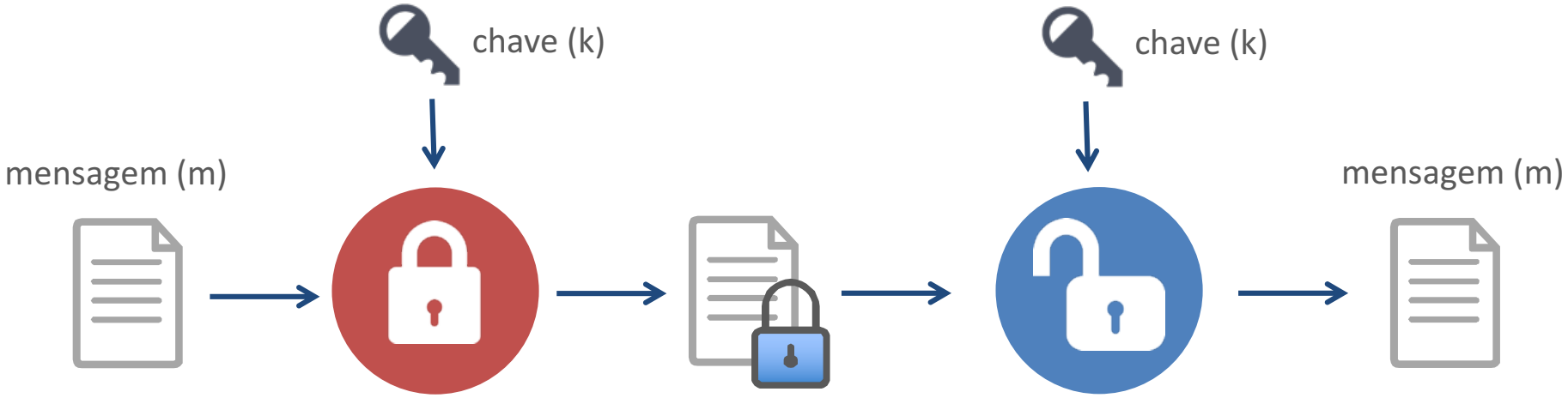
Criptografia

ALGORITMOS E ESTRUTURAS DE DADOS III

Prof. Marcos André S. Kutova

Criptografia

Do grego: *kryptós* (escondido) + *graphein* (escrita)



Cifragem (ou encriptação)

Transformação do documento
em algo incompreensível

c = E(k,m)

Decifragem (ou desencriptação)

Transformação do documento
cifrado em sua versão original

m = D(k,c)

Aplicações da criptografia

Confidencialidade

Manter as informações privadas

Integridade

Garantir que os dados não foram alterados

Autenticação

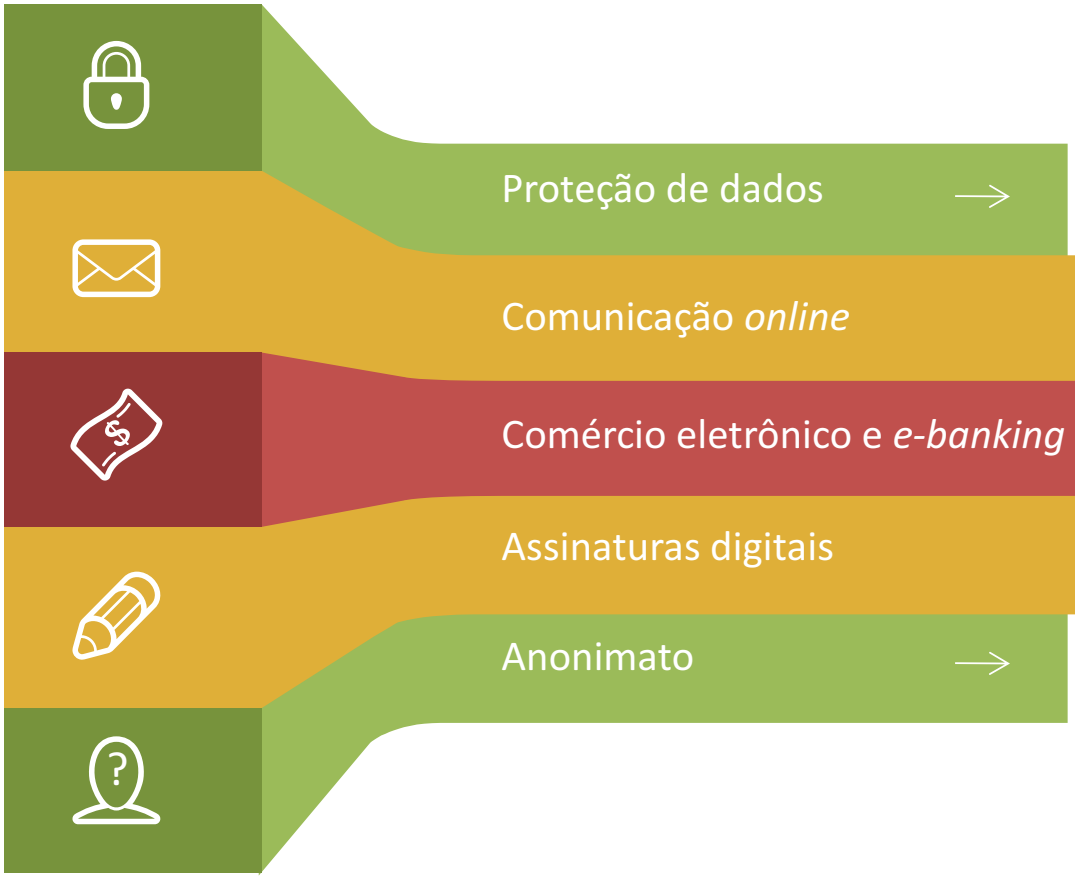
Estabelecer a identidade de um usuário ou sistema

Não-repúdio

Impedir que uma pessoa negue ter feito uma operação ou enviado uma mensagem

Os algoritmos criptográficos realizam uma ou mais operações, mas não todas. Assim, devem ser usados de forma combinada, se necessário.

Exemplos de aplicações



Proteção de dados → Sigilo de dados armazenados localmente ou em algum servidor na nuvem, com acesso controlado

Comunicação *online* → Troca de mensagens sigilosas, com autenticação das partes envolvidas

Comércio eletrônico e *e-banking* → Segurança para comprador e vendedor, inclusive nas operações bancárias

Assinaturas digitais → Formalização de operações e negócios realizados por meios eletrônicos

Anonimato → Garantia do direito de anonimato e sigilo em determinadas operações

Cifragem

Cifragem

Cifragem é o processo de conversão de um texto claro para um código cifrado.

Decifragem é o processo contrário, de recuperar o texto original a partir de um texto cifrado.

Cifragem

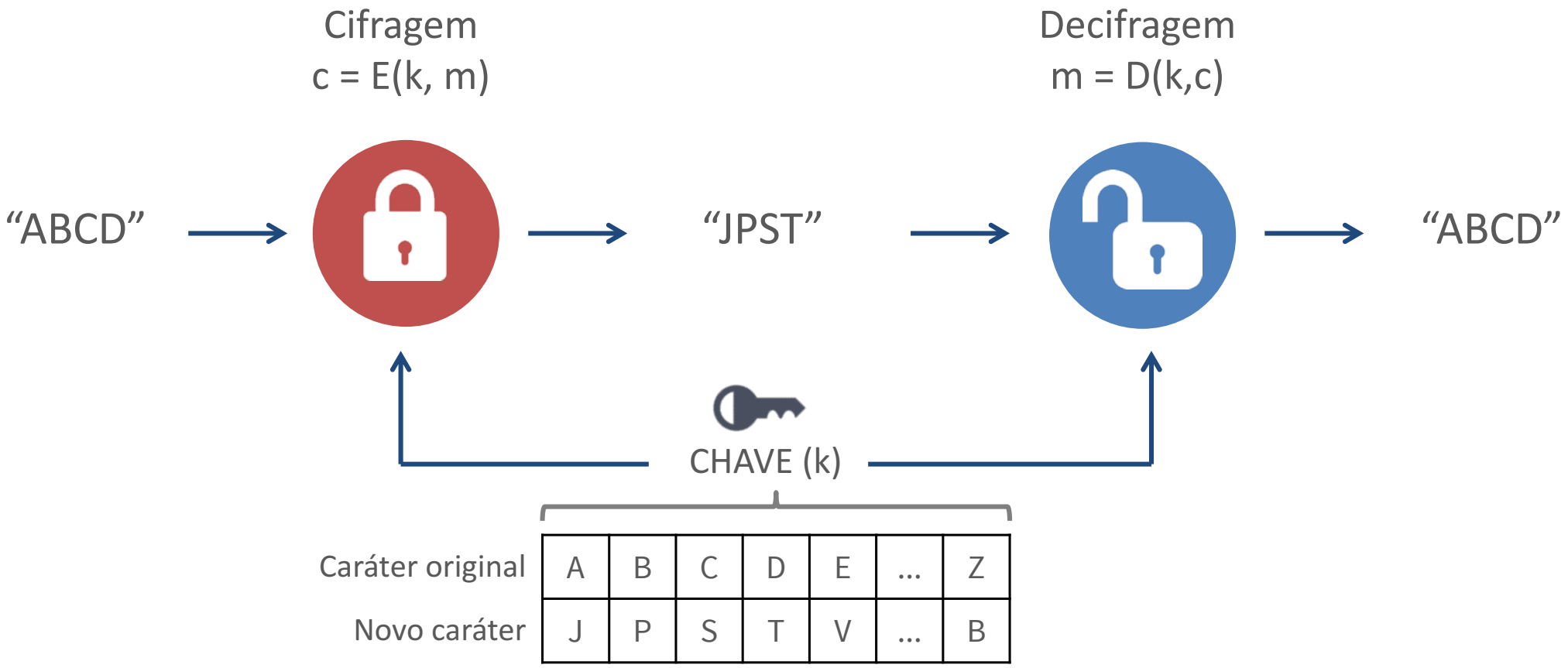
A cifra de substituição é um método de criptografia no qual os símbolos (letras, grupos de letras, números, ...) são substituídas por outros símbolos.

A **cifra de transposição** é um método de criptografia em que os símbolos são trocados de posição com outros símbolos.

Cifras de substituição

Cifras de substituição

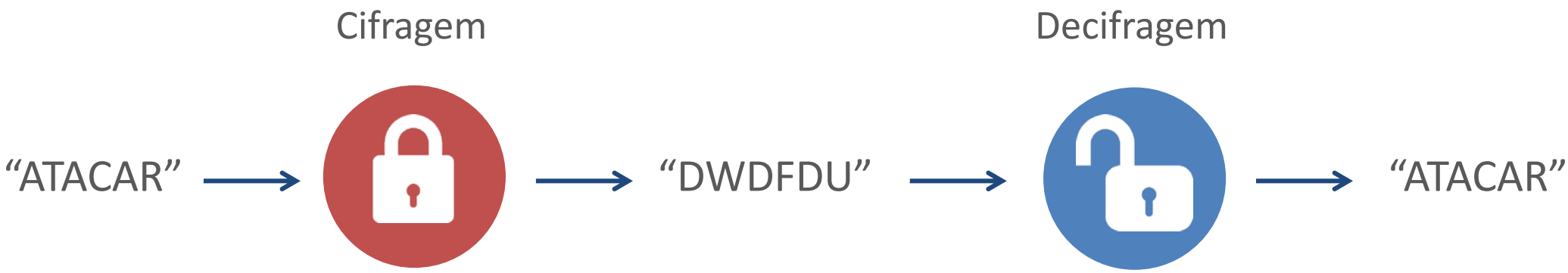
Cada símbolo é substituído por outro símbolo



Caráter original	A	B	C	D	E	...	Z
Novo caráter	J	P	S	T	V	...	B

Cifra de César

Homenagem a Júlio César (100 a.C. - 44 a.C.) que usava um alfabeto assim



Cada caráter é “deslocado” três posições para frente (não há chave)

$E(x) = (x + 3) \bmod 26$

Os caracteres originais são recuperados pelo procedimento inverso

$D(x) = (x - 3) \bmod 26$

Cifra de Vigenère

Cifra polialfabética

Inventada por Giovan Batista Belsa em 1553, apesar de ter sido atribuída durante muito tempo a Blaise de Vigenère.

Semelhante à Cifra de César, mas cada letra é deslocada um diferente número de posições, de acordo com uma senha.

Exemplo:

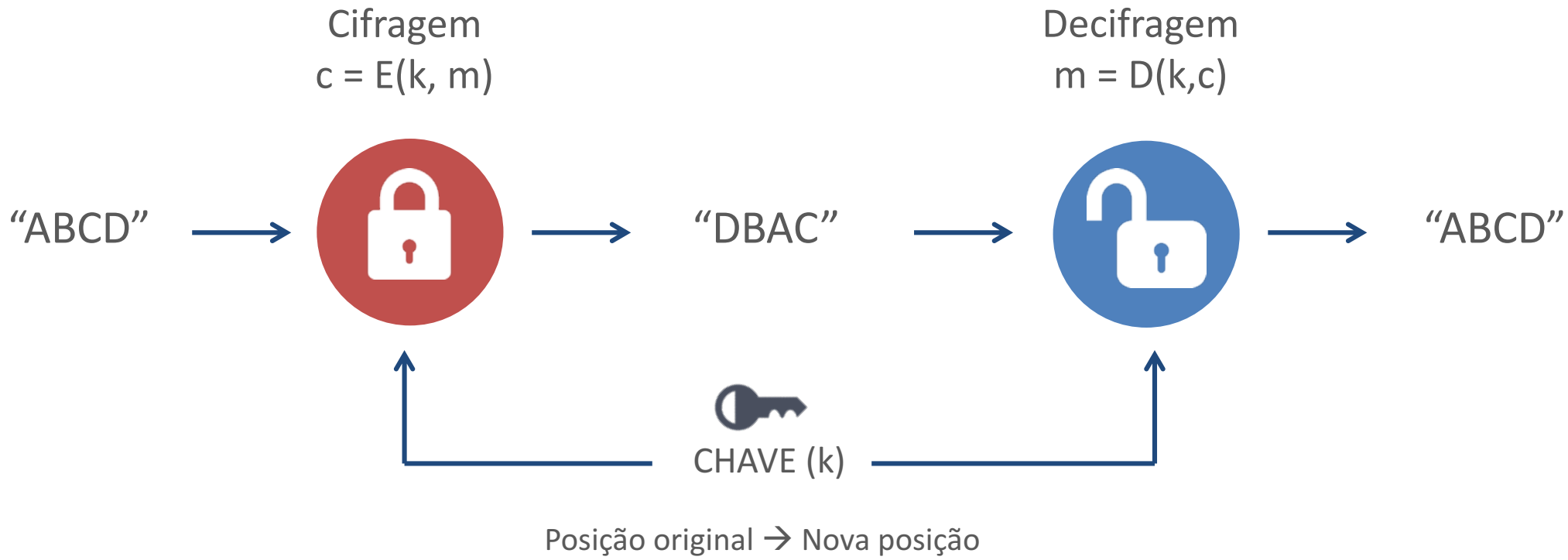
```
FIMDESEMANA  (FIM DE SEMANA)
CAROCAROCAR  (CARO)
HIDRGSUACNR
```

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
A	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
B	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
C	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
D	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
E	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
F	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
G	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F
H	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G
I	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H
J	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I
K	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J
L	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K
M	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L
N	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M
O	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N
P	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O
Q	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P
R	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q
S	S	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R
T	T	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S
U	U	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T
V	V	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U
W	W	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V
X	X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W
Y	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
Z	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y

Cifras de transposição

Cifras de transposição

Os símbolos são trocados de lugar

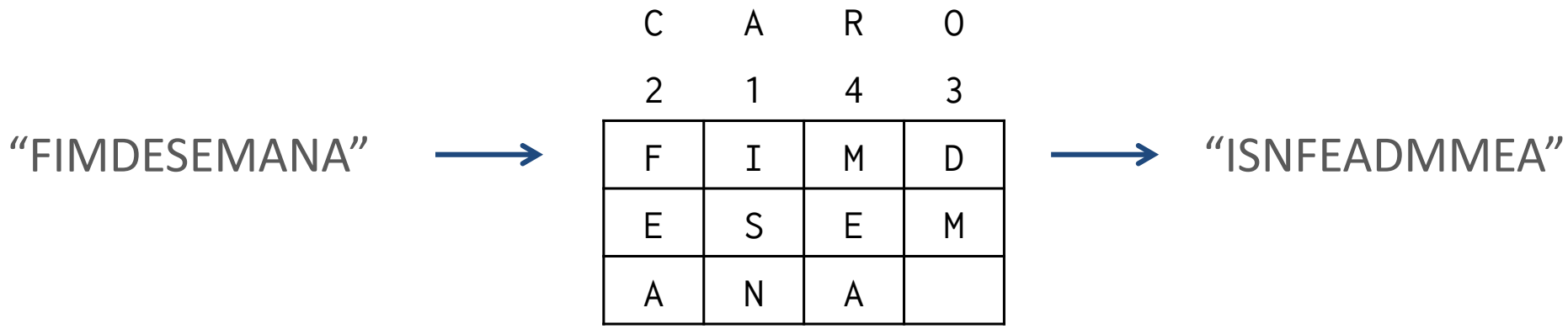


Posição original → Nova posição

Cifra das colunas

A informação é escrita em uma matriz, linha a linha. Em seguida, as colunas são extraídas, na ordem dos valores dos caracteres da palavra chave.

Exemplo:



Enigma

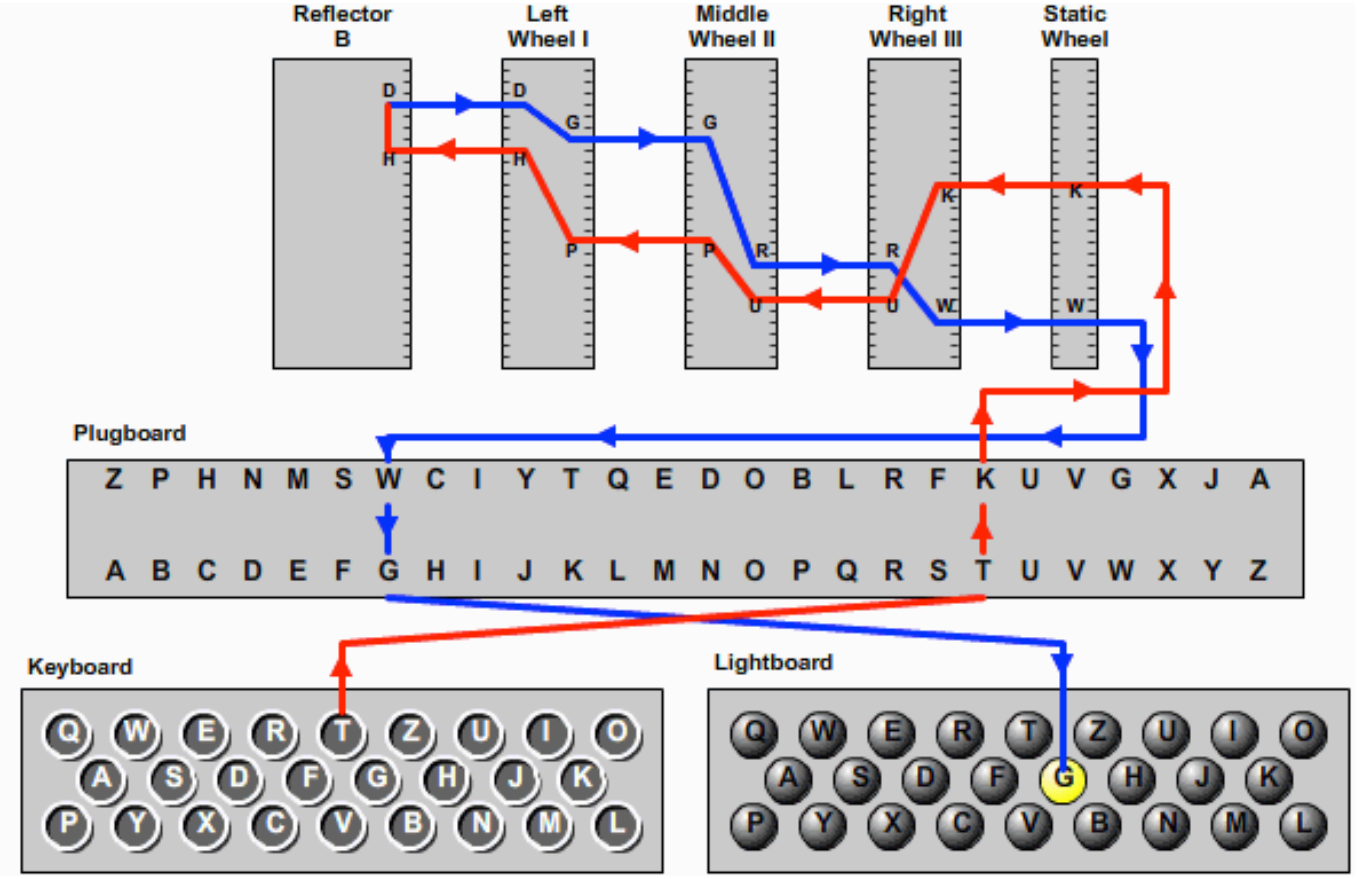
Enigma

A família Enigma de máquinas de cifragem, criadas pelos Alemães a partir de 1918, empregava três ou quatro rotores para fazerem a cifragem por substituição. A cada dia, a configuração deveria ser alterada.

Acredita-se que a decifragem das mensagens da Enigma ajudou a por fim à Segunda Guerra Mundial.

O **Enigma Machine Emulator** permite entender como as Enigmas funcionavam (http://enigma.louisedade.co.uk/index.html)

Enigma



Cada tecla era substituída pelo *plugboard* e depois embaralhada por meio de três rotores.

A configuração dos rotores e do *plugboard* era mudada diariamente.

DADE, Louise. Enigma Machine Emulator. 2006. http://enigma.louisedade.co.uk/index.html


U-571
Matthew
McConaughey
Harvey
Keitel
Bill
Paxton
Jon
Bon Jovi


"THE BEST BRITISH FILM OF THE YEAR"
★★★★★
THE INDEPENDENT
"AN INSTANT CLASSIC"
★★★★★
GLAMOUR
"A SUPERB THRILLER"
★★★★
EMPIRE
★★★★ ★★★★
TIME OUT THE TIMES
THE IMITATION GAME
BENEDICT CUMBERBATCH
KEIRA KNIGHTLEY
12A
BASED ON THE INCREDIBLE TRUE STORY
ALAN TURING

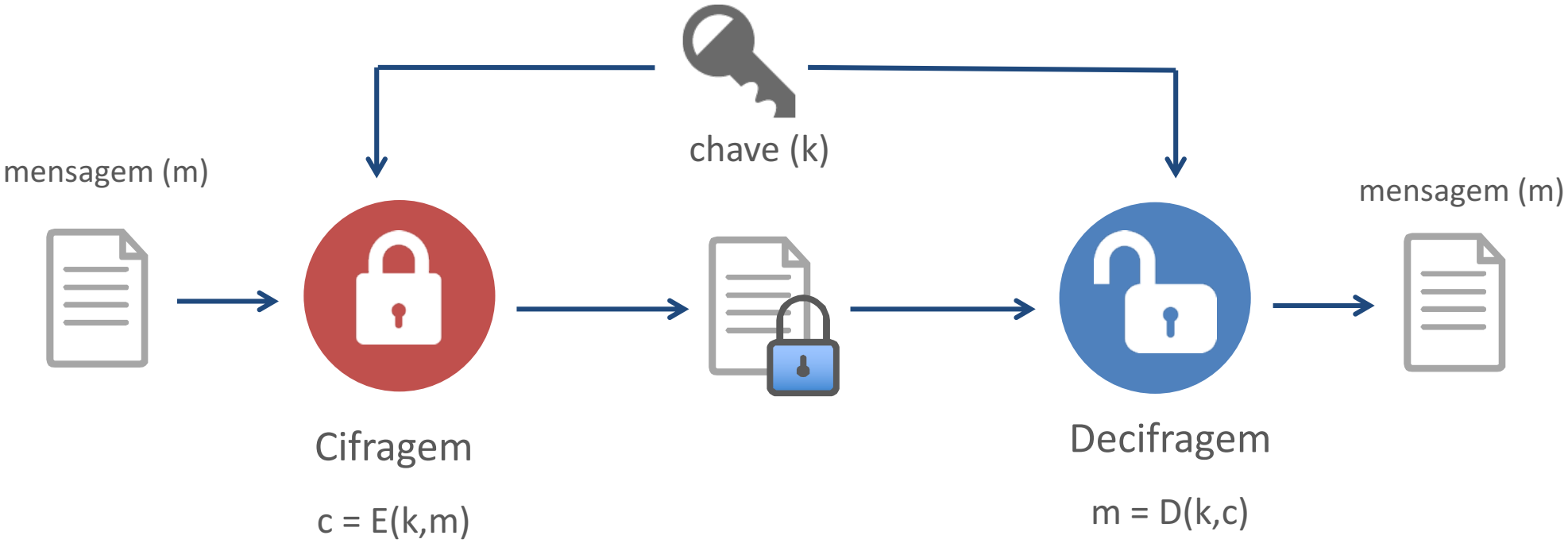
Tipos de criptografia

Tipos de criptografia

Criptografia simétrica – a mesma chave criptográfica é usada na cifragem e na decifragem.

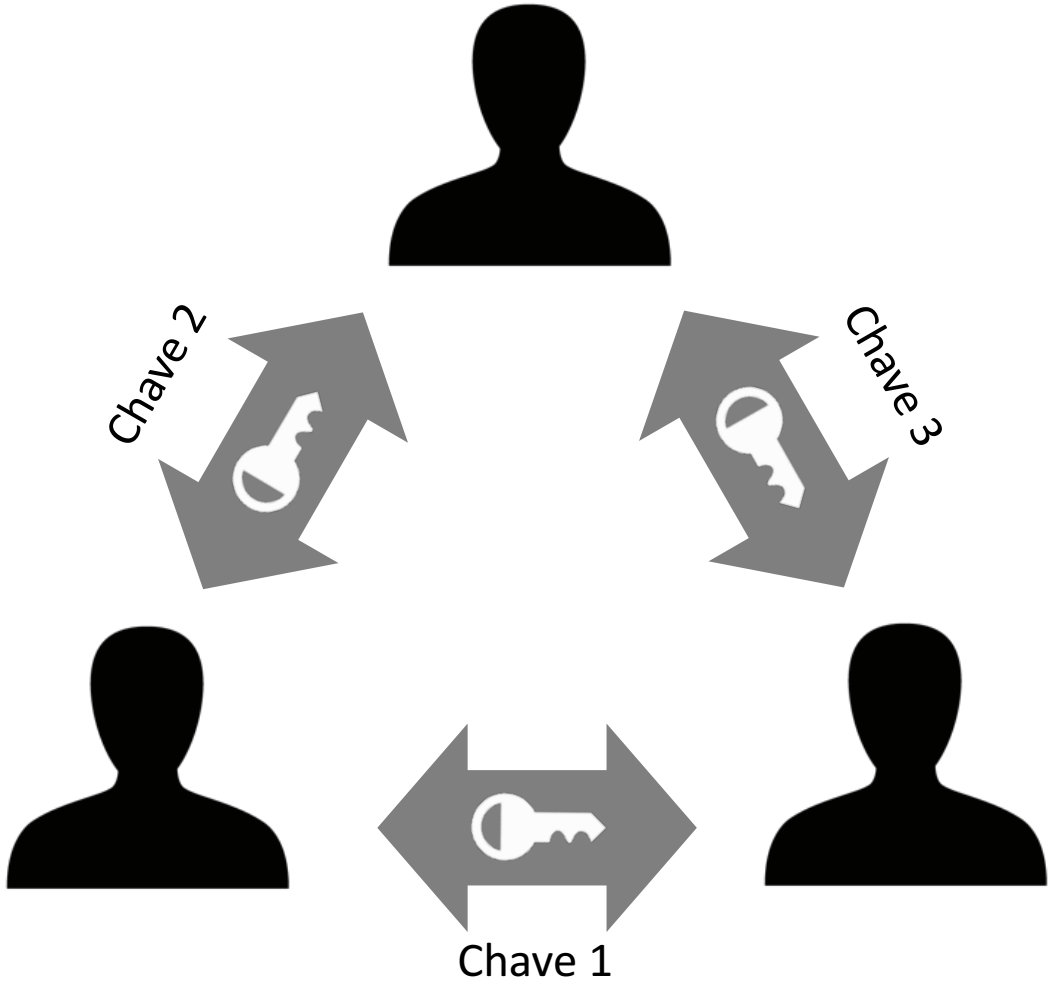
Criptografia assimétrica – chaves diferentes são usadas na cifragem e na decifragem, mas, geralmente, o processo é bidirecional.

Criptografia simétrica

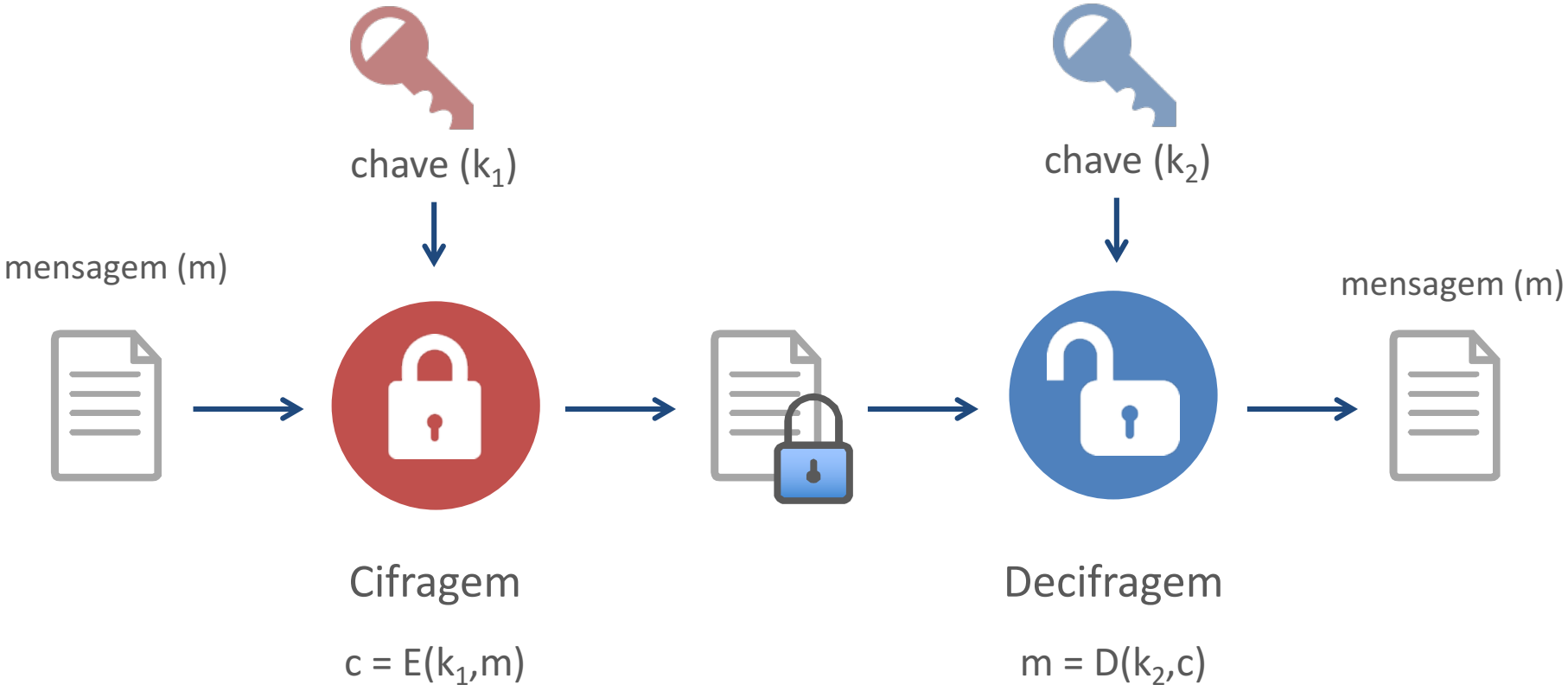


Desafios

- Compartilhar a chave de forma segura.
- Gerenciar um volume muito grande de chaves, quando há um número também muito grande de usuários.



Criptografia assimétrica



Criptografia Simétrica
Cifras de fluxo

Tipos de cifragem em criptografia simétrica

Cifras de fluxo *(stream cipher)*
A cifragem é feita bit a bit (ou símbolo a símbolo).
Ex.: Substituição simples

Cifras de bloco *(block cipher)*
A cifragem é feita em blocos, cada um contendo vários símbolos.
Ex.: Transposição de colunas

Cifra de fluxo

- Cifra de chave simétrica que combina os bits de um fluxo de bits (*bitstream*) com os bits de uma chave (*keystream*)
- A encriptação geralmente é feita por meio de uma simples operação XOR:

$$c = E(k,m) = k \oplus m$$

One Time Pad

- Desenvolvido em 1917 por Gilbert Vernam nos laboratórios da Bell, para cifrar fluxos.
- A chave é uma string de bits aleatória do **mesmo tamanho da mensagem** a ser criptografada.
- É **inquebrável** (matematicamente comprovado), desde que a chave seja realmente aleatória e mantida em segredo.

One Time Pad

$c = E(k,m) = k \oplus m$

Mensagem: 1 0 0 0 1 1 0

Chave: 1 1 0 0 0 1 1

Texto cifrado: 0 1 0 0 1 0 1

$m = D(k,m) = k \oplus c$

Texto cifrado: 0 1 0 0 1 0 1

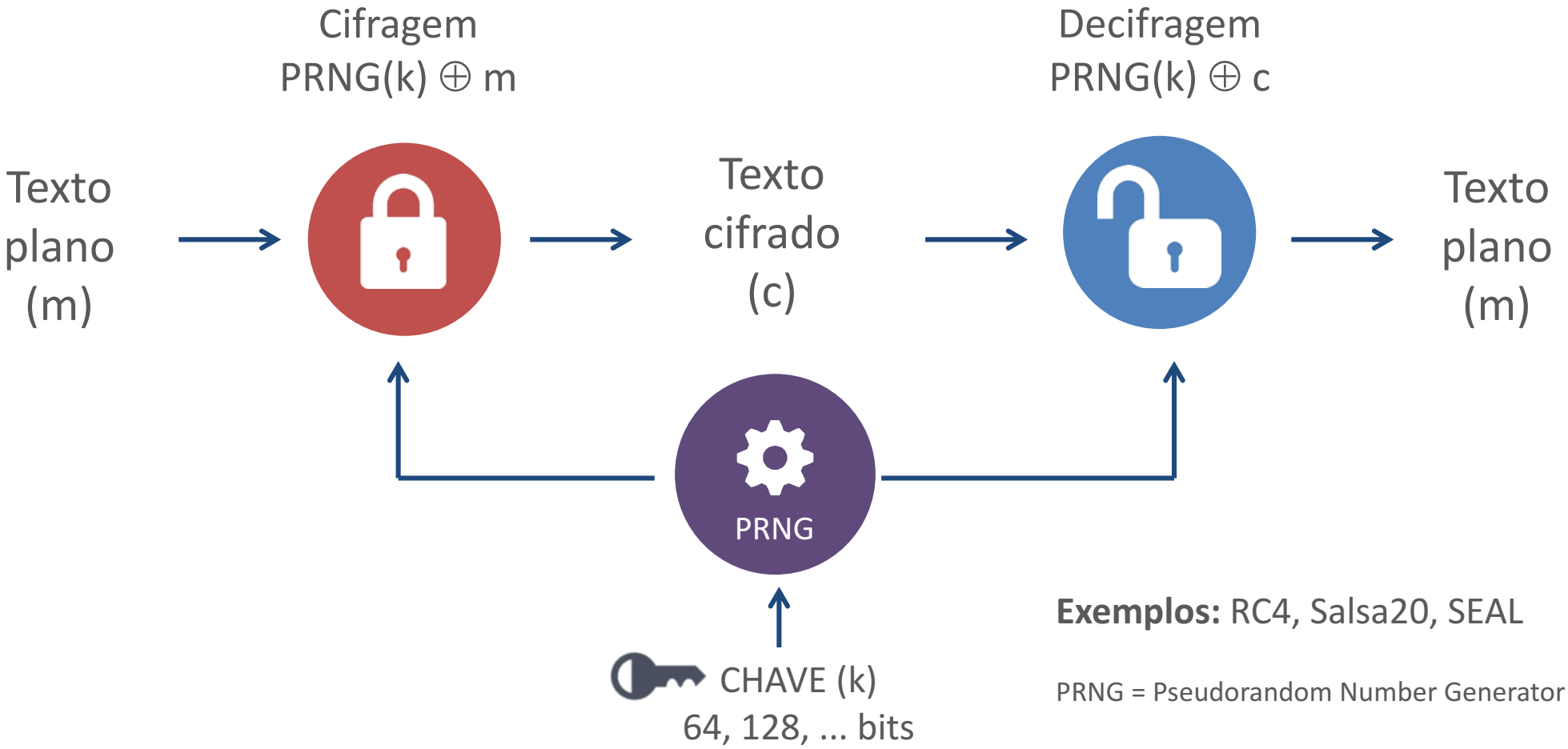
Chave: 1 1 0 0 0 1 1

Mensagem: 1 0 0 0 1 1 0

One Time Pad

- O OTP requer chaves muito longas, difíceis de serem gerenciadas e mantidas em sigilo.
- Os algoritmos usam, portanto, um **gerador de chaves pseudoaleatórias** usando uma **chave semente** de 64, 128, 256 ou mais bits.

Chaves pseudoaleatórias



Exemplos: RC4, Salsa20, SEAL

PRNG = Pseudorandom Number Generator

Cifras de fluxo

VANTAGENS

- **Alta velocidade**
  Os algoritmos são lineares no tempo e constantes no espaço.
- **Baixa propagação de erros**
  Um erro na cifragem de um símbolo dificilmente afetará os símbolos seguintes.

DESVANTAGENS

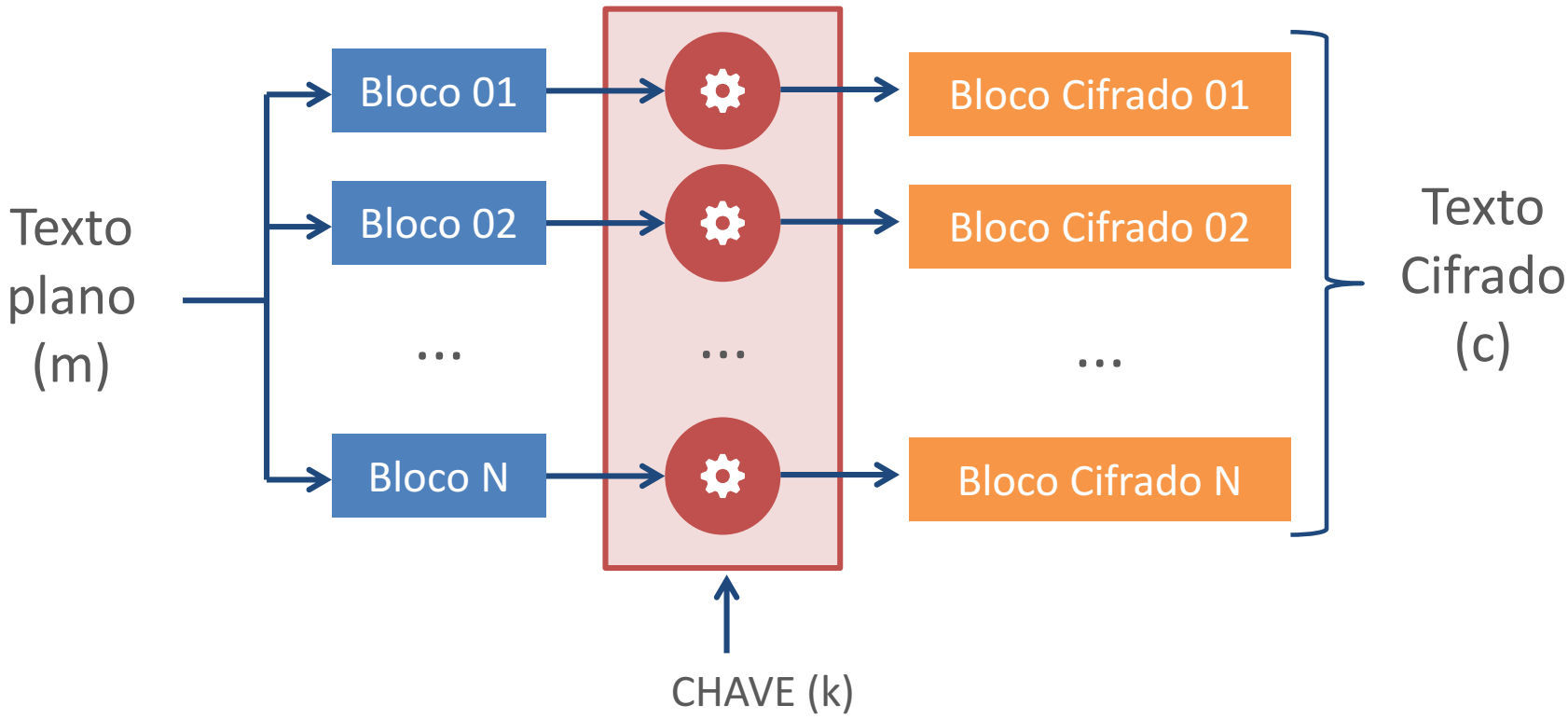
- **Baixa difusão**
  Toda a informação de um símbolo de texto simples é contido em um único símbolo de texto cifrado.
- **Suscetibilidade a inserções e modificações**
  Um intruso pode inserir texto falso que parece autêntico.

Cifras de bloco

Cifras de bloco

- Cifra um conjunto de símbolos como um único bloco.
- O tamanho do bloco pode variar
  (64 bits no DES, 128 bits no AES, etc.).
- Cada bloco é cifrado de forma independente.

Cifras de bloco



Exemplos:
IDEA
RC5
RC6
AES
Blowfish
CAST
Rijndael
3DES

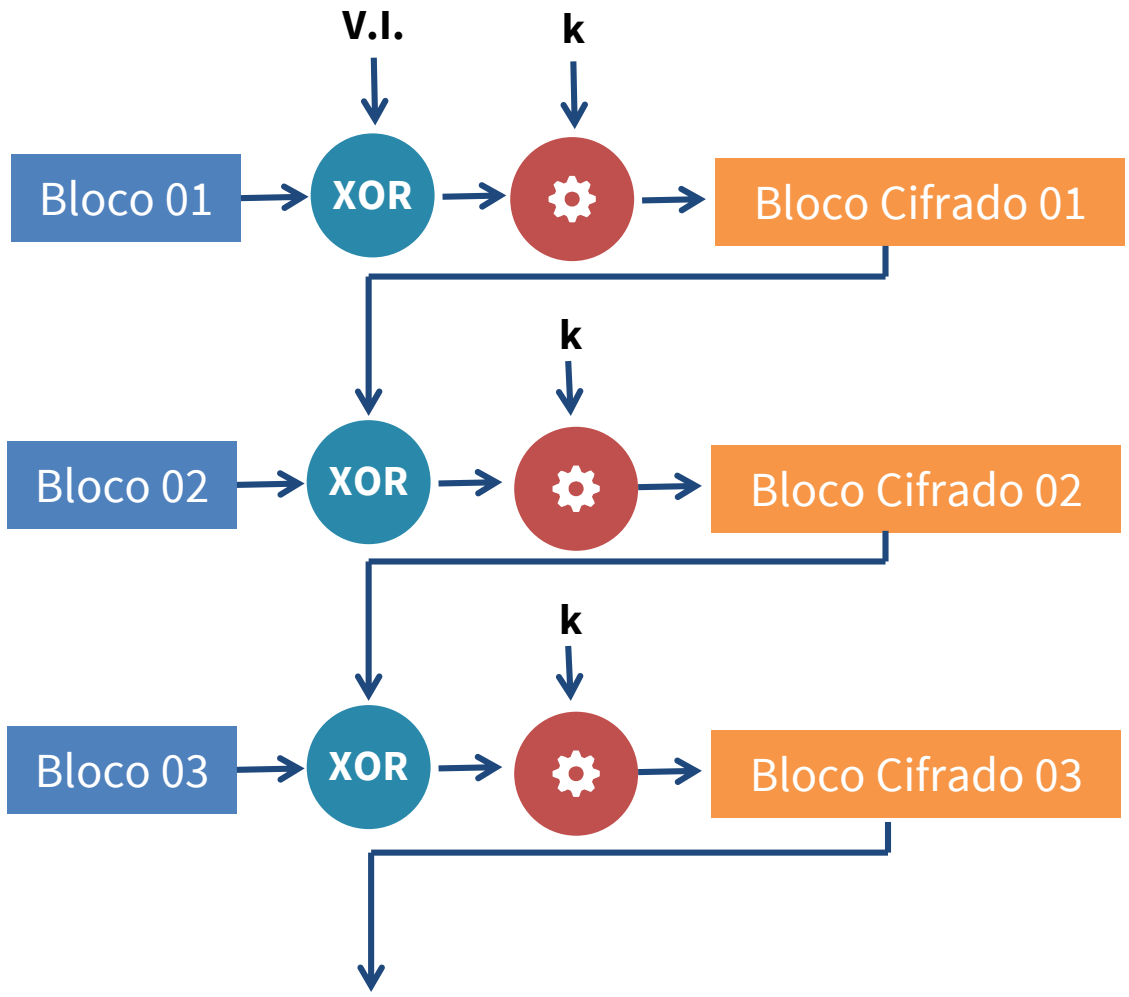
Cifras de bloco

- Se o mesmo bloco se repetir, os blocos cifrados serão iguais, facilitando a percepção de um padrão.
- Para evitar isso, existem algumas técnicas como a **realimentação**, em que o bloco anterior é usado na cifragem do bloco atual

Cifras de bloco por encadeamento

CBC (Cypher Block Chaining)

- Faz-se um XOR do bloco plano atual com o bloco cifrado anterior
- Para o primeiro bloco (sem bloco anterior), é feito um XOR com um vetor de inicialização (V.I.)



Cifras de bloco

VANTAGENS

- **Alta difusão**
  A informação de um símbolo é distribuída entre vários símbolos do texto cifrado.
- **Imunidade a alterações**
  É difícil inserir símbolos no texto cifrado sem detecção.

DESVANTAGENS

- **Baixa velocidade**
  Um bloco inteiro deve ser acumulado antes da cifragem ou decifragem começar.
- **Propagação de erros**
  O erro em um símbolo pode corromper todo o bloco.

Criptografia assimétrica

Criptografia assimétrica

ou Criptografia de Chave Pública

- Chaves diferentes são usadas na cifragem e na decifragem.
- Uma dessas chaves é tornada pública e a outra é mantida secreta (privada).

$C = E(K_{pub}, M)$ $\qquad\qquad$ $M = D(K_{priv}, C)$

- Em alguns algoritmos, as chaves são intercambiáveis.

$C = E(K_{priv}, M)$ $\qquad\qquad$ $M = D(K_{pub}, C)$

Criptografia assimétrica

ou Criptografia de Chave Pública

$C = E(K_{pub}, M)$ $M = D(K_{priv}, C)$

Cada um tem
o seu par
de chaves

$C = E(K_{pub}, M)$ $M = D(K_{priv}, C)$

Princípio matemático

- Criação de um função unidirecional, facilmente computada, mas difícil de ser invertida.
- Exemplo:
  - é fácil multiplicar dois números primos grandes, mas é difícil fatorar o resultado para descobrir os números originais (sem se ter pelo menos um deles).
- Um algoritmo assimétrico pode ser até 10.000 vezes mais lento do que um algoritmo simétrico.

Algoritmo RSA

Rivest – Shamir – Adelman

- Escolha dois números primos extensos, p e q (maiores de 10100)
- Calcule $n = p * q$ e $z = (p - 1) * (q - 1)$
- Escolha um número relativamente primo a z e chame-o de d
- Escolha e de forma que $(e * d)\ mod\ z = 1$
- Para cifrar, calcule $C = P^e\ mod\ n$
- Para decifrar, calcule $P = C^d\ mod\ n$
- A chave pública será composta por e e n
- A chave privada será composta por d e n`

Algoritmo RSA

Rivest – Shamir – Adelman

$p = 3$
$q = 11$
$n = p \cdot q = 33$
$z = (p - 1)(q - 1) = 20$
$d = 7$, primo em relação a z
$e = 3$, pois $(e \cdot d) mod\ z = 1$

Cifragem

Texto	P	P^3	C = P^3mod(33)
A	1	1	1
T	20	8.000	14
A	1	1	1
Q	17	4.913	29
U	21	9.261	21
E	5	125	26

Decifragem

C	C^7	P = C^7mod(33)	Texto
1	1	1	A
14	105.413.504	20	T
1	1	1	A
29	17.249.876.309	17	Q
21	1.801.088.541	21	U
26	8.031.810.176	5	E

Assinatura digital

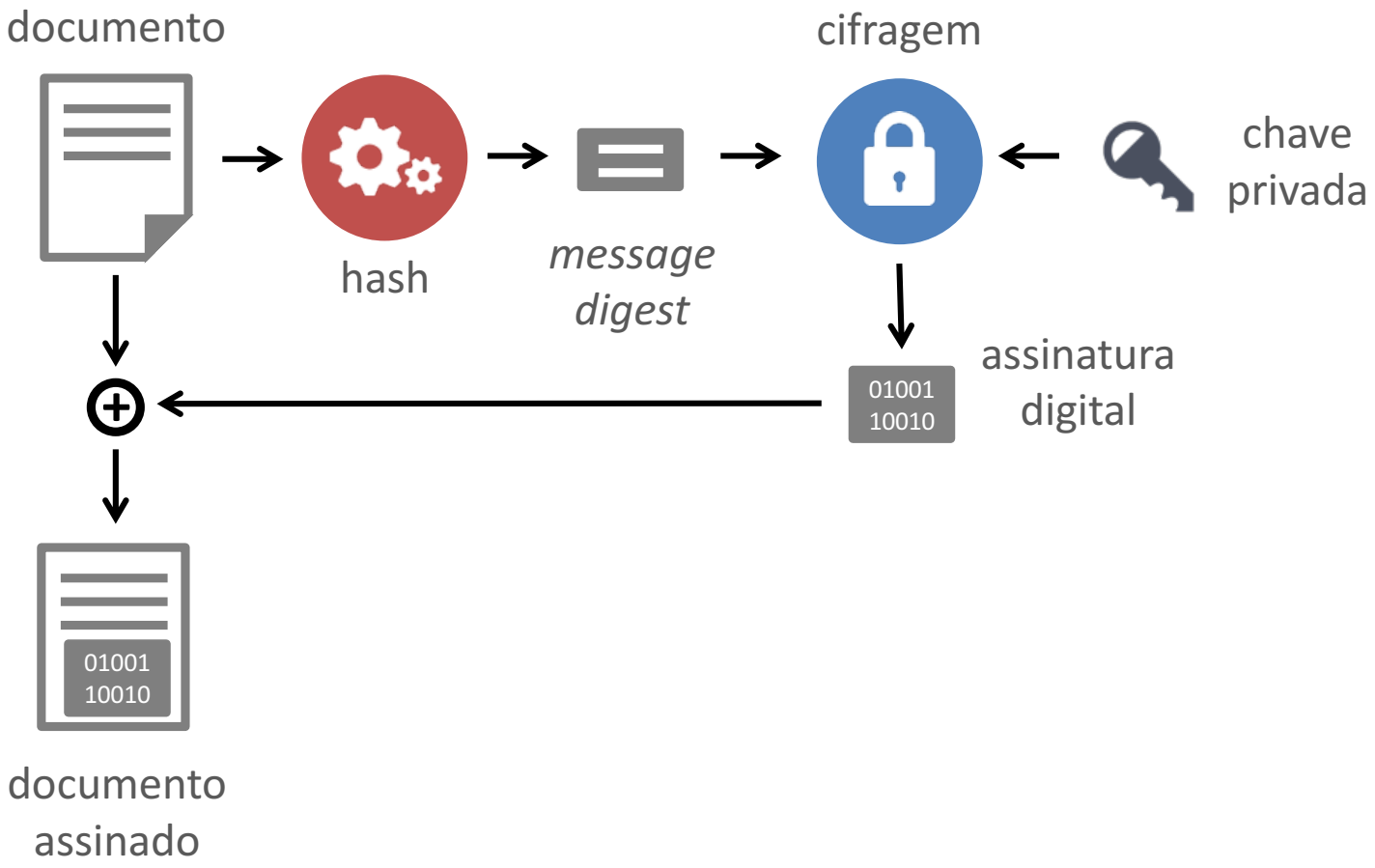
Assinaturas digitais

- Uma assinatura é uma autorização de transação.
- Se necessário, uma entidade pode autenticar a assinatura.
- O documento (transação) não pode ser alterado
- A assinatura é parte do documento e não pode ser separada dele.

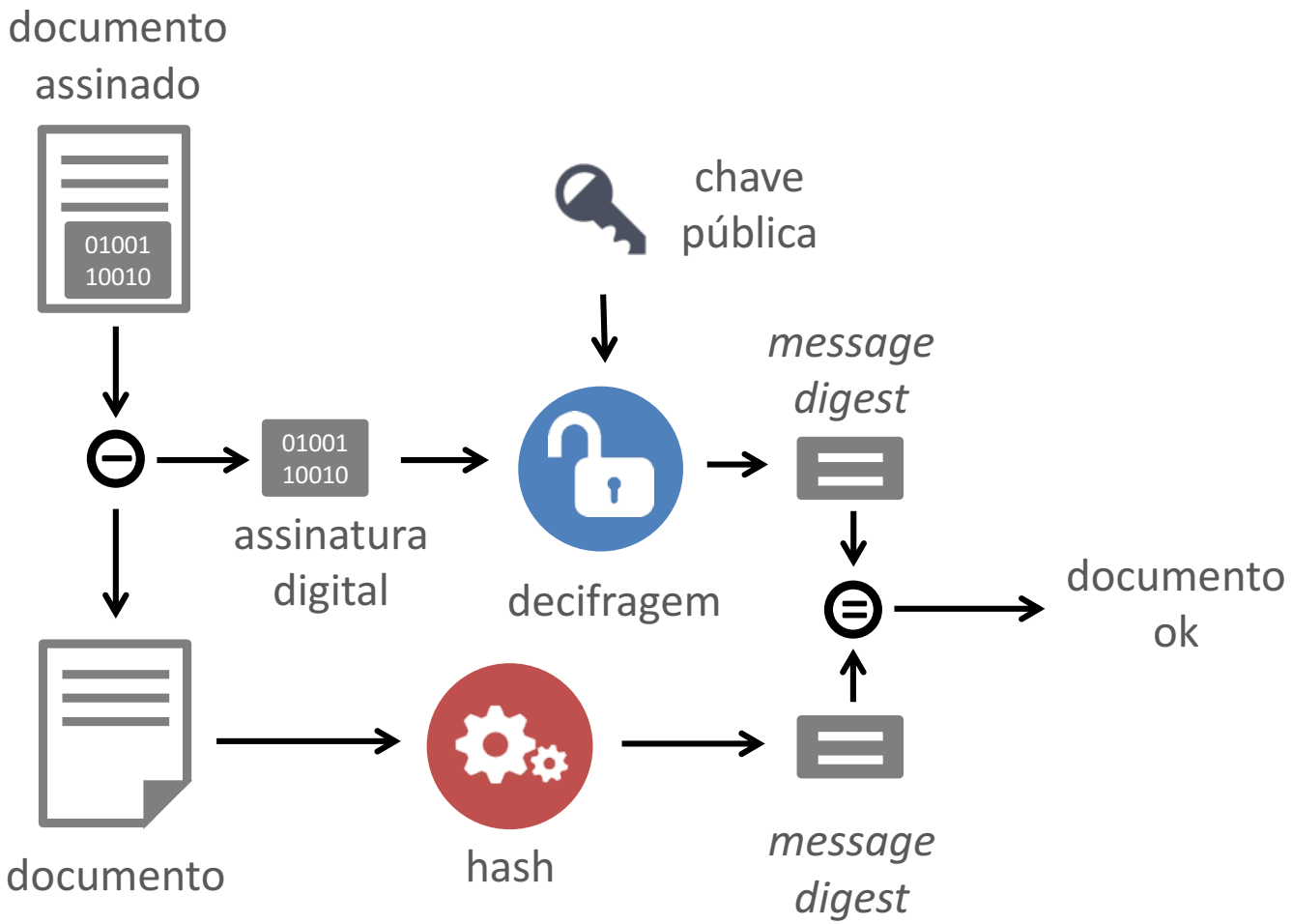
Assinaturas digitais

- Uma assinatura digital é:
  - **Não fraudável**: é impossível alguém produzir a assinatura de outro.
  - **Autenticável**: é possível verificar se a pessoa assinou o documento.
  - **Não repudiável**: não é possível negar ter produzido a assinatura.
  - **Inviolável**: após geração, o documento não pode ser alterado.
  - **Não reusável**: a assinatura não pode ser usada em outro documento.

Assinatura


documento
hash
message
digest
cifragem
chave
privada
01001
10010
assinatura
digital
01001
10010
documento
assinado

Autenticação



Certificado digital

Certificado digital

- Um certificado digital é um arquivo que contém a identidade de um indivíduo ou entidade e a sua chave pública.
- O certificado digital é emitido por uma entidade certificadora, a partir de uma rede de confiança (*web of trust*) descentralizada.

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Solicita conexão via SSL/TSL

Cliente

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

$E(K_{sessão} , "ok")$

Servidor

Comunicação segura

SSL – Secure Socket Layer
TSL – Transport Layer Security

Cliente

Solicita conexão via SSL/TSL

Retorna certificado digital com chave pública K_{pub}

$E(K_{pub} , K_{sessão})$

$E(K_{sessão} , "ok")$

$E(K_{sessão} , mensagens)$

Servidor