Algoritmos Criptográficos

Criptografia Simétrica e Assimétrica

Prof. Dr. Adriano Mauro Cansian

adriano.cansian@unesp.br

Algoritmos Criptográficos

O que são algoritmos criptográficos?

A criptografia de dados é controlada por algoritmos e fórmulas matemáticas (razoavelmente) complicadas.

Existem vários tipos de subtipos de algoritmos criptográficos.

Mas as categorias mais importantes são algoritmos simétricos e assimétricos.

Há 2 tipos principais de criptografia

Cripto Simétrica

&

Cripto Assimétrica

(Os sistemas também podem combinar as duas técnicas)

Criptografia simétrica

Criprografia Simétrica

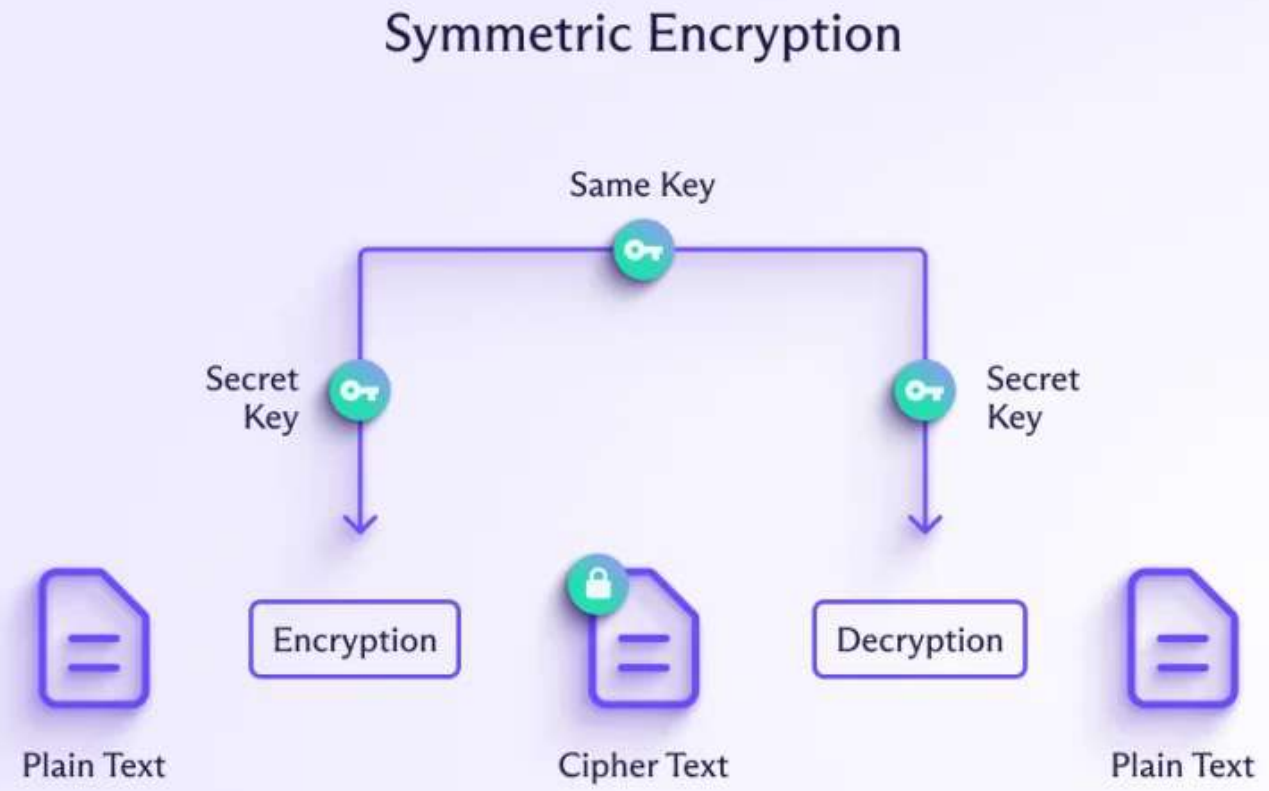


Figura - créditos: https://proton.me/blog/what-is-encryption

Criptografia com Chave Simétrica (1)

Código de substituição: deslocamento '*k*' ou "Cifra de César"

- Consiste em deslocar as letras do alfabeto por uma distância "*k*".

```
texto aberto:   abcdefghijklmnopqrstuvwxyz
                   ↓       ↓       ↓
texto cifrado:  xyzabcdefghijklmnopqrstuvw
```

Ex.:

```
Texto "claro": Ola. Tenho um segredo para contar. -Alice
Texto cifrado:  Lix. Qbkel rk qbdobal mxox zlkqxo. -Xifzb
```

Quão difícil é quebrar este código simples?

- Há somente 25 valores diferentes para as chaves.
- Não é difícil de descobrir.

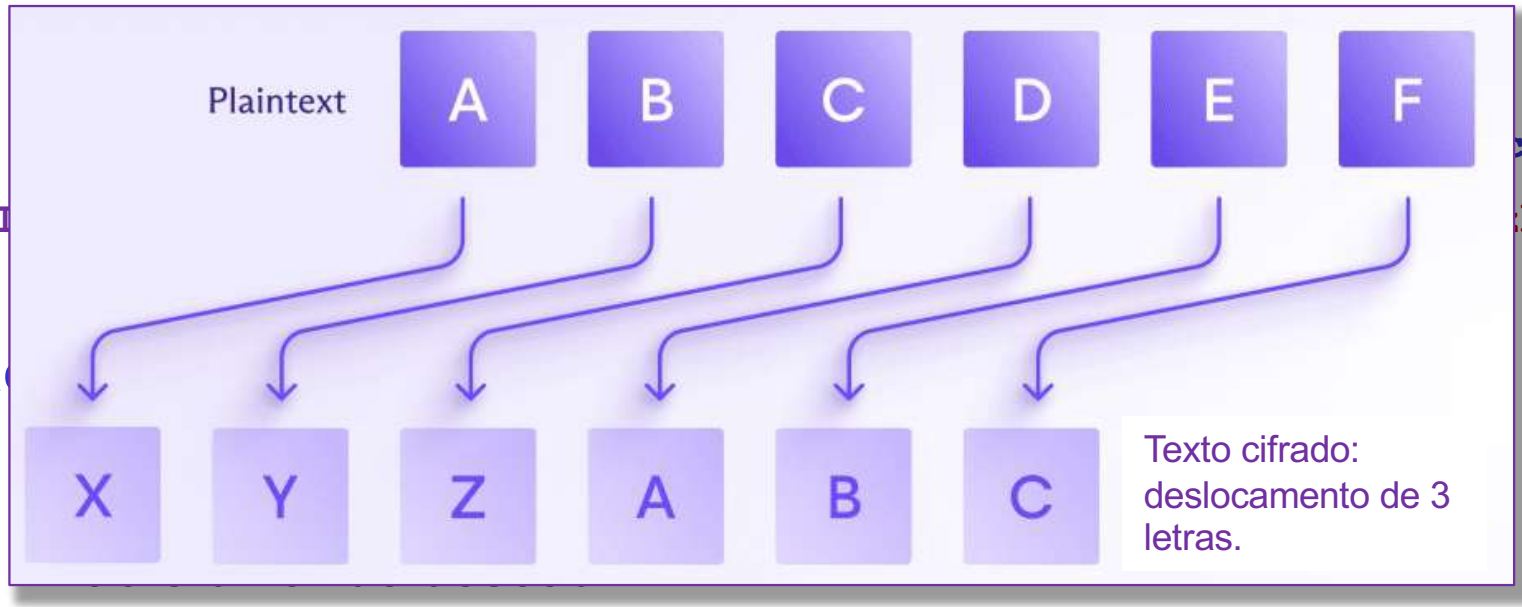
Criptografia com Chave Simétrica (2)

Código de substituição: deslocamento '*k*' ou "Cifra de César"

- Consiste em deslocar as letras do alfabeto por uma distância "*k*".

```
texto aberto:   abcdefghijklmnopqrstuvwxyz
texto cifrado:  xyzabcdefghijklmnopqrstuvw
```

Ex.:



Quã

Criptografia com Chave Simétrica (3)

Código de substituição: substituindo um caractere por outro

- código mono-alfabético: consiste em substituir uma letra por outra.

```
texto aberto:   abcdefghijklmnopqrstuvwxyz
                  ↓                   ↓
texto cifrado:  mnbvcxzasdfghjklpoiuytrewq
```

Texto "claro": Ola. Tenho um segredo para contar. -Alice

Texto cifrado: Kgm. Ucjak yh iczocvk lmom bkjumo. -Mgsbc

Complicou (um pouco) para quebrar este código simples?

Força bruta: 26! pares possíveis de letras = ordem de 10^{26}

Faça você mesmo: https://www.dcode.fr/monoalphabetic-substitution

Algoritmos simétricos - 2 tipos principais:

Algoritmos simétricos funcionam de duas maneiras distintas:

- Codificam as informações bit a bit, ou byte a byte.
  - São chamados de "**cifras de fluxo**".
- Quebram as informações em blocos e os codificam.
  - São chamados de "**cifras de blocos**".

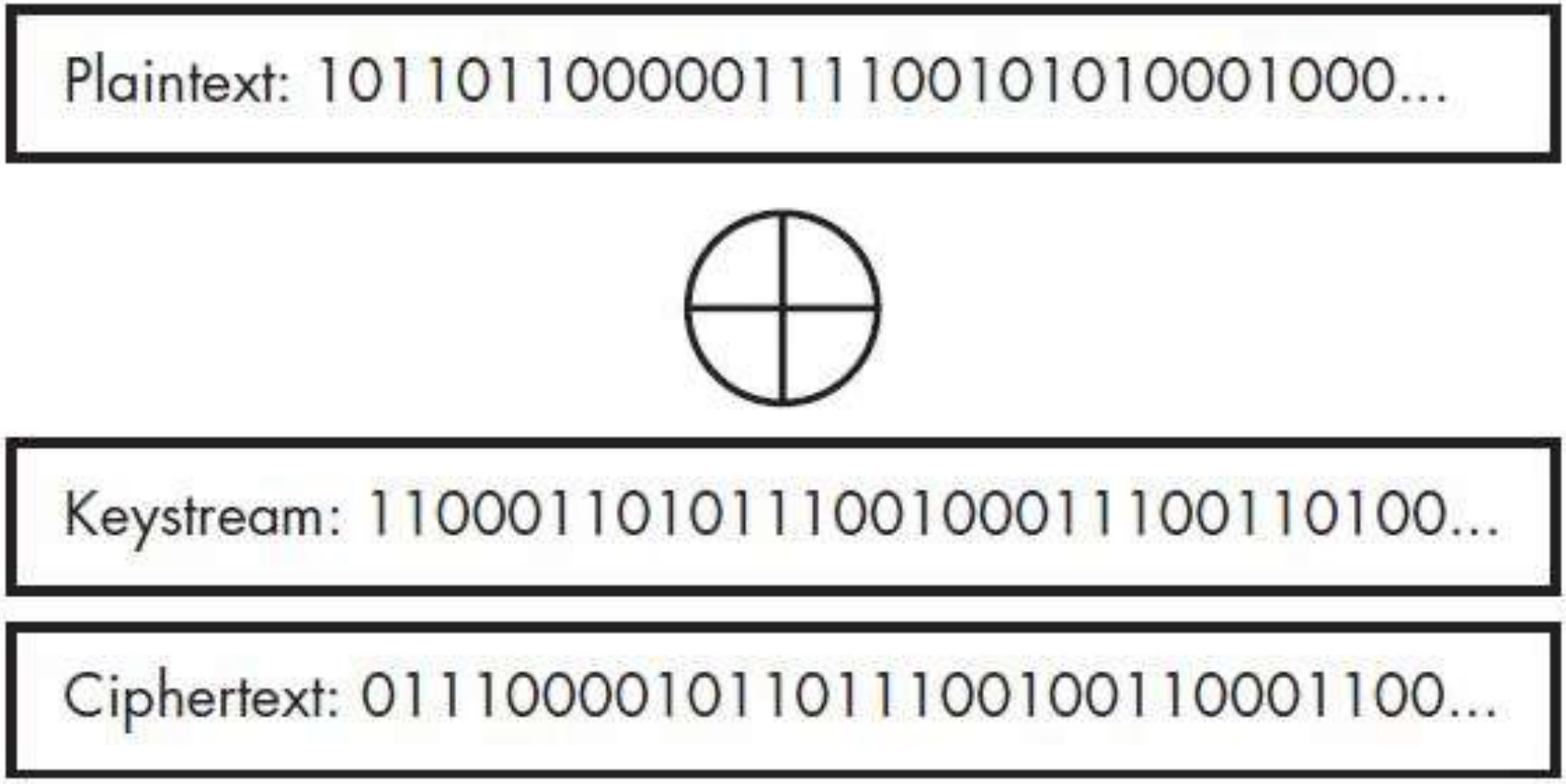
Algoritmos de Cifra de Fluxo

Como funciona uma Cifra de Fluxo (1)

1. Geração de Keystream e Cifragem :

- Inicia com chave secreta (*K*) e um vetor de inicialização (*VI*).
- Com *K* e o *VI*, o algoritmo gera um conjunto de bytes chamado "*keystream*".
- O *keystream* é então combinado com texto plano usando uma operação matemática (chamada XOR - "Ou Exclusivo").
- Cada byte do texto plano é cifrado ao ser combinado com o correspondente byte do *keystream*.

Keystream e cifragem

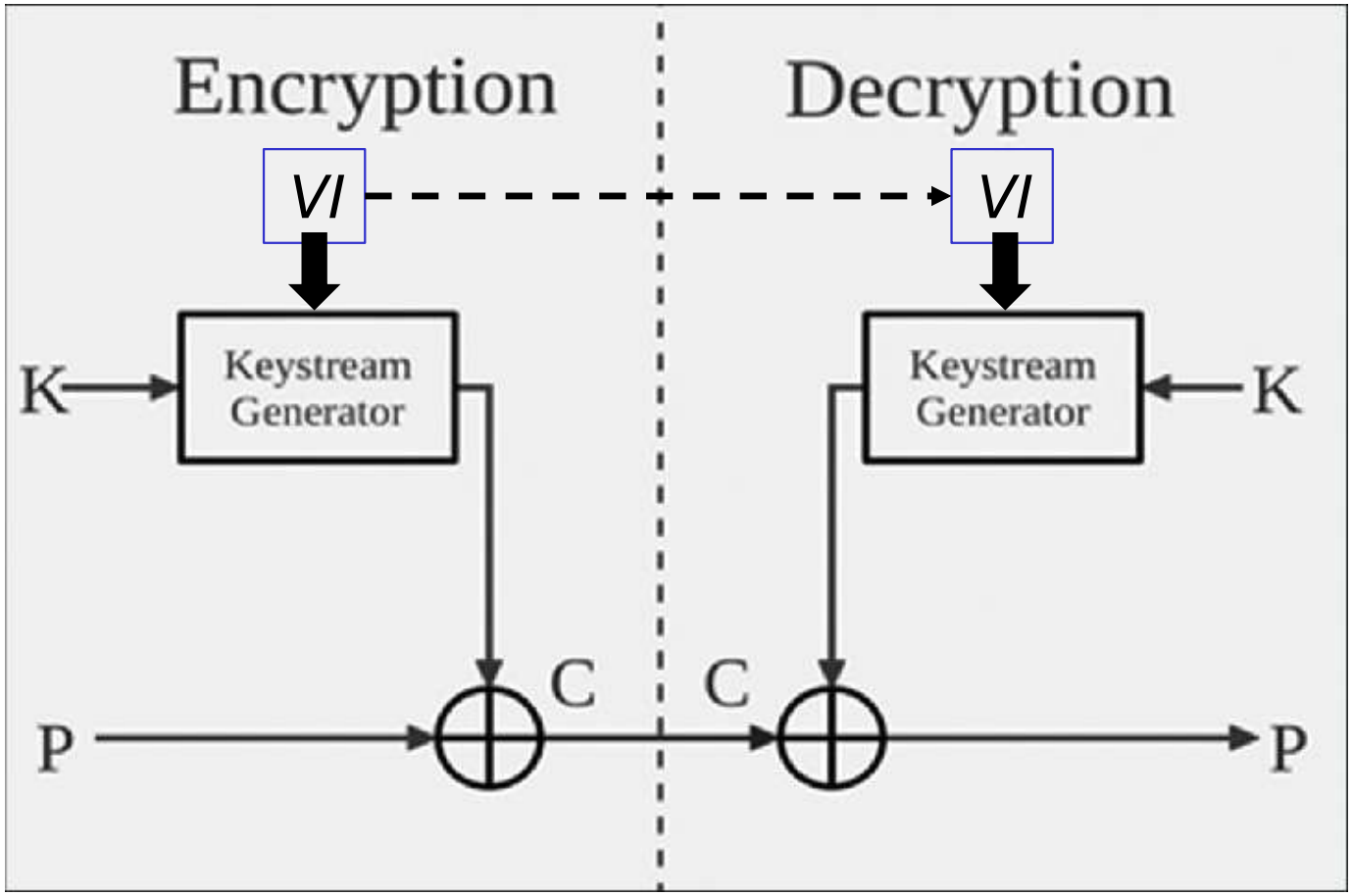


Como funciona uma Cifra de Fluxo (2)

3. Decifragem:

- Para decifrar os dados, o destinatário gera o mesmo *keystream* usando a chave *K* (simétrica, que ele conhece) e o *VI* originais.
- O *keystream* é então combinado com o texto cifrado usando a operação XOR, revertendo o processo e recuperando o texto claro original.

Como funciona uma Cifra de Fluxo (3)



Créditos - figura: https://www.researchgate.net/figure/Stream-cipher-diagram_fig2_318517979

Exemplo de Algoritmos de Cifras de Fluxo

- **RC4**: Um dos algoritmos de cifra de fluxo mais conhecidos.
  - Embora tenha sido amplamente usado, agora é considerado inseguro para algumas aplicações devido a várias vulnerabilidades descobertas ao longo dos anos.
- **A5/1**: Utilizado em comunicações móveis GSM.
- **Salsa20/ChaCha**: Cifras de fluxo modernas conhecidas por sua segurança e desempenho.
  - ChaCha20 é amplamente usado no protocolo TLS 1.3.

Algoritmos de Cifra de Blocos

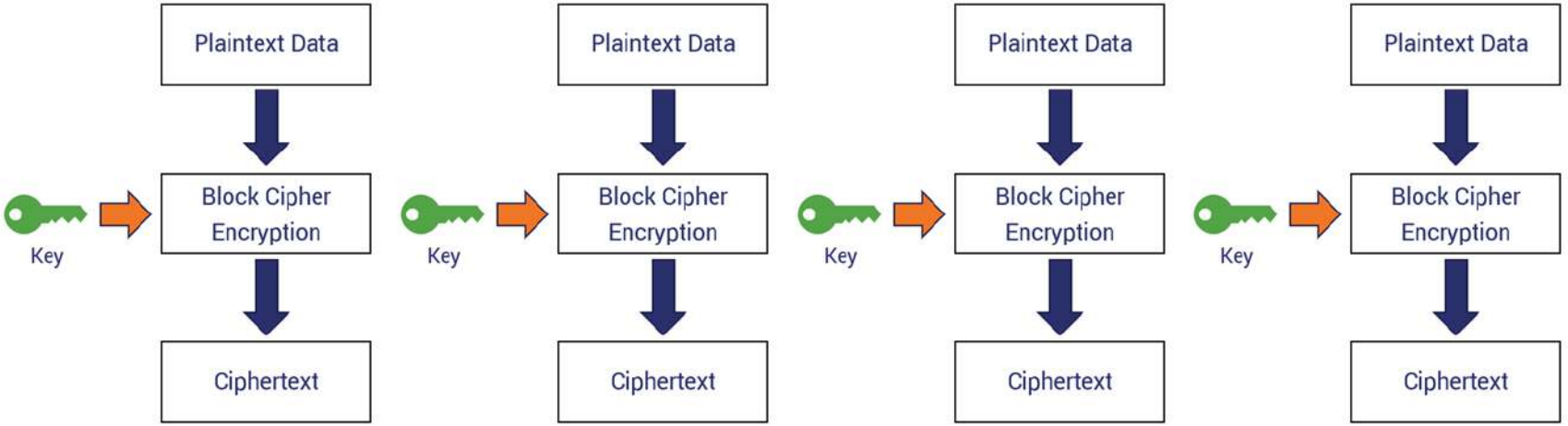
Como funciona uma Cifra de Bloco

- **Divisão em Blocos**:
  - O texto claro é dividido em blocos de tamanho fixo, como 64 bits (8 bytes) ou 128 bits (16 bytes).
- **Cifragem de Blocos**:
  - Cada bloco de texto claro é cifrado separadamente, usando uma **chave secreta** e um algoritmo específico.
- **Combinação dos Blocos Cifrados**:
  - Os blocos cifrados são então combinados para formar o texto cifrado final.

Cifra de bloco simples – ideia básica:

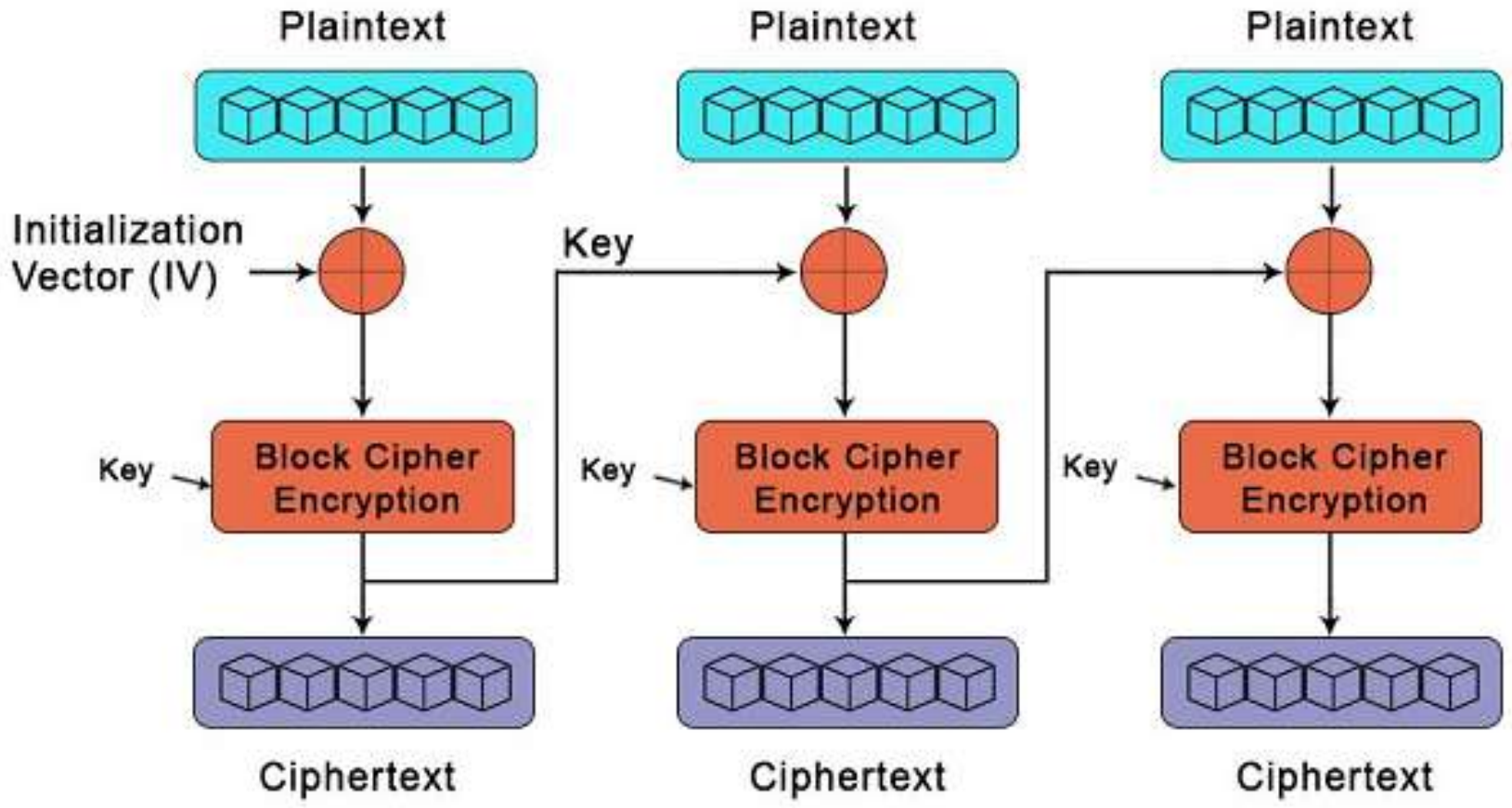
ASCII:	Binário:
“Segredo”	**01110011 01100101** 01100111 01110010 01100101 01100100 01101111 00001010

01110011 01100101 01100111 01110010 01100101 01100100 01101111 00001010



10101111 11100110 01010101 01100110 01110101 00100101 01111111 00110010

Cifra de bloco com encadeamento



Créditos – Figura: https://www.javatpoint.com/block-cipher-vs-stream-cipher

Exemplos de algoritmos de cifras de blocos

- **DES (*Data Encryption Standard*)**:
  - Algoritmo mais antigo com blocos de 64 bits e chaves de 56 bits.
  - Hoje é considerado inseguro devido ao seu tamanho de chave pequeno.
- **AES (*Advanced Encryption Standard*)**:
  - O padrão atual para criptografia, usa blocos de 128 bits e chaves de 128, 192 ou 256 bits.
  - É amplamente considerado seguro e eficiente.
- ***Blowfish* e *Twofish***:
  - Cifras de bloco com diferentes tamanhos de bloco e chave, usadas em várias aplicações.

AES: Padrão para cripto simétrica

- AES – *Advanced Encryption Standard*
- Novo padrão do NIST para cripto com chaves simétricas.
- Criado em 2001 e definido como padrão em 2005
- Processa dados em blocos de 128 bits.
- Chaves de 128, 192 ou 256 bits.
- Estimativa:

  Decodificação por força bruta que leva 1 seg no DES (testar as $\mathbf{2^{55}}$ chaves por segundo), levaria 149 trilhões de anos no AES de 128 bits.

  - https://doi.org/10.1016/j.procs.2016.02.108 (16-Jul-24)

Alguns algoritmos simétricos e autores

- DES - Data Encryption Standard (FIPS 46-3, 1976) (Ataques bem sucedidos) [Bloco]
- RC4 - Prof. Ron Rivest (1987) (Ataques bem sucedidos) [Fluxo]
- RC5 - Prof. Ron Rivest (1994) (Seguro mas pouco utilizado) [Bloco]
- IDEA - J Massey e X Lai – (1990) (Seguro mas pouco utilizado) [Bloco]
- Blowfish - Bruce Schneier (1993) (Seguro – amplamente utilizado) [Bloco]
- Twofish – B. Schneier, J. Kelsey, D. Whiting, D. Wagner e C. Hall (1998) (Seguro – idem) [Bloco]
- **AES - também conhecido como RIJNDAEL (padrão FIPS-197) (2001) (Seguro – idem)** [Bloco]
- RC6 - Prof. Ron Rivest (1998) (Seguro mas pouco utilizado) [Bloco]
- Salsa20 - Prof. Daniel Bernstein (2005) (Seguro – amplamente utilizado) [Fluxo]
- ChaCha20 - Prof. Daniel Bernstein (2005) (Seguro – amplamente utilizado TLS 1.3) [Fluxo]

Criptografia Assimétrica

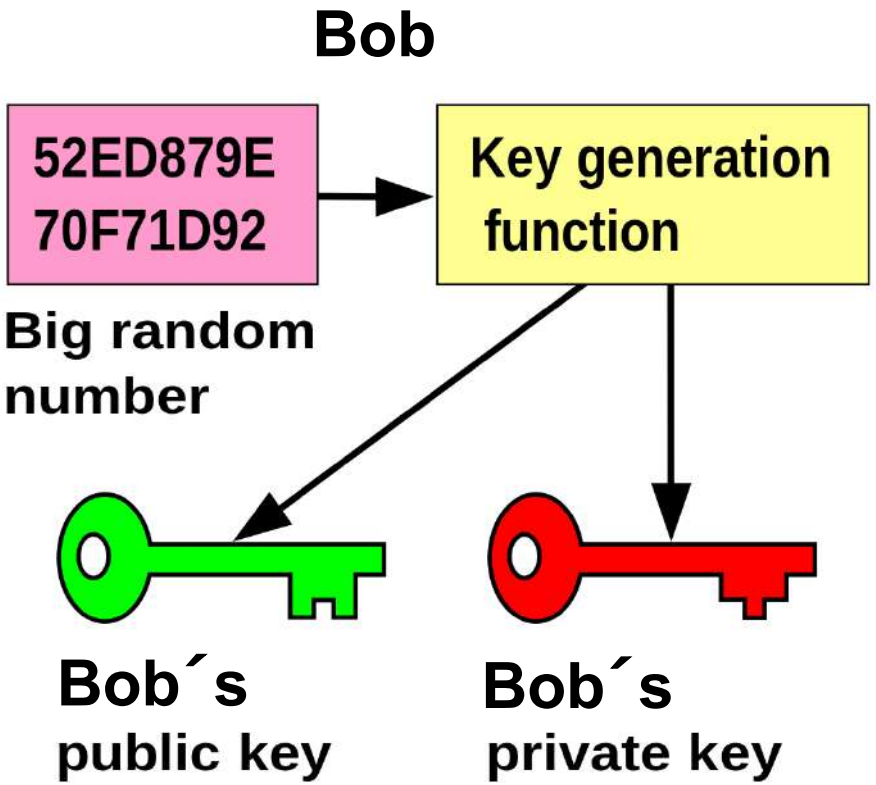
ou

Criptografia de Chave Pública

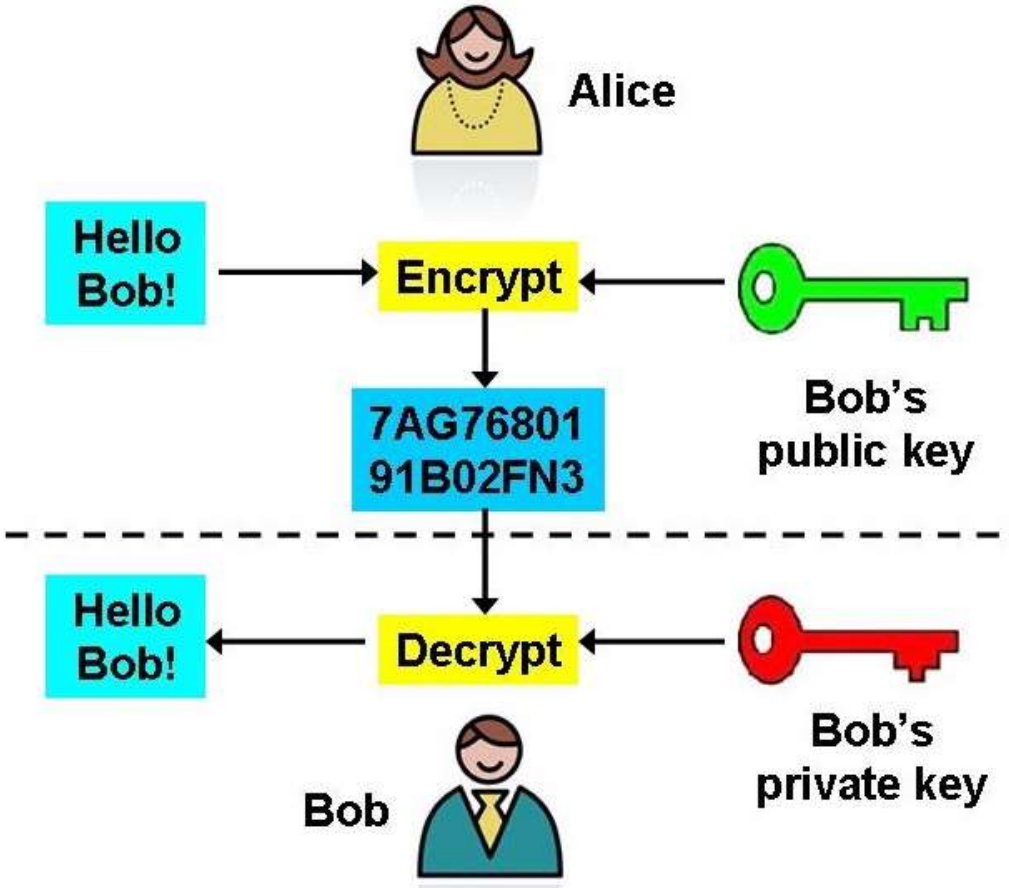
Criptografia com Chave Pública

- Abordagem radicalmente diferente.
- Principais algoritmos: Diffie-Hellman e RSA.
- Usuários **não** compartilham uma chave secreta (simétrica).
- A chave de criptografia é pública (conhecida por todos).
- Chave de decriptografia é privada (conhecida só pelo receptor).

Criptografia com Chave Pública



Criptografia com Chave Pública



Como funciona a cripto assimétrica

Algoritmo de criptografia assimétrica RSA

- e_b = Chave criptográfica **pública**.
- d_b = Chave criptográfica **privada**.
- m = mensagem

$[\ e_b(m)\ ]$ = **Texto cifrado.**

Aplicar a chave pública sobre a msg e obter uma msg cifrada.

Algoritmo de criptografia assimétrica RSA

- e_b = Chave criptográfica **pública**.
- d_b = Chave criptográfica **privada**.
- m = mensagem [$e_b(m)$] **= Texto cifrado.**

Duas exigências correlatas:

$$d_b\,[\,(\,e_b(m)\,]\,=\,m$$

- Aplicando a chave **pública** e, **em seguida**, a **chave privada**, à mensagem *m*, recuperamos *m*, para qualquer mensagem *m*.

$$e_b\,[\,d_b(m)\,]\,=\,d_b\,[\,e_b(m)\,]\,=\,m$$

A reversão é verdadeira.

Escolha das chaves
RSA: Algoritmo de Rivest, Shamir & Adleman.

1. Encontre dois números primos muito grandes ***p, q***
   - Por exemplo com 1024 bits cada um.
2. Calcule $n = p.q$ e $z = (p-1).(q-1)$
3. Escolha "***e***" *(com* $e < n$*)* que não tenha fatores primos em comum com z, exceto o 1.

   ou seja, ***e*** e ***z*** são ditos "**primos entre si**".
3. Escolha ***d*** tal que (***ed−1***) é divisível **exato** por *z*.
   - Ou seja: **não há resto** na divisão de ***(e.d-1)*** por ***z*** → **resto zero*:***
   - ***(e.d-1) mod z = 0 → (e.d) mod z = 1 :***
   - Dado ***e*** escolhemos ***d*** , tal que o **resto** da divisão de ***e.d*** por ***z*** seja ***1***.

- **Chave *Pública* é o par *(n,e).***
- **Chave *Privada* é o par *(n,d).***

Note que ***n*** é comum às duas chaves.

RSA: Criptografia e Decriptografia

1. Dado chaves **(*n*,*e*)** e **(*n*,*d*)** como mostrado antes.

2. Para **criptografar** o padrão de bits ***m*** calcula-se:

$C = m^e \bmod n$ (i.e., resto quando m^e é dividido por n)

3. Para **decriptografar** o padrão de bits recebidos, c :

$m = C^d \bmod n$ (i.e., resto de c^d quando é dividido por n)

Mágica acontece!

$$m = (\underbrace{m^e \bmod n}_{C})^d \bmod n$$

C → Mensagem cifrada

Exemplo RSA:

- Bob escolhe *p=5*, *q=7*.
- Então *n=35*, *z=24*.
- *e = 5* (assim ***e***, ***z*** são primos entre si).
- *d = 29* (assim ***ed–1*** é exatamente divisível por z)

e.d – 1 =5x29 – 1 = 144 / 14 = 6

	letra	m	m^e	$c = m^e \bmod n$
criptografia:	L	12	248832	17

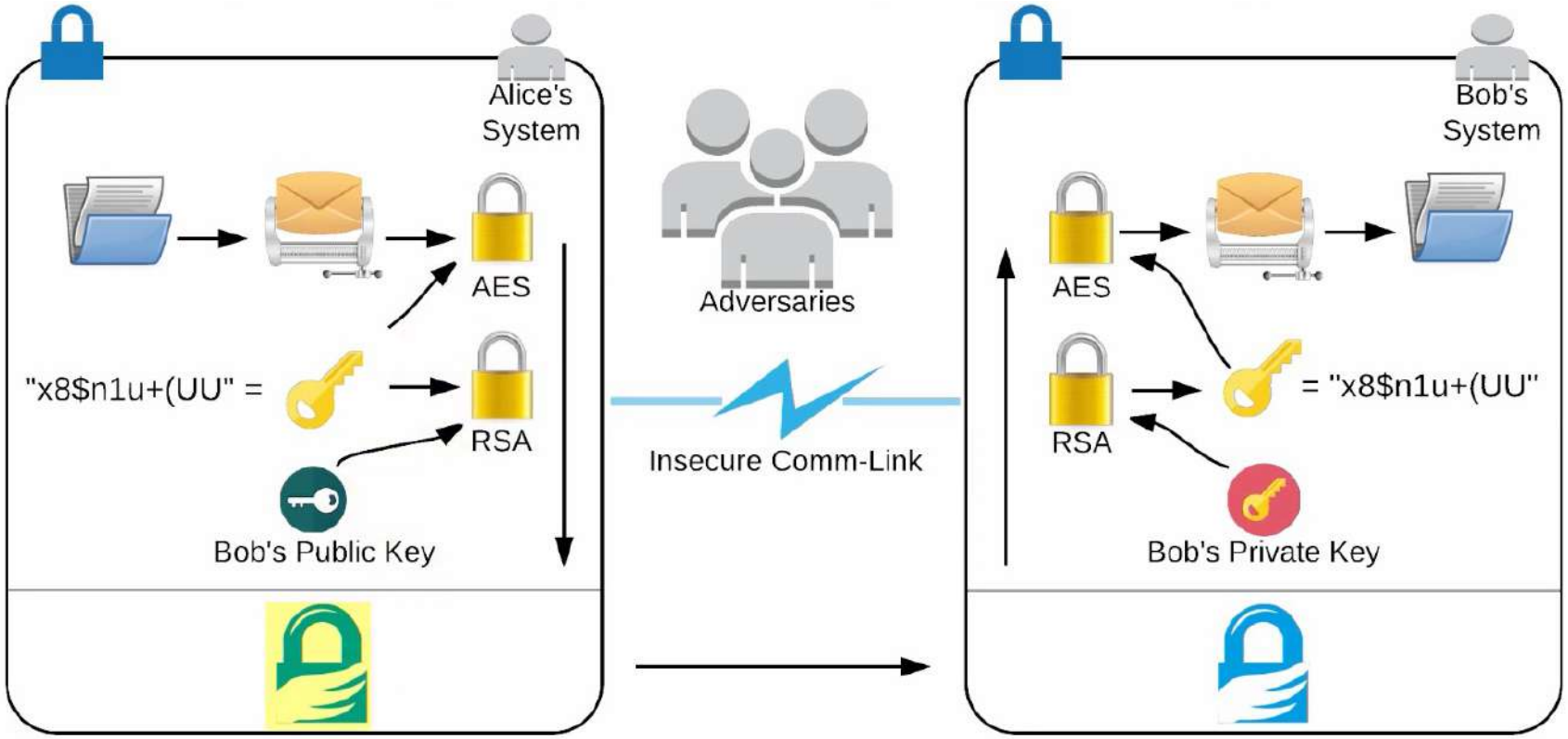
	c	c^d	$m = c^d \bmod n$	letra
decripto:	17	48196857210675091509141182522307200 0	12	L

Pretty Good Privacy (PGP)

- Híbrido:

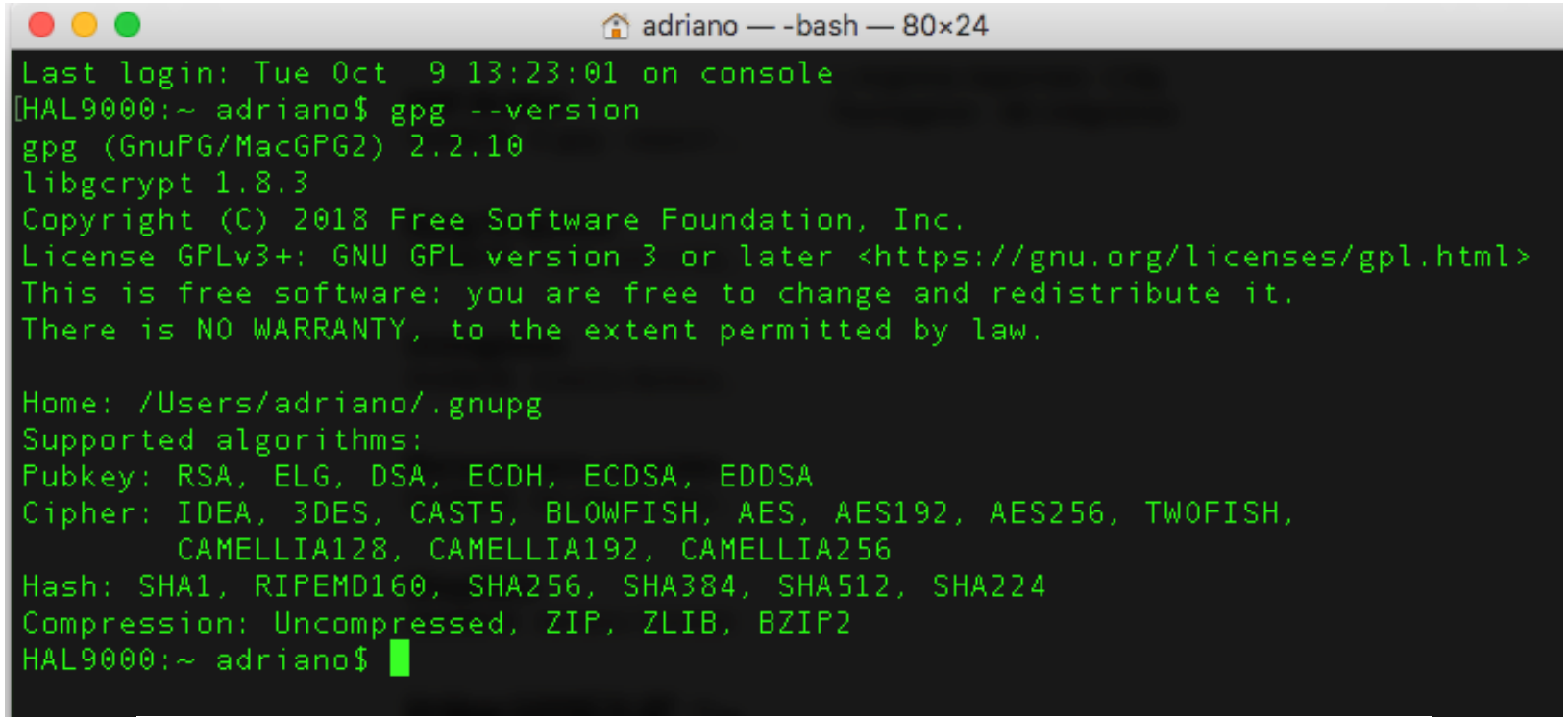
  Combina criptografia de chave simétrica e assimétrica.
- Possui recursos de função de *hash* e assinatura digital.
- Oferece privacidade, autenticação do transmissor e integridade.
- O inventor, Phil Zimmerman foi alvo de uma investigação federal durante três anos.

O PGP é híbrido:



Créditos Figura: https://youtu.be/3dybuC_XxCQ

PGP pode usar diversos algoritmos simétricos



Cypher: 3DES, CAST5, BLOWFISH, AES, AES192, AES256,

TWOFISH, CAMELLIA128, CAMELLIA192, CAMELLIA256, etc…

Algoritmos assimétricos ou de chave pública

- Curvas elípticas
- Diffie-Hellman
- DSA de curvas elípticas
- El Gamal
- RSA

Referências

- "Redes de Computadores", Kurose & Ross. 6a. Edição, Cap. 8 – Seção 8.2
- "O Livro dos Códigos", Simon Singh (esgotado em português), ou "*The Code Book*" em inglês.
- "*Foundations of Cryptography: Volume 1, Basic Tools*". Oded Goldreich. Cambridge University Press; 1st edition (August 21, 2008).
- "O que é uma cifra de bloco e como ela funciona para proteger seus dados?". Megan Kaczanowski. CryptoID, 07/07/2021.

Obrigado!

Adriano Cansian, Prof. Dr.

adriano.cansian@unesp.br

Linkedin: *@adrianocansian*

PGP KeyID: 0x3893CD2B

unesp

Professor Associado