Criptografia:

o que é, aplicações e futuro

Thaís Bardini Idalino - INE - UFSC

Meetup Pyladies Floripa - 2023

Minha trajetória na computação

2009 - 2012
Graduação em CCO

2013 - 2015
Mestrado PPGCC

2015 - 2019
Doutorado em CCO

2019 - 2021
Pós-Doc SFU

2021
Prof INE

UFSC

UFSC

uOttawa
Faculté de génie
Faculty of Engineering

SFU

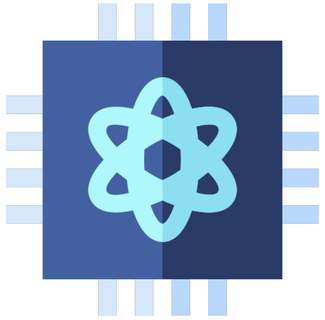
UFSC

https://www.linkedin.com/in/thaisidalino/
https://thaisidalino.github.io/

Qual o significado desse texto?

Khoor Zruog

Uma breve história da criptografia



Criptografia Clássica

Criptografia Moderna

Futuro

1900 AC - 1970

1970 - Hoje

Hoje - 20??

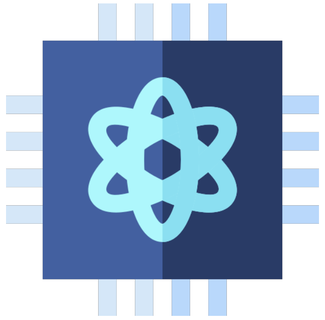
Criptografia

- Texto claro
- Texto cifrado
- Algoritmos de cifragem e decifragem
- Chave secreta

Criptoanálise

- Ataque da natureza do algoritmo (pontos fracos)
- Ataque das características do texto (claro e cifrado)
- Força bruta

Uma breve história da criptografia



Criptografia Clássica

1900 AC - 1970

Criptografia Moderna

1970 - Hoje

Futuro

Hoje - 20??

Criptografia Clássica

- O objetivo era **confidencialidade**

Criptografia Clássica

- O objetivo era **confidencialidade**
- Técnicas de *transposição*
  - Embaralhar as letras
  - Gregos
- Técnicas de *substituição*
  - Substituir uma letra por outra
  - Roma antiga

Olá Mundo

↓

Odnum Alo

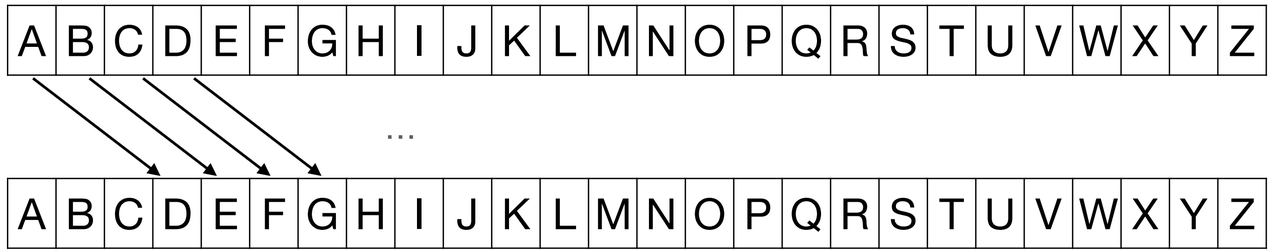
A B C …

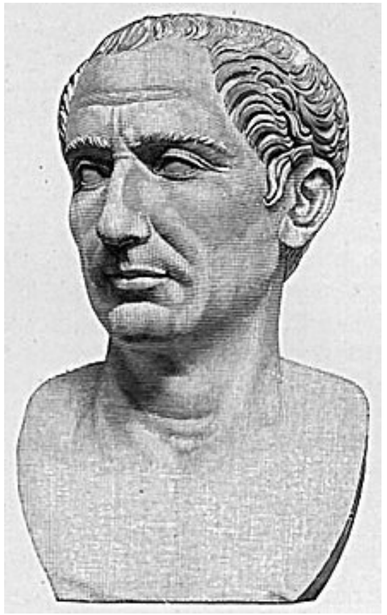
↓ ↓ ↓

B J F

Substituição

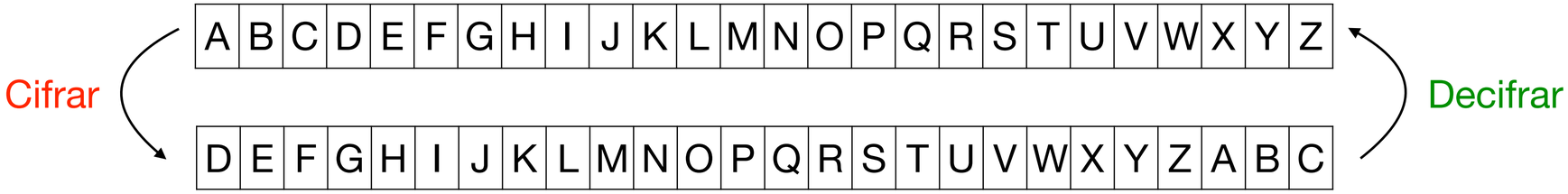
Cifra de César 100-44 BC

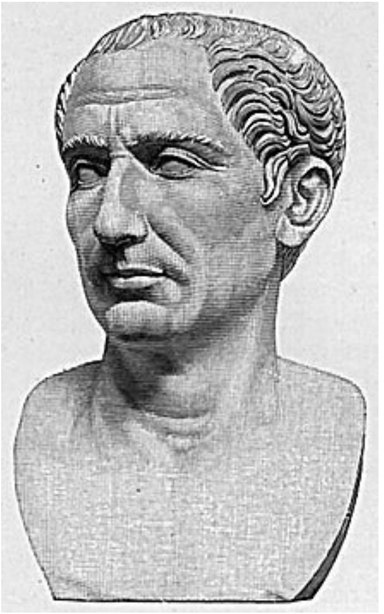




Cifra de César

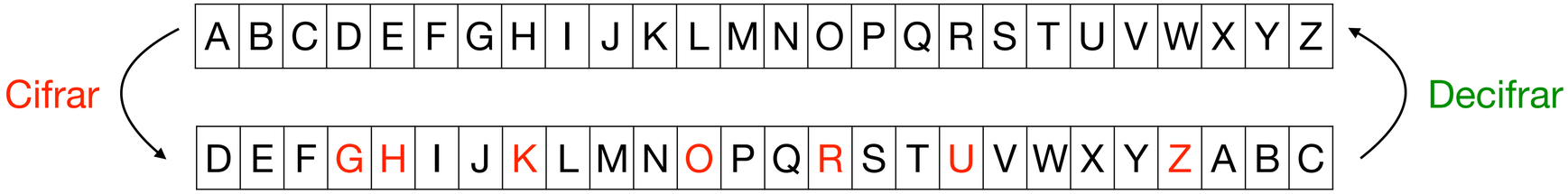
100-44 BC



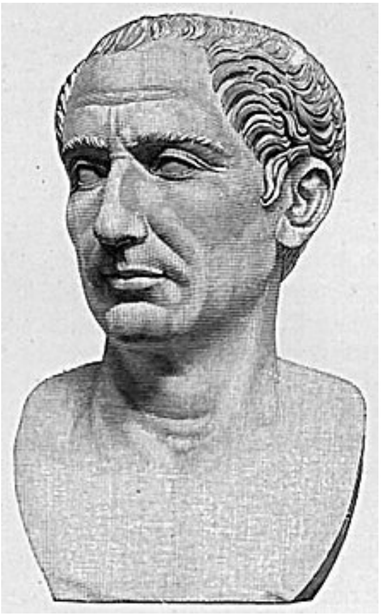


Cifra de César

100-44 BC

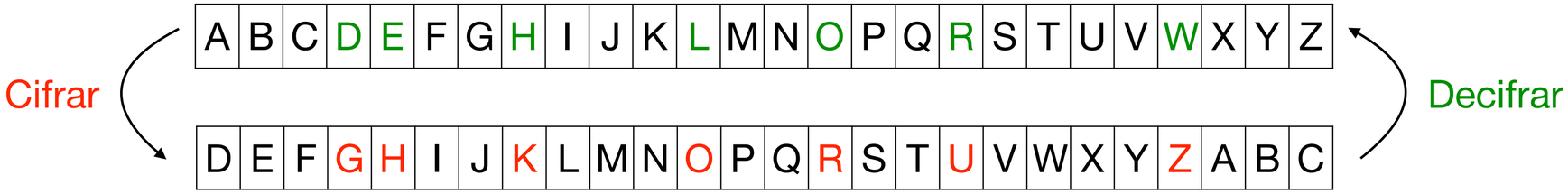


Khoor Zruog



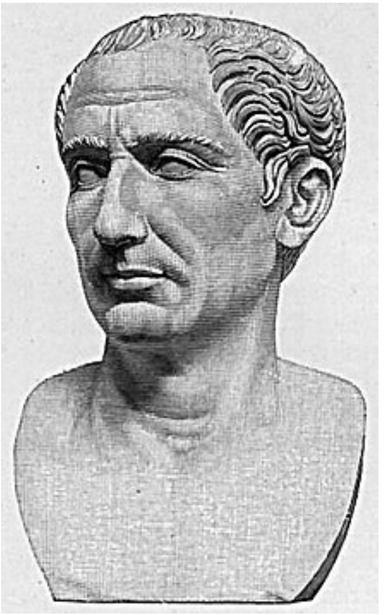
Cifra de César

100-44 BC



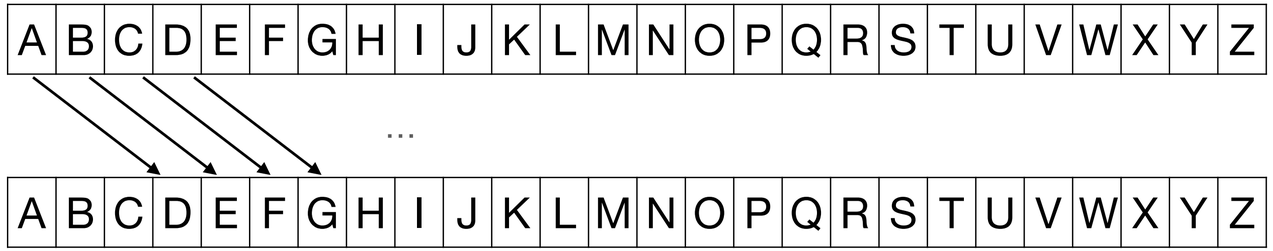
Khoor Zruog

Hello World

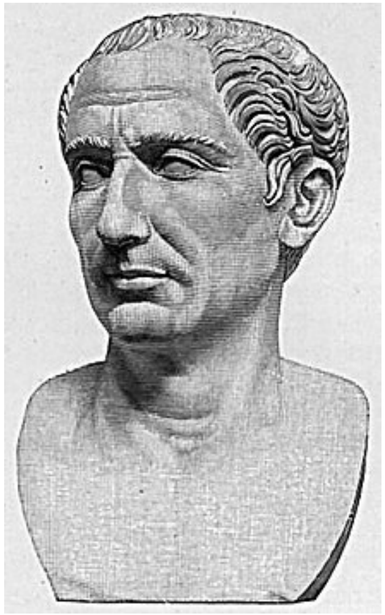


Cifra de César

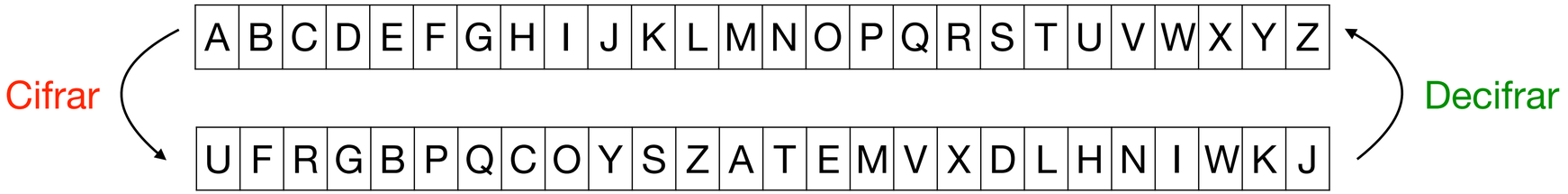
100-44 BC



- **César**: Adiantar 3 letras pra frente no alfabeto
- **Outras alternativas**: adiantar 1, 2, 3, 4, 5, …., 25
- **Criptoanálise por força-bruta**: testar todas as 25 opções



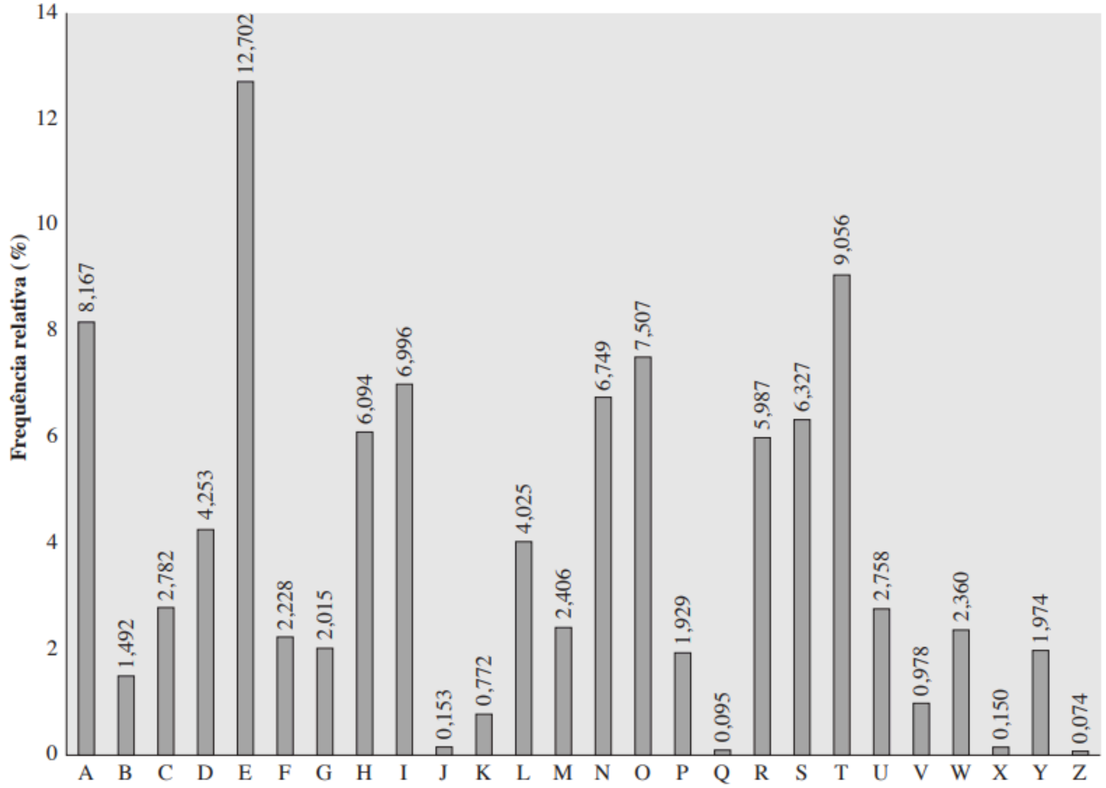
Cifradores mono-alfabéticos



- Espaço de chave: $26! \approx 4 \times 10^{26}$
- Força bruta é muito difícil
- Chave = alfabeto escolhido

Cifradores mono-alfabéticos

- Criptoanálise de frequência



Fonte: Segurança de Computadores: Princípios e Práticas
Stallings

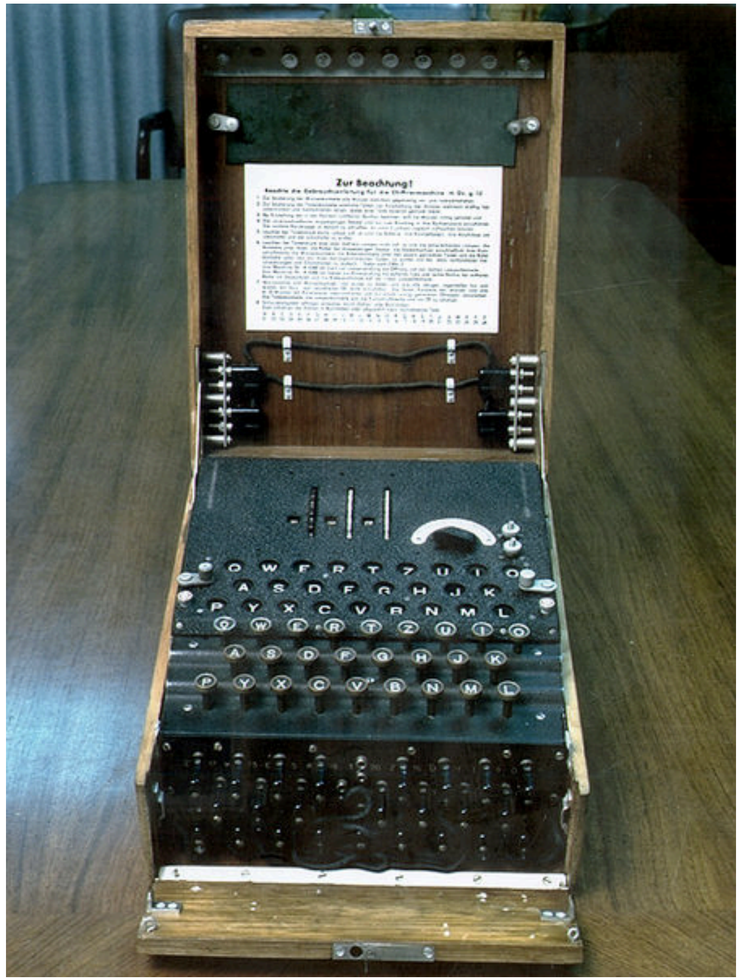
Substituição

- Playfair
- Vigenère
- Cifradores poli-alfabéticos
- One-time pad
- E muito mais…

Enigma

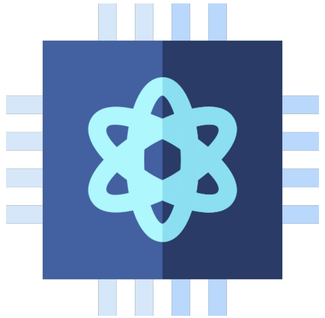
1920

- Máquina eletromecânica utilizada na segunda guerra mundial
- Cada cilindro é um cifrador monoalfabético
- Alan Turing e outros cientistas desenvolveram uma máquina para decifrar mensagens da enigma



Sede da inteligência Britânica - Bletchley Park

Uma breve história da criptografia



Criptografia Clássica

Criptografia Moderna

Futuro

AC - 1970

1970 - Hoje

Hoje - 20??

Condição fundamental

Um sistema de criptografia deve ser seguro ainda que o adversário conheça todos os detalhes do sistema, com exceção da chave secreta.

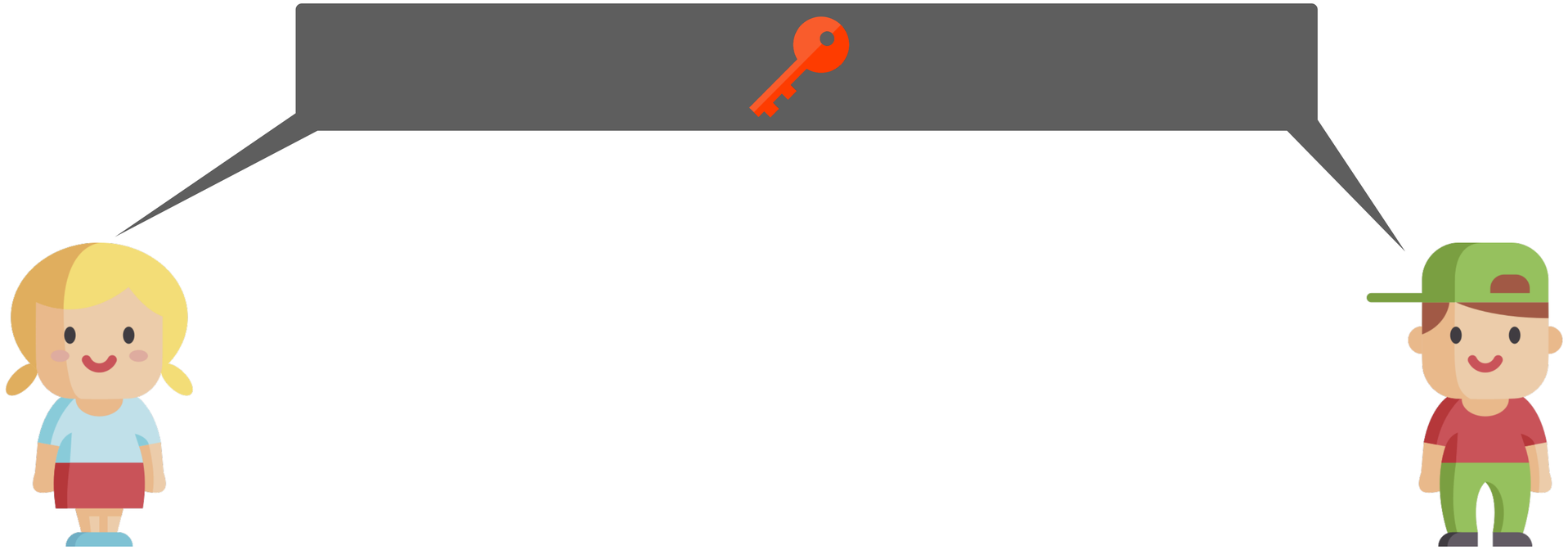
Auguste Kerckhoffs, 1883

Criptografia moderna

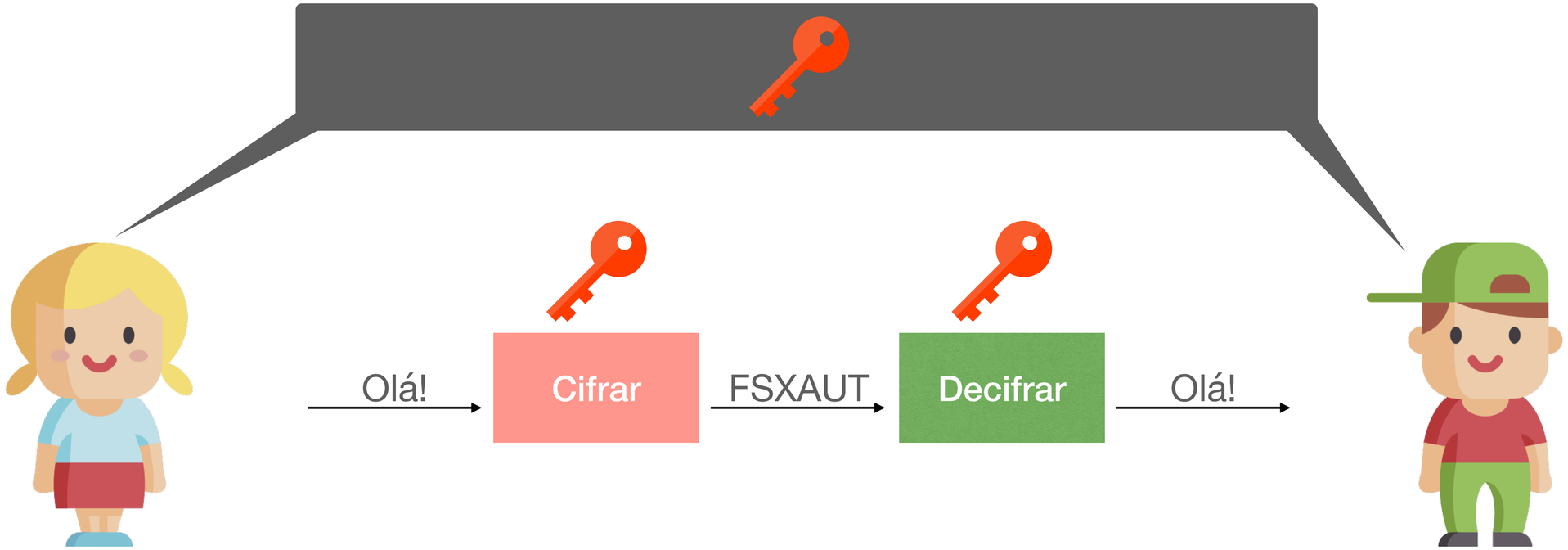
- Criptografia simétrica 
- Criptografia assimétrica 
- Novos objetivos:
  - Confidencialidade 

  - Autenticidade 
  - Não-repúdio 
  - etc.

Criptografia simétrica



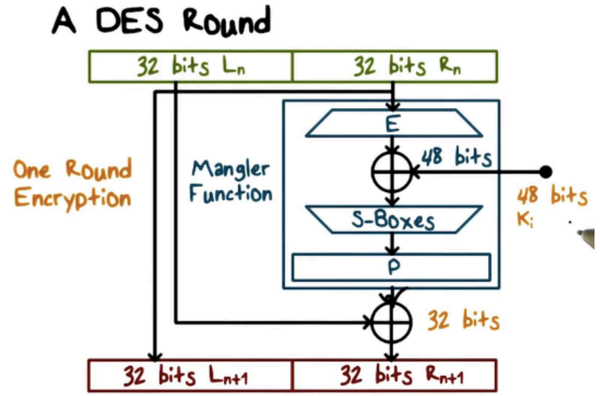
Criptografia simétrica



Criptografia simétrica

1976

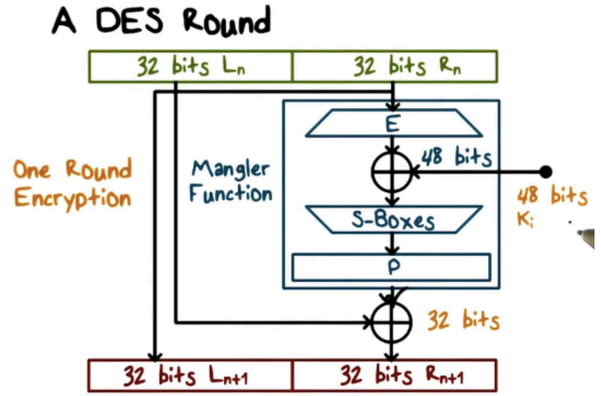
- Data Encryption Standard (DES)
  - Primeiro padrão criptográfico eletrônico
  - Permutações, substituições e XORs
  - Chaves de 56 bits

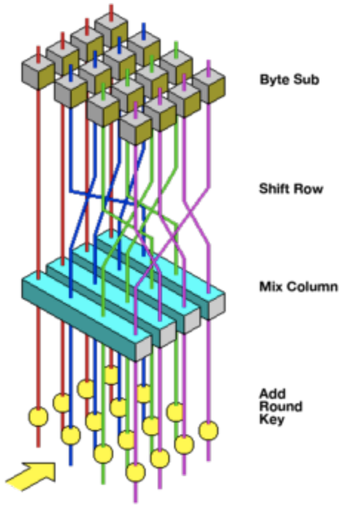


Criptografia simétrica

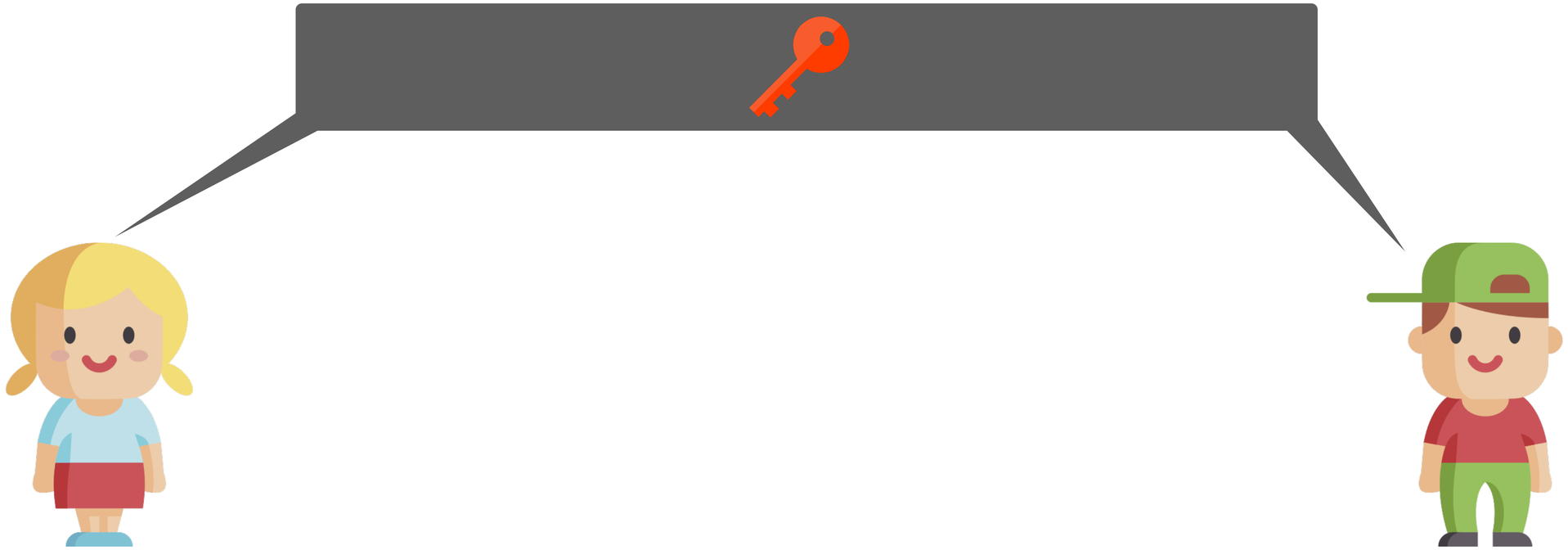
2001

- Data Encryption Standard (DES)
  - Primeiro padrão criptográfico eletrônico
  - Permutações, substituições e XORs
  - Chaves de 56 bits
- Advanced Encryption Standard (AES)
  - Chaves de 128, 192 e 256 bits
  - Simples, eficiente

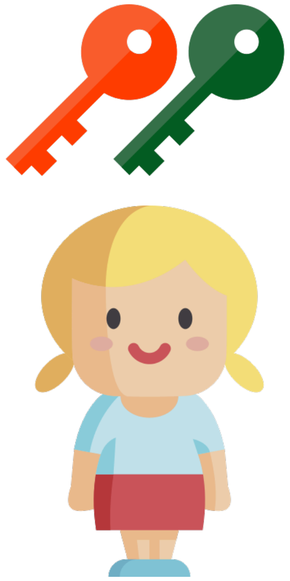




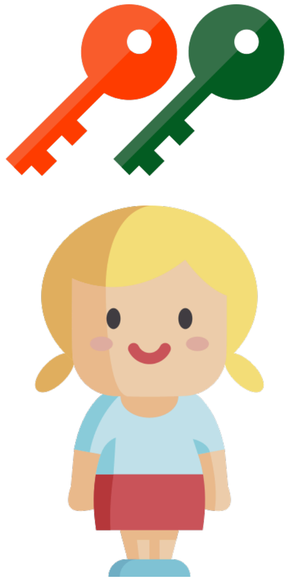
Criptografia simétrica

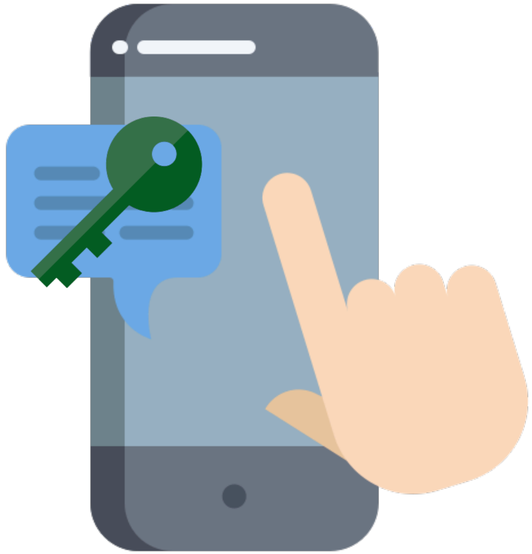


Criptografia assimétrica

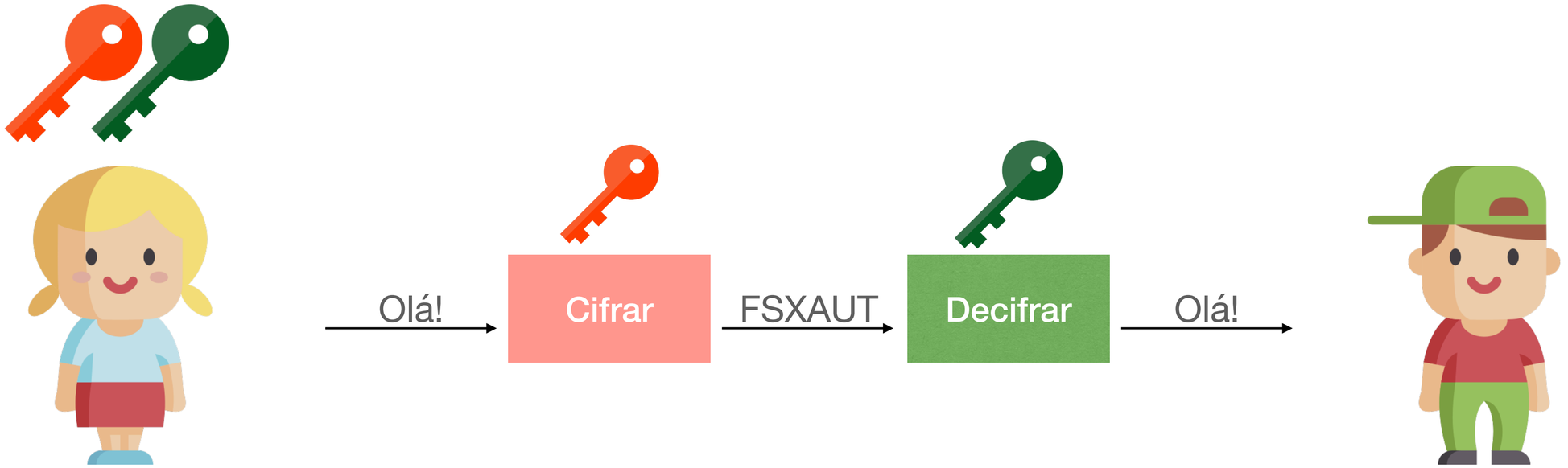


Criptografia assimétrica

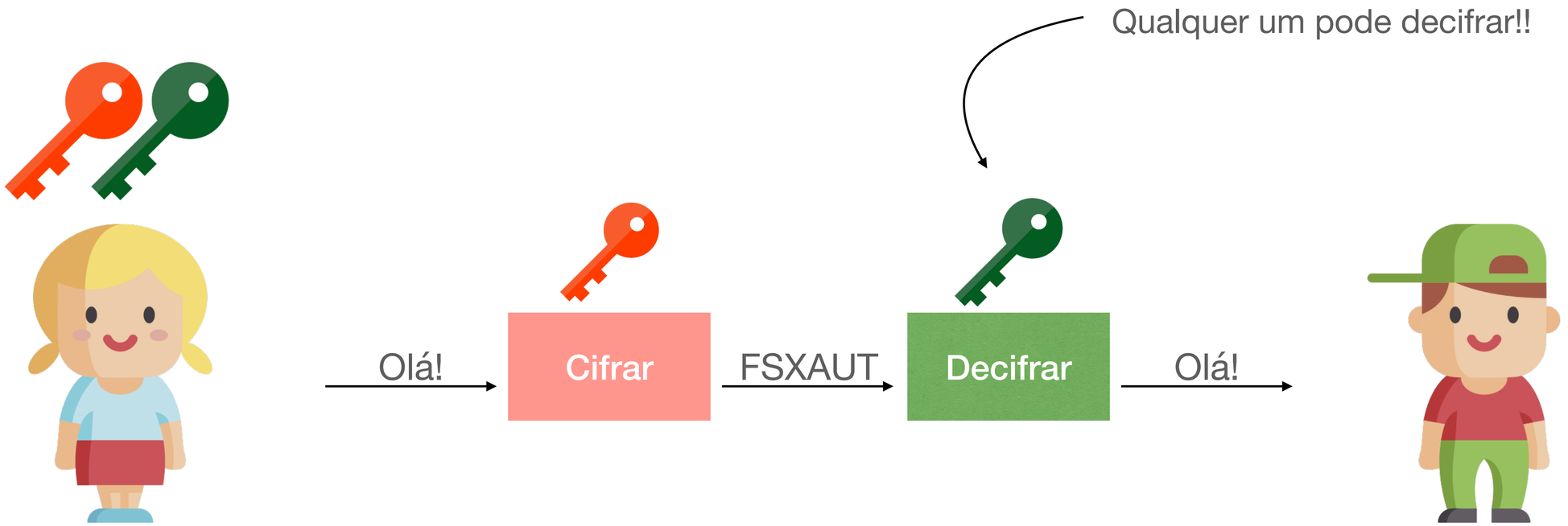




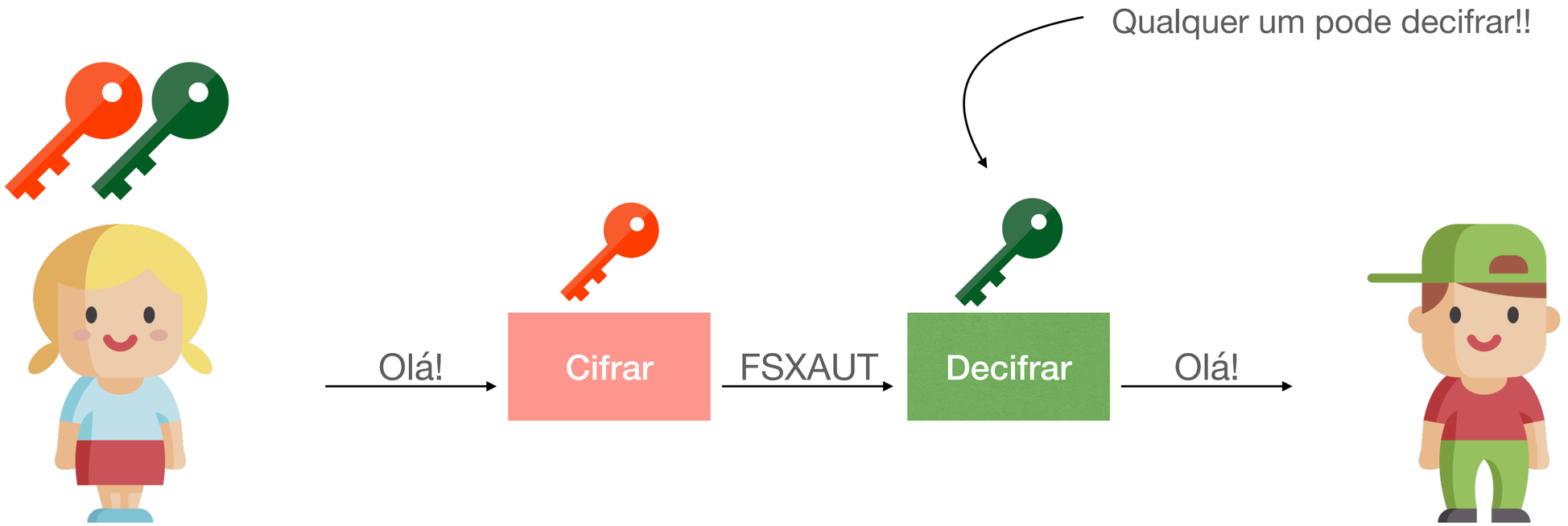
Criptografia assimétrica



Criptografia assimétrica

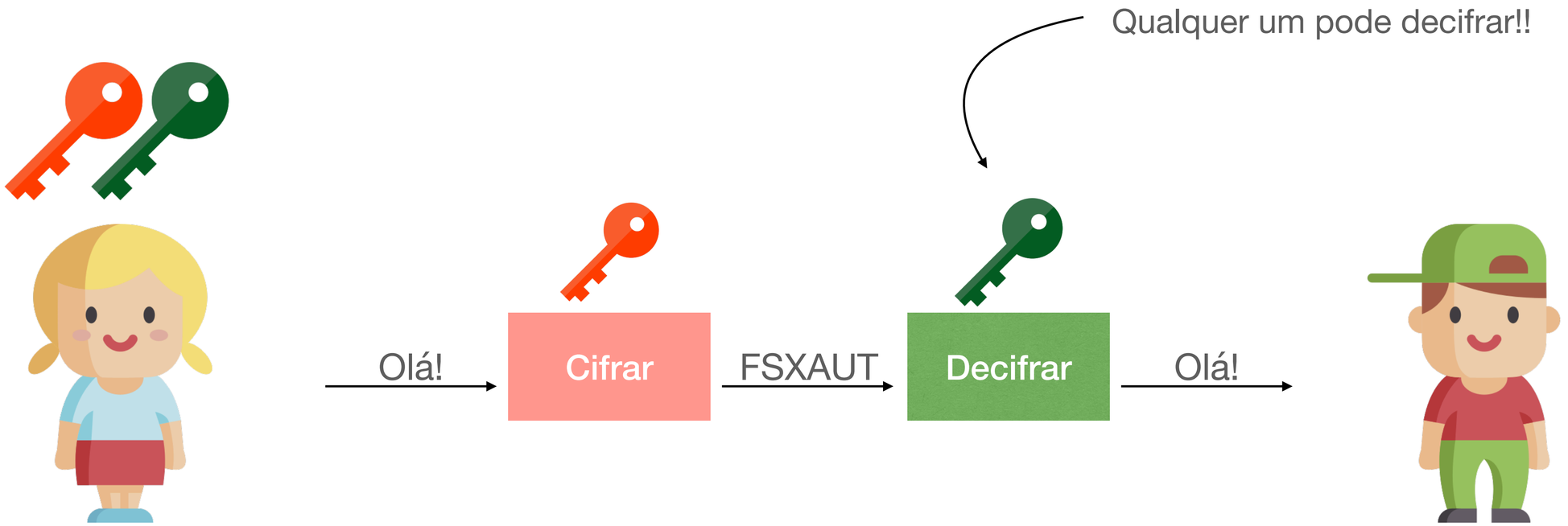


Criptografia assimétrica



Autenticidade: Temos certeza que a mensagem veio da Alice

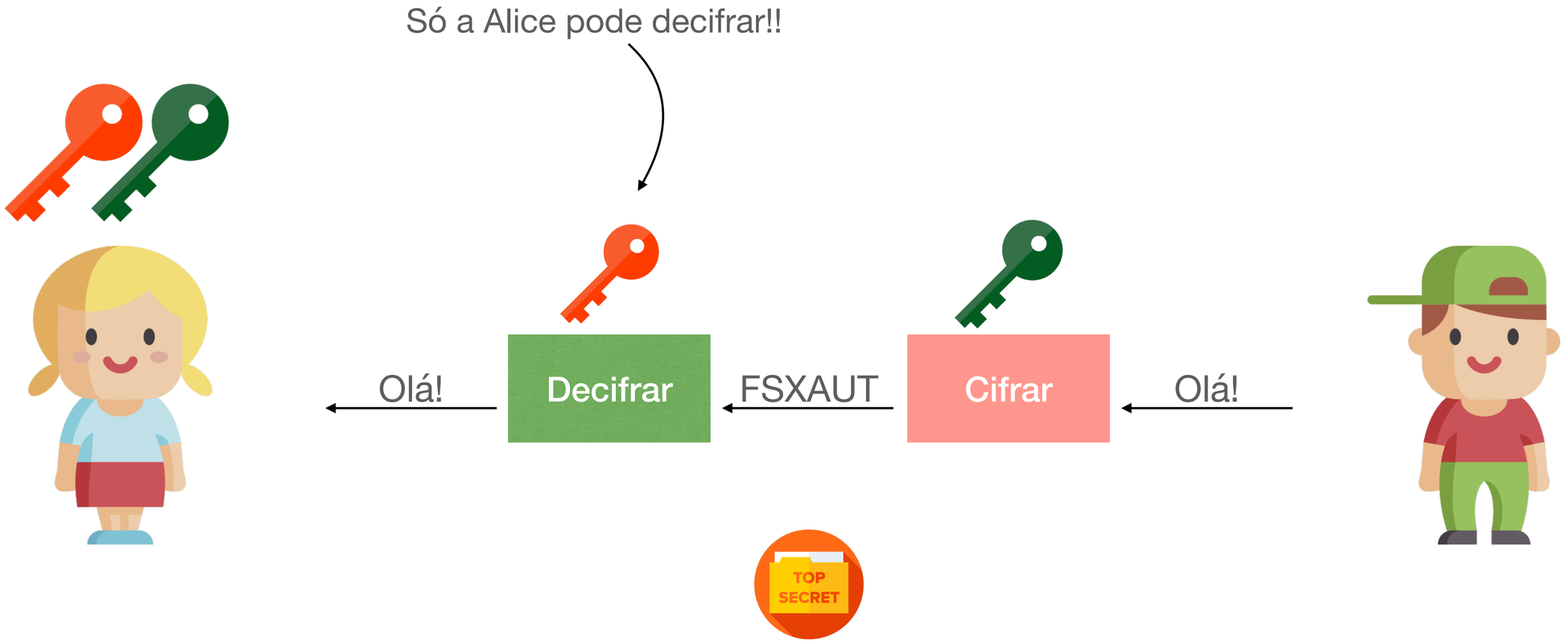
Criptografia assimétrica



Autenticidade: Temos certeza que a mensagem veio da Alice

Não-repúdio: Alice não pode negar ter assinado a mensagem

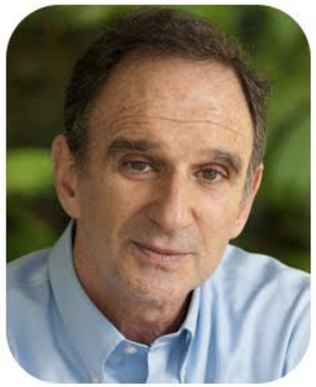
Criptografia assimétrica

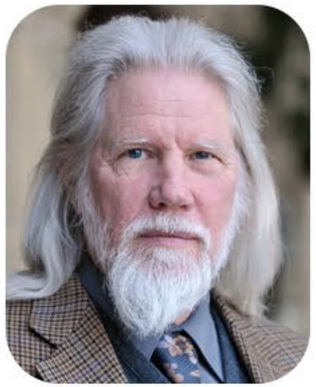


Criptografia assimétrica

1976

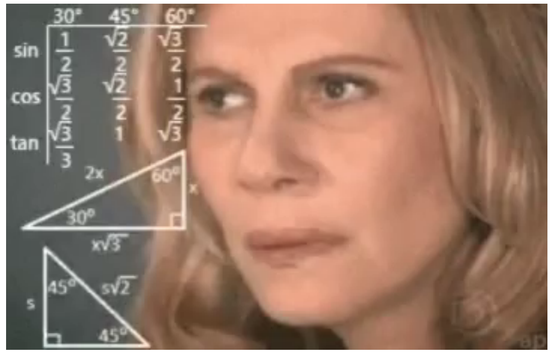
- Idealizada por Diffie e Hellman (1976)
- Criação do criptossistema RSA por Rivest, Shamir e Adleman (1977)





RSA

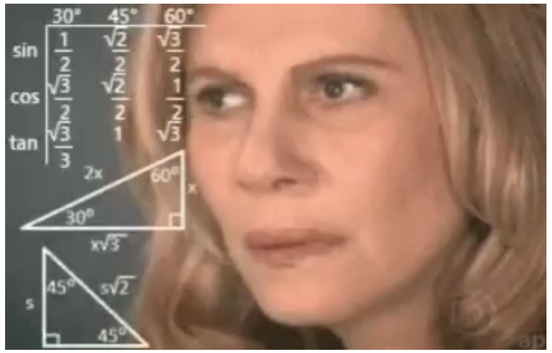
1977



- Usa números **primos** na criação das chaves
- Segurança baseada na **dificuldade de fatoração**
- Cifragem e decifrarem são operações de exponenciação modular

RSA

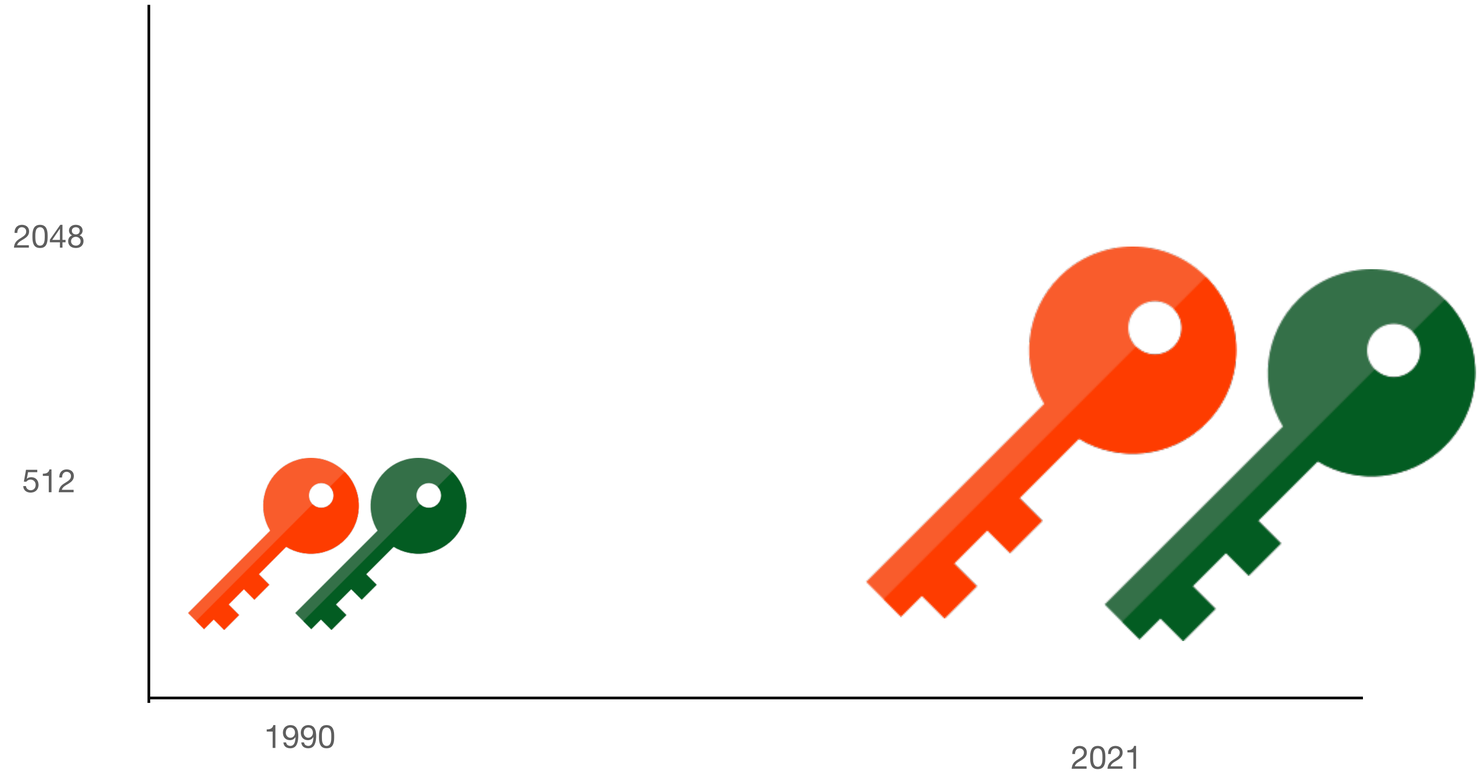
1977



- Usa números **primos** na criação das chaves
- Segurança baseada na **dificuldade de fatoração**
- Cifragem e decifrarem são operações de exponenciação modular
  - c = m mod n
  - m = c mod n

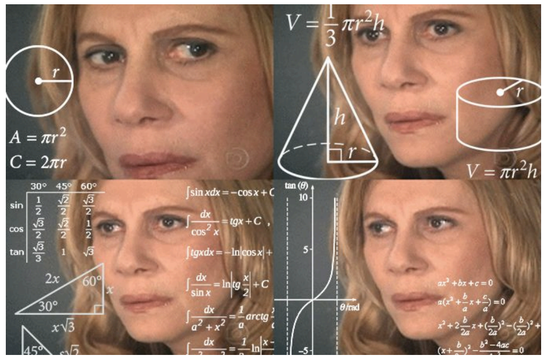
- Chaves de 1024 e 2048 bits

Problema de criptografia assimétrica

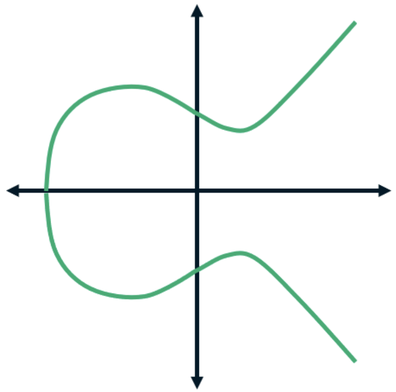


ECDSA

2005



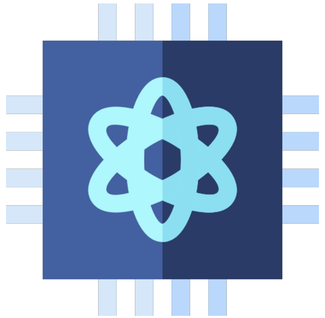
- Mesma segurança do RSA, mas com chaves **muito** menores
  - RSA com 2048 bits **vs** ECDSA com 224 bits
- São usadas nas transações de bitcoin para garantir que as moedas possam ser gastas apenas por seus donos



Criptografia moderna

- Criptografia simétrica 🔑
- Criptografia assimétrica 🔑🔑

Uma breve história da criptografia



Criptografia Clássica

Criptografia Moderna

Futuro

1900 AC - 1970

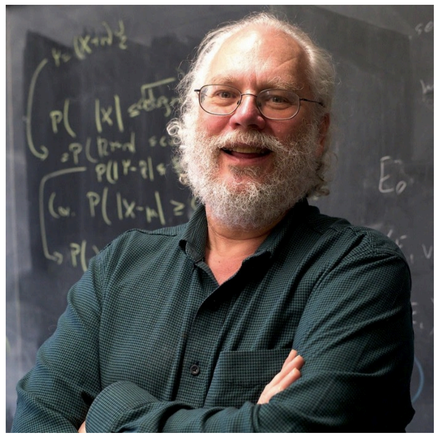
1970 - Hoje

Hoje - 20??

Criptografia no futuro

1996

- Grande ameaça apresentada por Peter Shor
- Algoritmos que conseguem quebrar a **criptografia assimétrica**

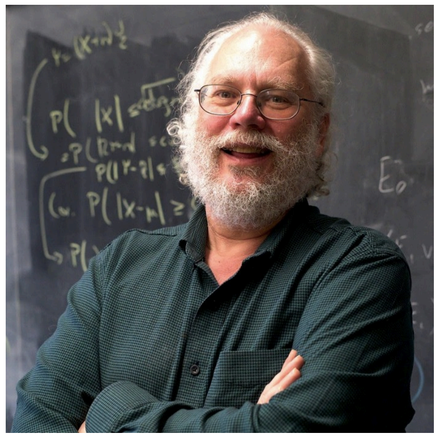


Peter Shor

Criptografia no futuro

1996

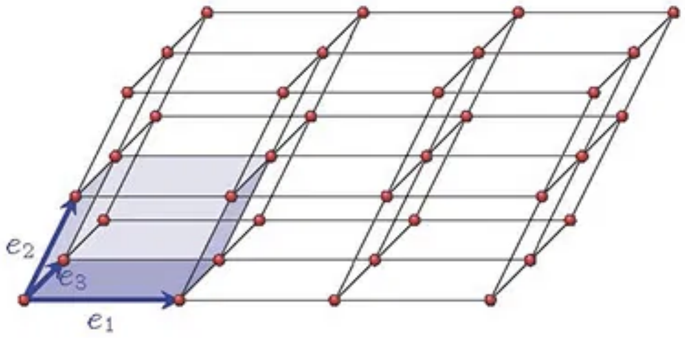
- Grande ameaça apresentada por Peter Shor
- Algoritmos que conseguem quebrar a **criptografia assimétrica**
- Os algoritmos só funcionam se tivermos **computadores quânticos**
- Computador quântico da IBM conseguiu fatorar o número **15** com esse algoritmo



Peter Shor

Criptografia no futuro

- Pesquisa extensa em criptografia pós-quântica
  - Segurança baseada em outros problemas matemáticos



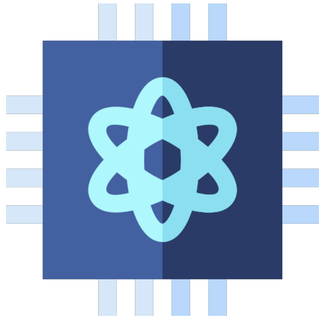
Criptografia no futuro

- Competição do NIST
  - Cifragem e decifragem: CRYSTALS-Kyber
  - Assinatura digital: CRYSTALS-Dilithium , FALCON e SPHINCS+
- Está tudo resolvido então?

Criptografia no futuro

- Competição do NIST
  - Cifragem e decifragem: CRYSTALS-Kyber
  - Assinatura digital: CRYSTALS-Dilithium , FALCON e SPHINCS+
- Está tudo resolvido então?
  - Diminuir chaves
  - Diminuir assinatura
  - Melhorar desempenho
  - NIST abriu o processo novamente para novos candidatos

Uma breve história da criptografia



Criptografia Clássica

Criptografia Moderna

Futuro

1900 AC - 1970

1970 - Hoje

Hoje - 20??

Reuljdgd!

Reuljdgd!

Obrigada!