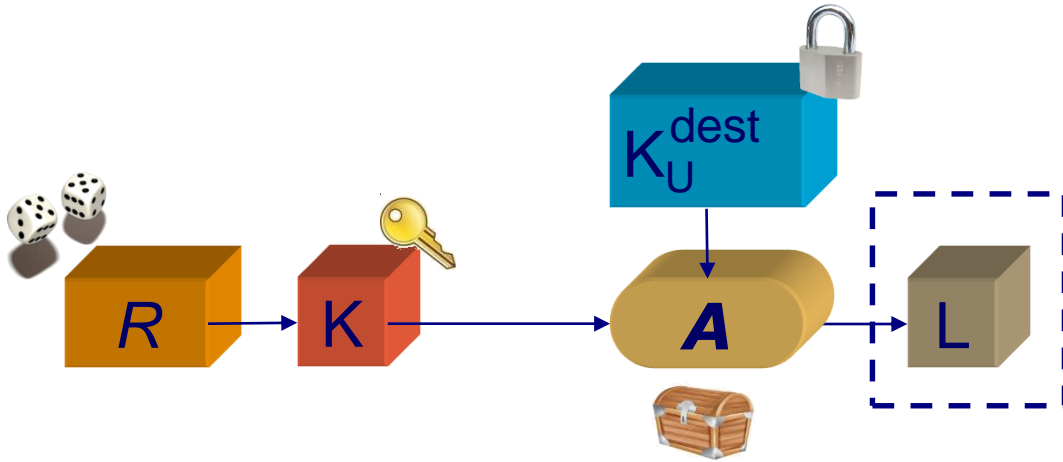


# Transmissão de chave simétrica



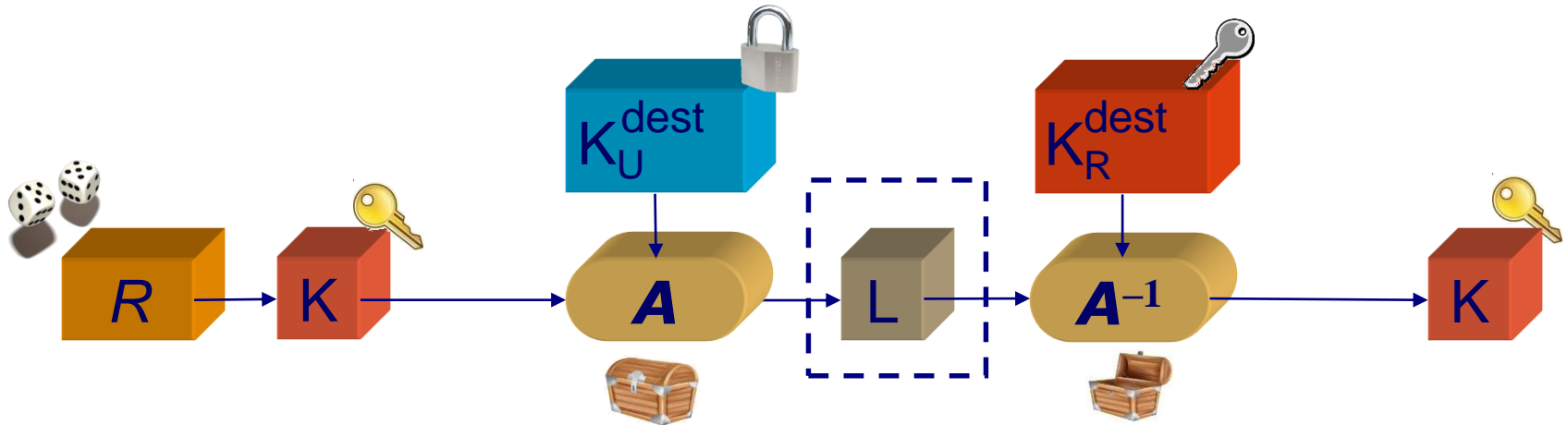
- ***Transmissão de chave*** simétrica  $K$ 
  - $R$ : número aleatório (fonte de entropia) gera chave  $K$

# Transmissão de chave simétrica



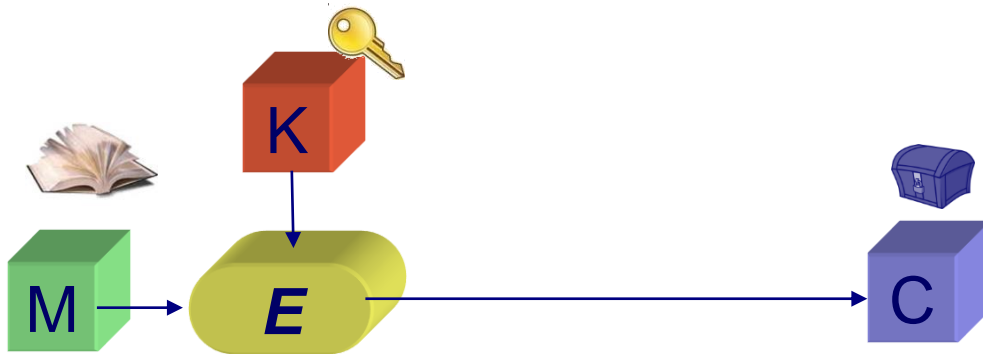
- **Transmissão de chave simétrica  $K$** 
  - $R$ : número aleatório (fonte de entropia) gera chave  $K$
  - $L$ : chave  $K$  protegida por chave pública do destinatário ( $K_U$ )
    - Enviado pela rede para o destinatário

# Transmissão de chave simétrica



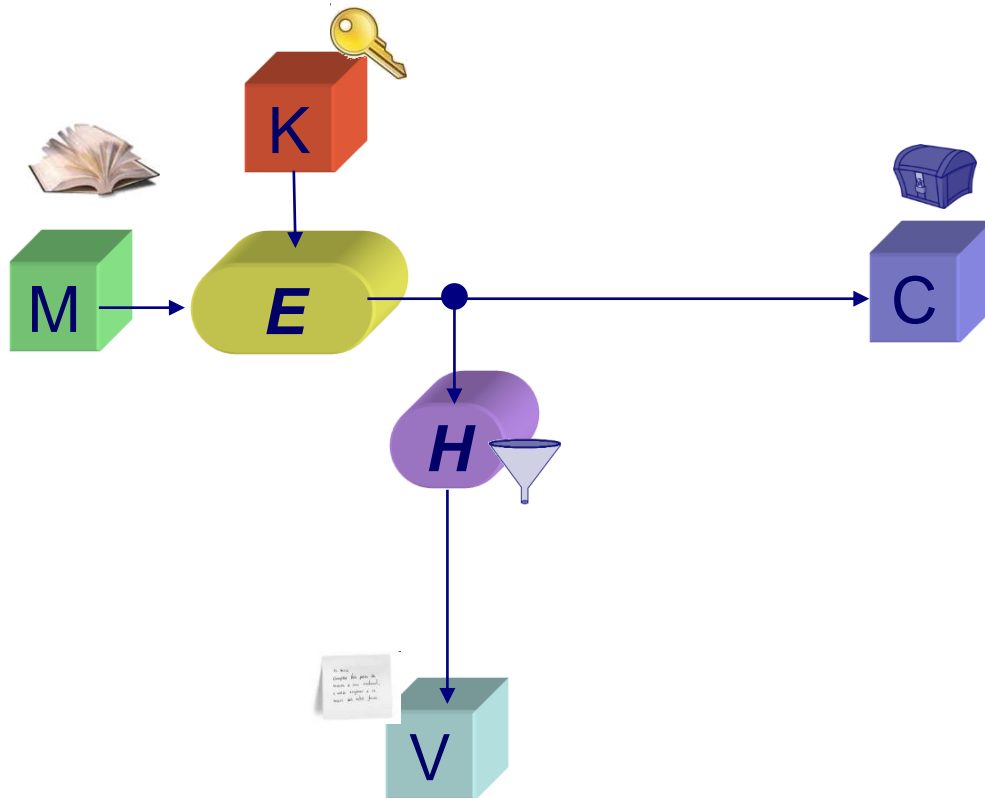
- **Transmissão de chave** simétrica  $K$ 
  - $R$ : número aleatório (fonte de entropia) gera chave  $K$
  - $L$ : chave  $K$  protegida por chave pública do destinatário ( $K_U$ )
    - Enviado pela rede para o destinatário
  - Apenas dono da chave  $K_R$  pode recuperar  $K$
- **Utilidade:** cifras simétricas são mais **eficientes**

# Envelope criptográfico



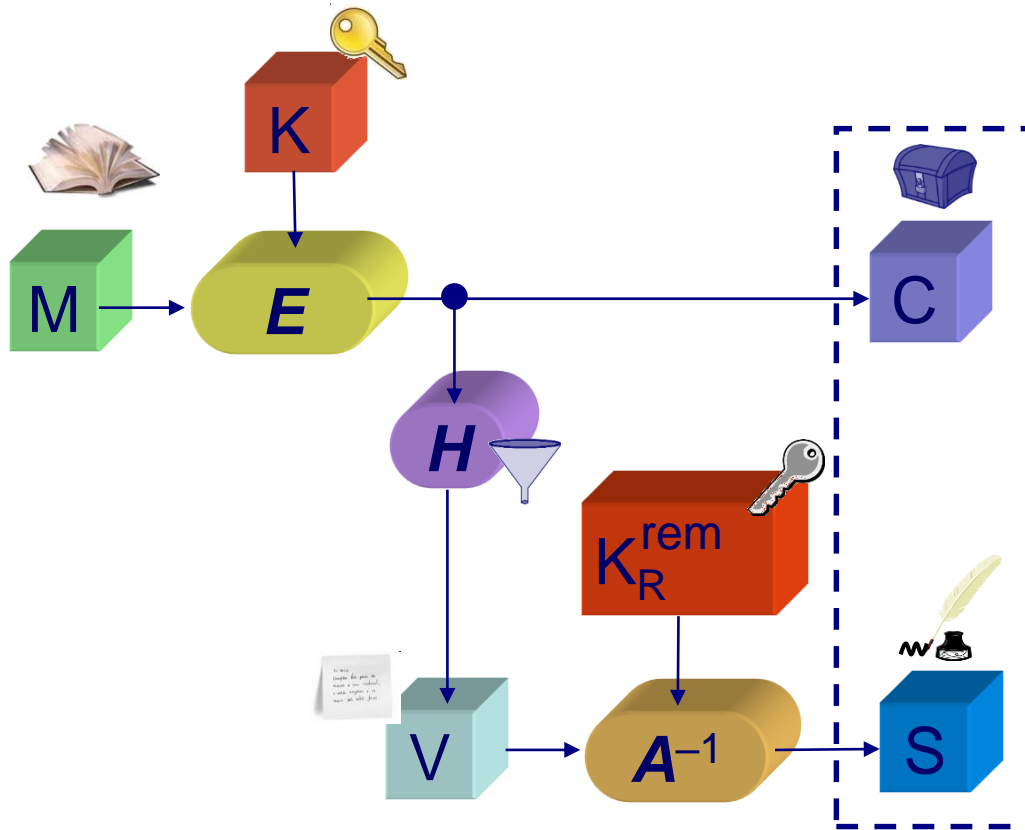
- Mensagem ***confidencial*** (C) e ***assinada*** (S)
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade:** mais eficiente assinar hash das mensagens

# Envelope criptográfico



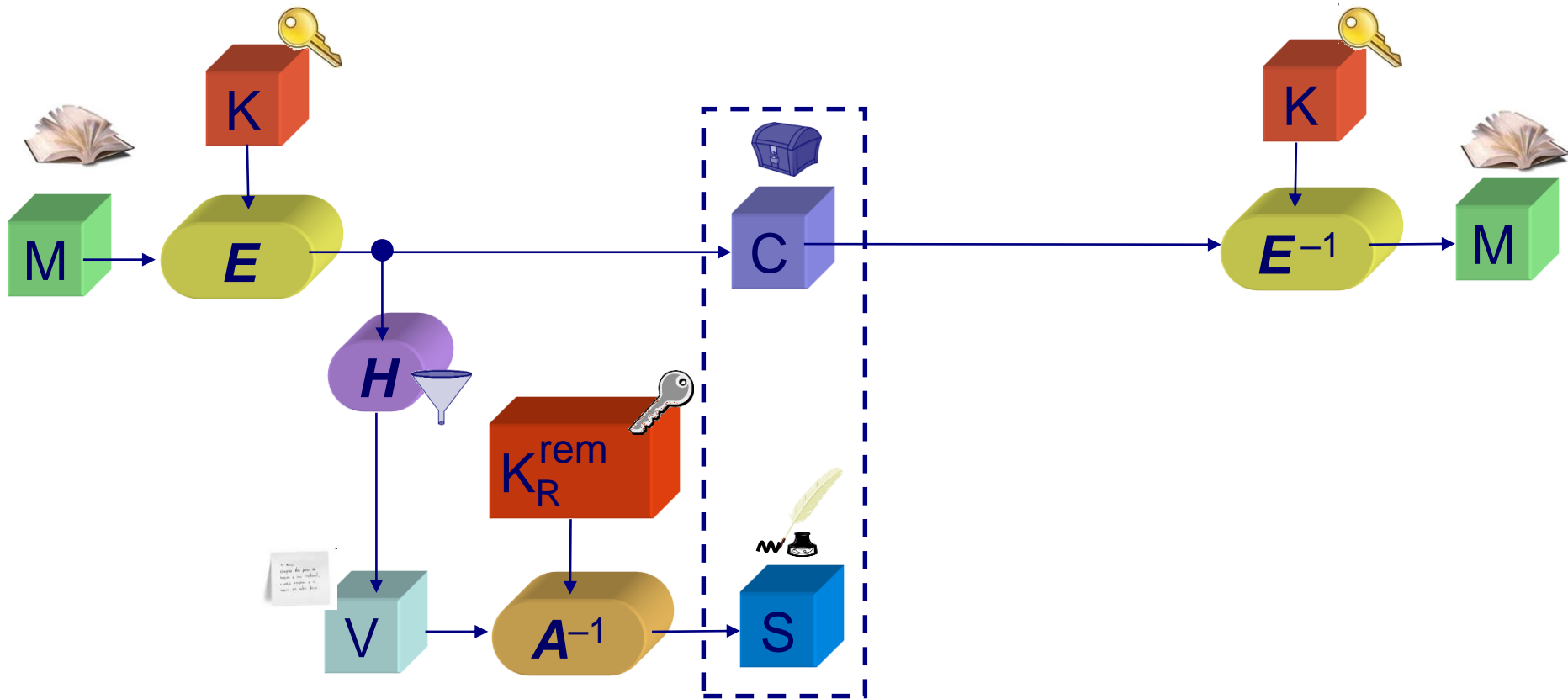
- Mensagem **confidencial** (C) e **assinada** (S)
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade**: mais eficiente assinar hash das mensagens

# Envelope criptográfico



- Mensagem **confidencial** ( $C$ ) e **assinada** ( $S$ )
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade:** mais eficiente assinar hash das mensagens

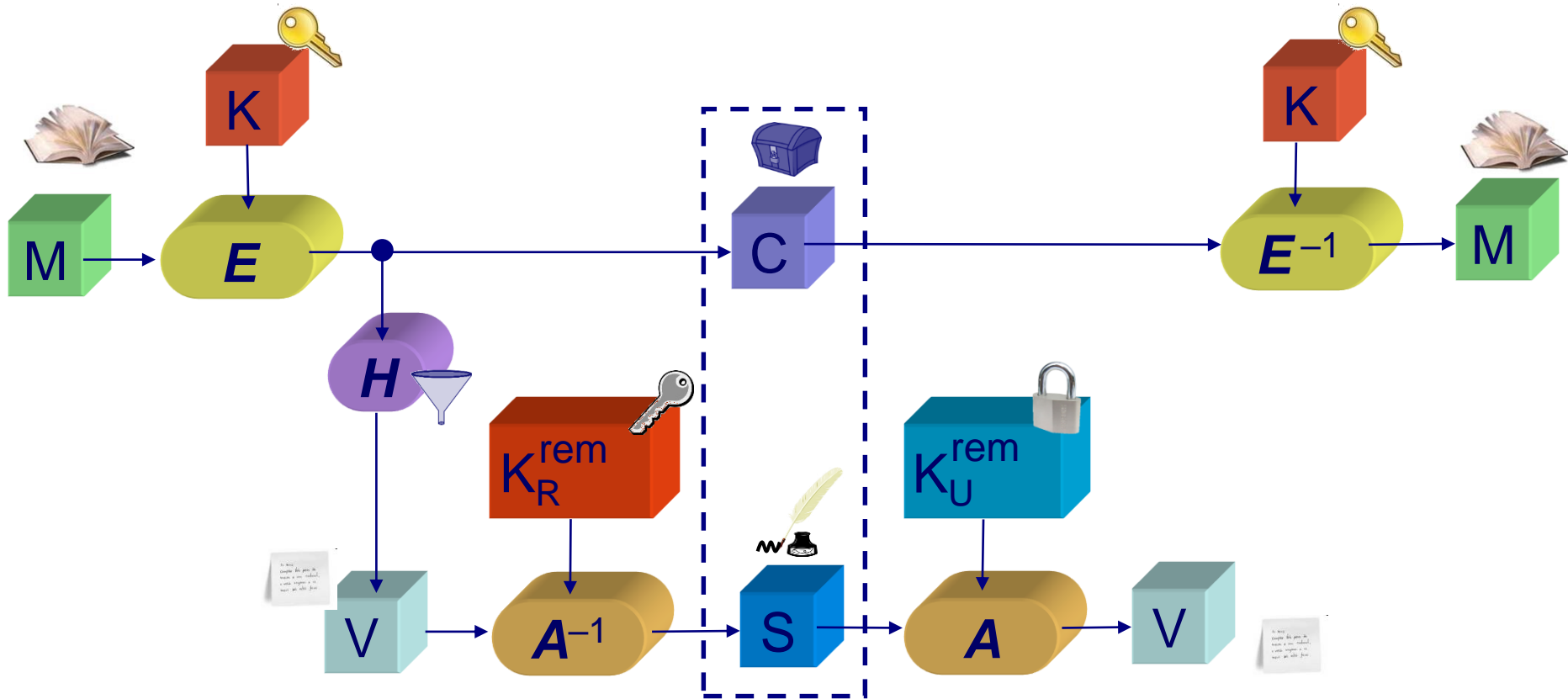
# Envelope criptográfico



- Mensagem **confidencial** (C) e **assinada** (S)
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade:** mais eficiente assinar hash das mensagens

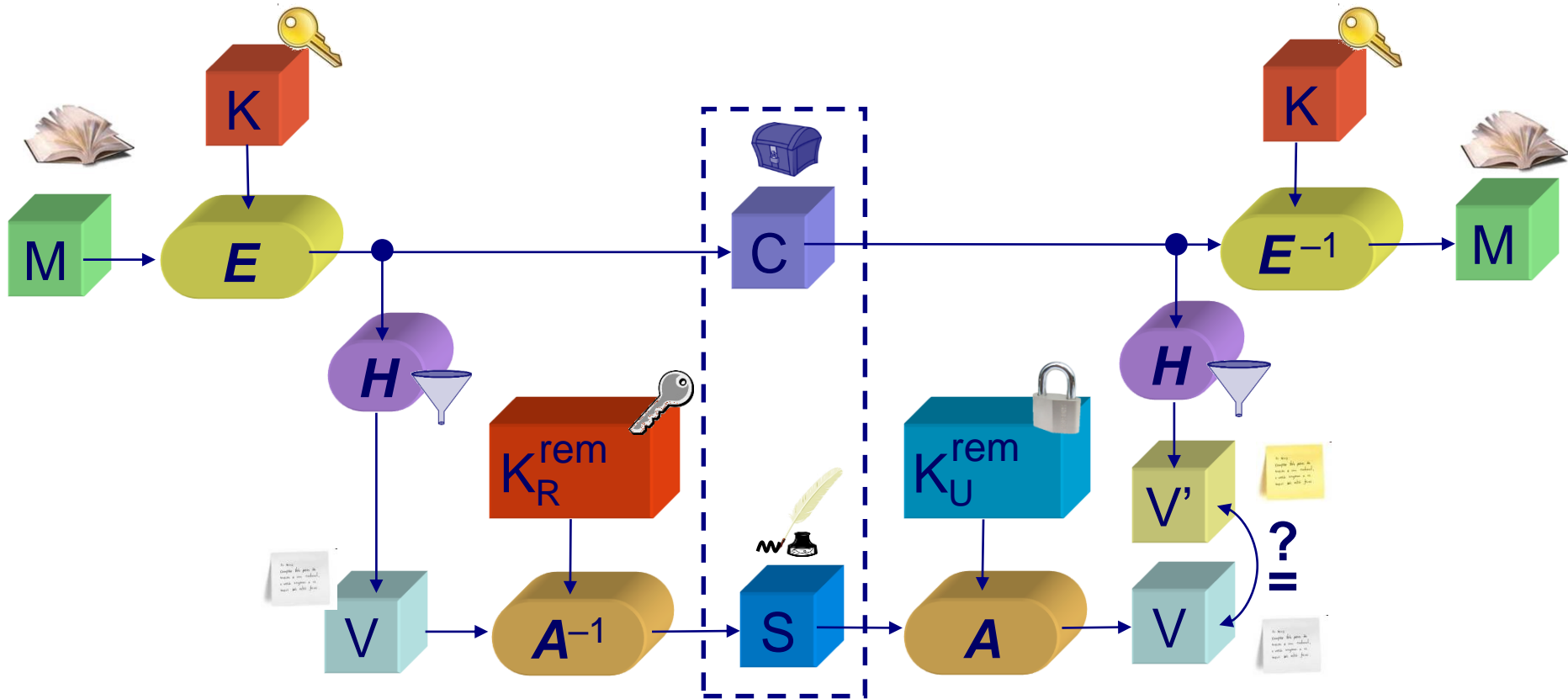


# Envelope criptográfico



- Mensagem **confidencial** ( $C$ ) e **assinada** ( $S$ )
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade:** mais eficiente assinar hash das mensagens


# Envelope criptográfico



- Mensagem **confidencial** ( $C$ ) e **assinada** ( $S$ )
  - Serviços: confidencialidade (cifra simétrica), integridade, autenticidade e irretratabilidade (assinatura digital)
- **Utilidade:** mais eficiente assinar hash das mensagens

# Funções de hash e assinaturas

- Assinaturas físicas: baixa segurança...

Conta: xxxx Banco: xx Agência: xxxx R\$ 10,00#	
Valor: # dez reais #	"Proteção de integridade"
Para: Sacanas Maximus	
 Data: 01/Janeiro/2022	"Autenticidade + Irretratabilidade"
Ser. 001 Assinatura: Marcos A. Simplicio Jr.	

- Assume que folhas de cheque sejam guardadas em local seguro...

# Funções de hash e assinaturas

- Assinaturas físicas: baixa segurança...



Conta: xxxx Banco: xx Agência: xxxx R\$ 10,00#

Valor: # dez reais # -----

Para: Sacanas Maximus

Data: 01/Janeiro/2022

Ser. 001 Assinatura: Marcos A. Simplicio Jr.

Conta: xxxx Banco: xx Agência: xxxx R\$ 250,11#

Valor: # duzentos e cinquenta reais e onze centavos#

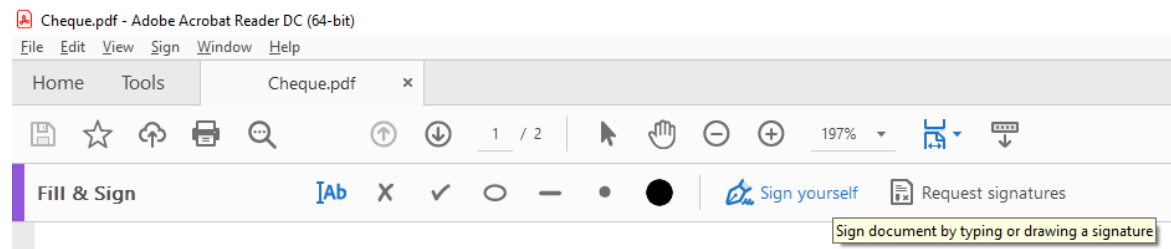
Para: Sacanas Maximus

Data: 01/Abril/2022

Ser. 002 Assinatura: Marcos A. Simplicio Jr.

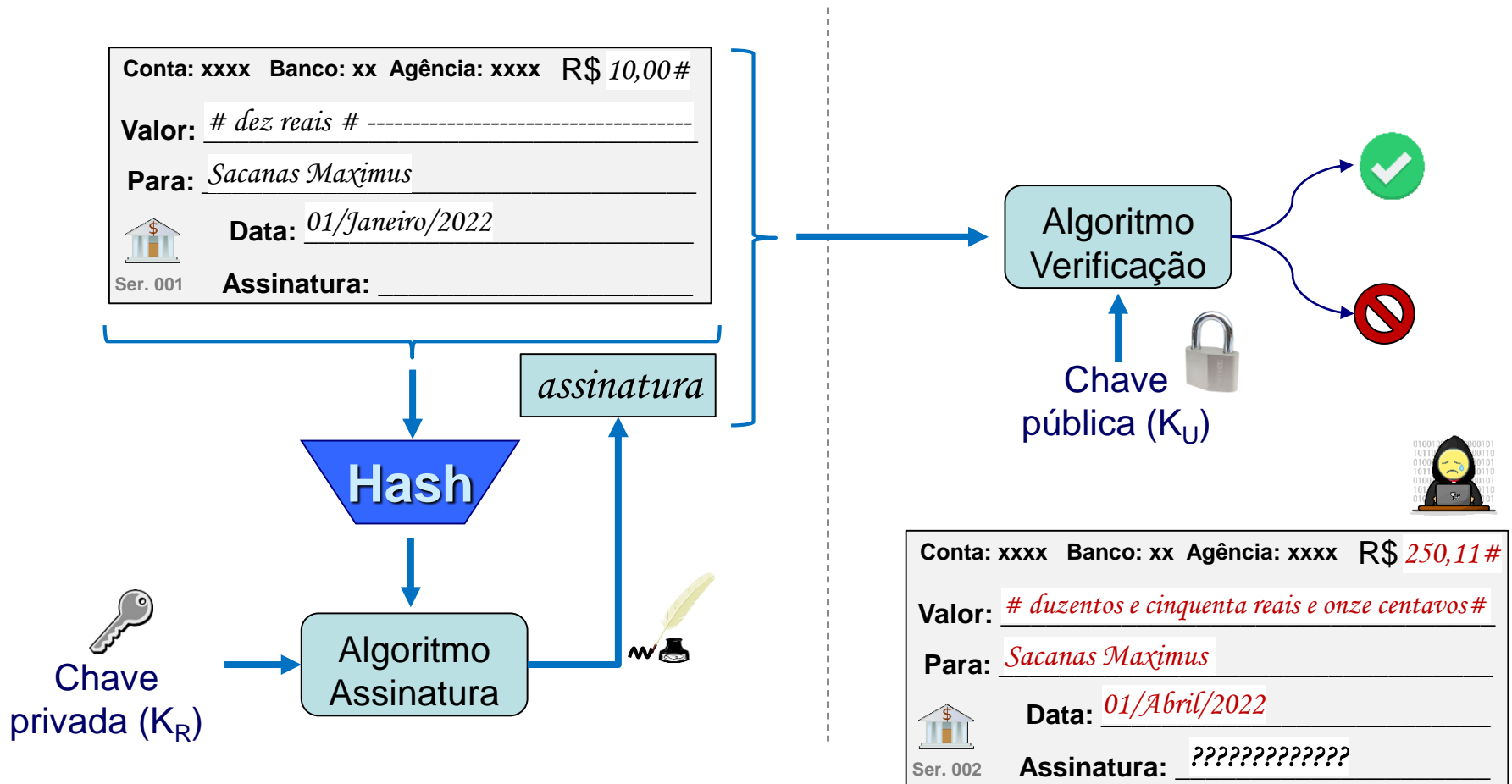
- Ou assinatura pode ser copiada
  - E cópia é muito fácil no mundo digital!

Ex: Adobe  
Acrobat Reader



# Funções de hash e assinaturas

- Assinatura digital: depende do documento completo!



# Esquemas Assimétricos: Exemplos

- **Encapsulamento de chaves** simétricas (KEM) / **cifração assimétrica**
  - Tradicionais: **Diffie-Hellman** clássico (**DH**) ou com curvas elípticas (**ECDH**), baseados em fatoração (**RSA**), ou logaritmos discreto elíptico (**ECIES**)
  - Pós-quânticos: baseados em reticulados (**CRYSTALS-KYBER**)
- **Assinatura digital**
  - Tradicionais: baseados em fatoração (**RSA**), ou logaritmo discreto (**DSA**) elíptico (**ECDSA**, **EdDSA**)
  - Pós-quânticos: baseados em reticulados (**FALCON**, **CRYSTALS-Dilithium**), ou hash (**SPHINCS+**)

# Esquemas Assimétricos:

## Exemplos

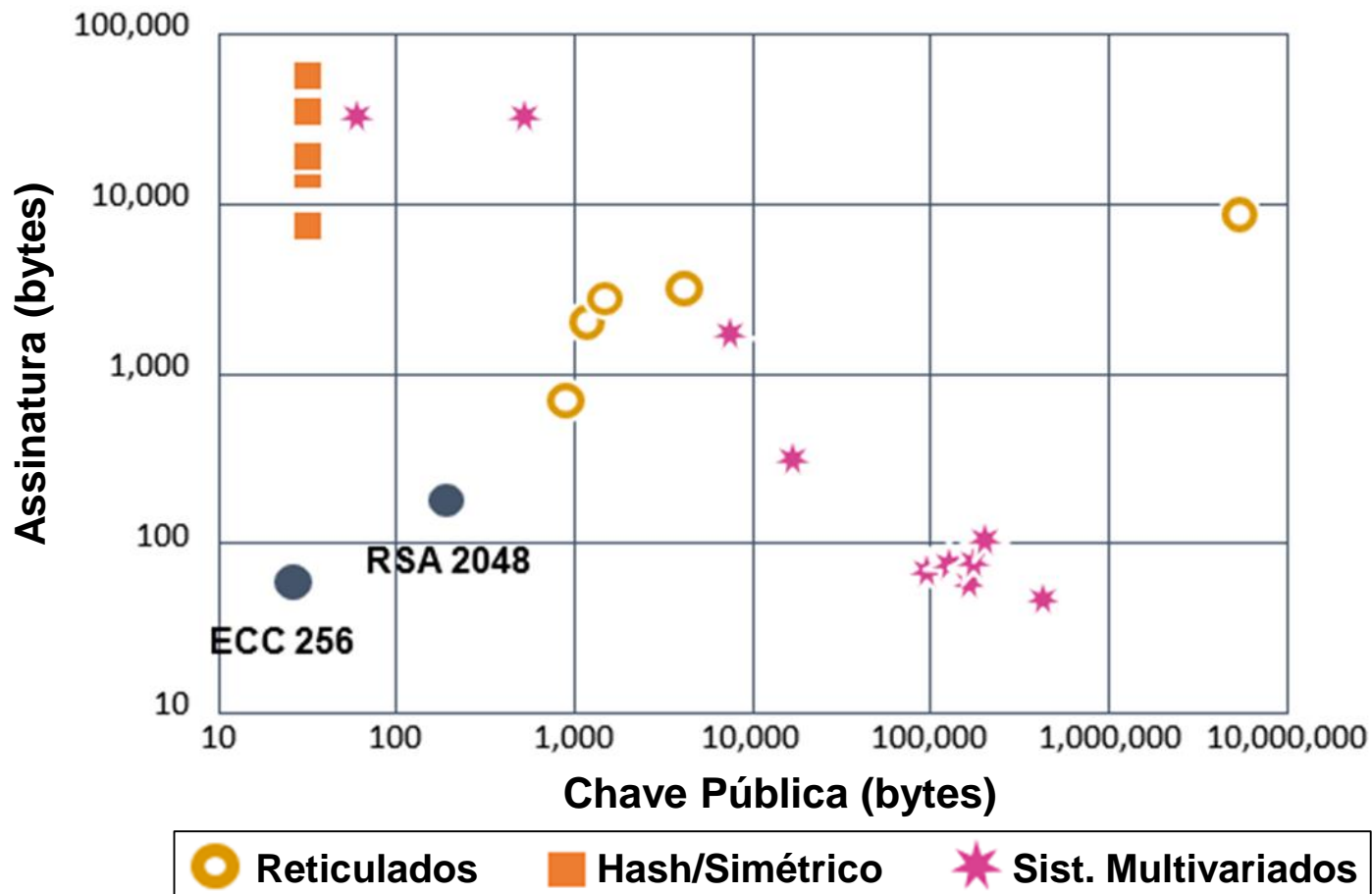
Nome	Uso	Chaves (128 bits)	Tamanhos
RSA	Assinatura ou KEM	3072	3072 (assinaturas ou dados cifrados*)
DH	KEM	3072	3072 (mensagens trocadas)
DSA	Assinatura	3072	512 (assinaturas)
ECDSA	Assinatura	256	512 (assinaturas)
EdDSA	Assinatura	256	512 (assinaturas)
ECIES	KEM	256	256 + 64** (dados cifrados*)

\* *Tamanho adicional ao da mensagem cifrada em si, usando cifra simétrica*

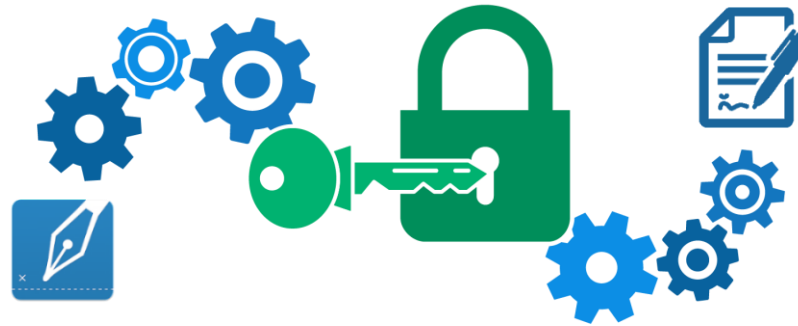
\*\* *ECIES usa MAC para calcular um tag de autenticação (64 bits ou maior)*

# Esquemas Assimétricos: Exemplos

- Visão geral: assinaturas clássicas vs. propostas pós-quânticas







# Blockchain, Criptomoedas & Tecnologias Descentralizadas

## Criptografia assimétrica: Assinaturas digitais & distribuição de chaves

Prof. Dr. Marcos A. Simplicio Jr. – [mjunior@larc.usp.br](mailto:mjunior@larc.usp.br)  
Escola Politécnica, Universidade de São Paulo

# Referências

- W. Stallings, L. Brown “Computer Security Principles and Practice – 2nd/3rd/4th edition”. Prentice-Hall, ISBN: 0-13-277506-9. 2011/2015/2018.
  - Em português: W. Stallings, L. Brown. “Segurança de Computadores - Princípios e Práticas” (2ª Ed), Elsevier, 2014
- W. Stallings: “Cryptography and Network Security” (6th/7th Ed.), Prentice-Hall 2013/2016.
  - Em português: W. Stallings: “Criptografia e Segurança de Redes” (6ª Ed.), Pearson-Prentice-Hall (2014).
- S. Wykes. Criptografia Essencial: A Jornada do Criptógrafo, 1a ed. Elsevier, 2016.
- A. Narayanan, J. Bonneau, E. Felten. "Bitcoin and Cryptocurrency Technologies: A Comprehensive Introduction". Princeton University Press, 2016. ISBN: 0691171696. Available:  
[https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton\\_bitcoin\\_book.pdf?a=1](https://d28rh4a8wq0iu5.cloudfront.net/bitcointech/readings/princeton_bitcoin_book.pdf?a=1)
- C. Adams, P. Cain, D. Pinkas, R. Zuccherato. RFC 3161: Internet X.509 Public Key Infrastructure - Time-Stamp Protocol (TSP). Internet Engineering Task Force, August 2001. URL: <https://datatracker.ietf.org/doc/html/rfc3161>