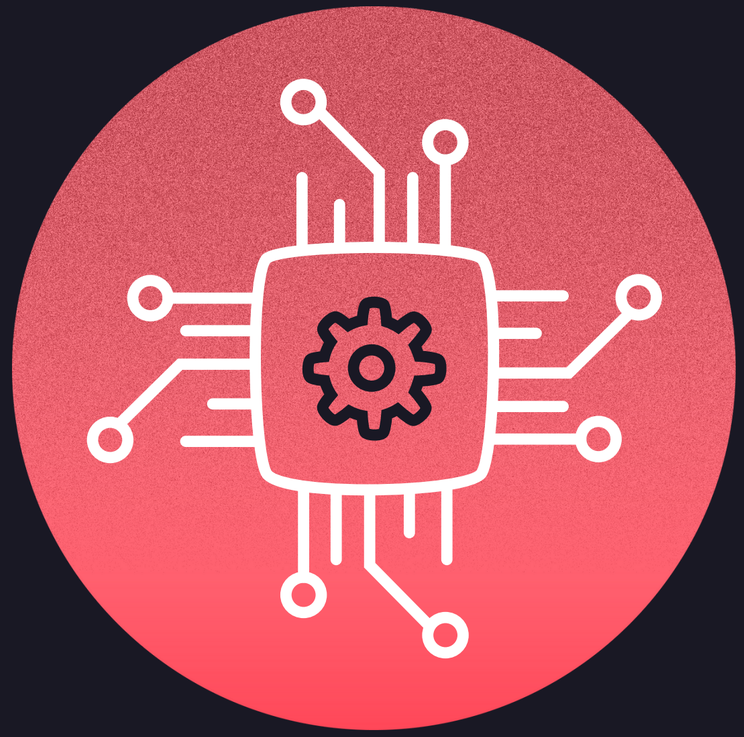
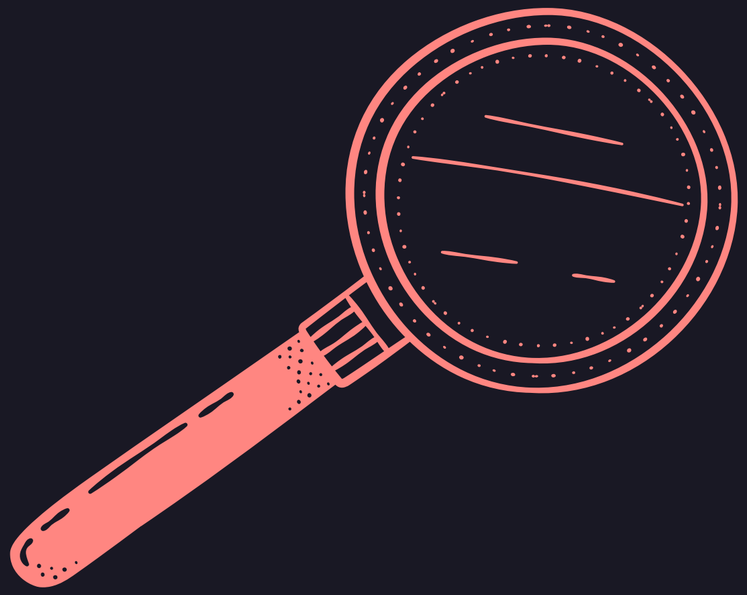


Computação Quântica: Algoritmo de Shor

Bruna Shinohara - Doutoranda em Física - USP
Arthur Faria- Doutorando em Física - UNICAMP/ U. of Stuttgart

- O que é um protocolo de criptografia?
- Problemas NP
- Algoritmo de Shor - passos
- Versão quântica
  - transformada de Fourier quântica
  - estimativa de fase quântica
- Implementação em Qiskit

O QUE É UM PROTOCOLO DE CRIPTOGRAFIA?



O QUE É UM PROTOCOLO DE CRIPTOGRAFIA?

É alguma função na qual se transforma uma mensagem em alguma outra mensagem, de forma em que a comunicação seja privada.

- Trocar letras por outras letras, ou um conjunto de letras, seguindo um padrão
- Dificultar a visualização da mensagem (estenografia)

Entre outros.

Fonte: https://null-byte.wonderhowto.com/how-to/steganography-hide-secret-data-inside-image-audio-file-seconds-0180936/

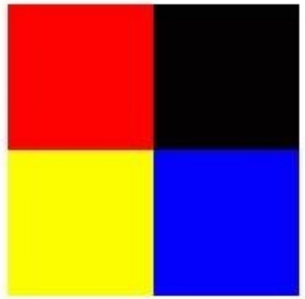
Original Image

```
11111111  00000000
00000000  00000000
00000000  00000000

11111111  00000000
11111111  00000000
00000000  11111111
```

Least Significant Bit Steganography

Stego Image

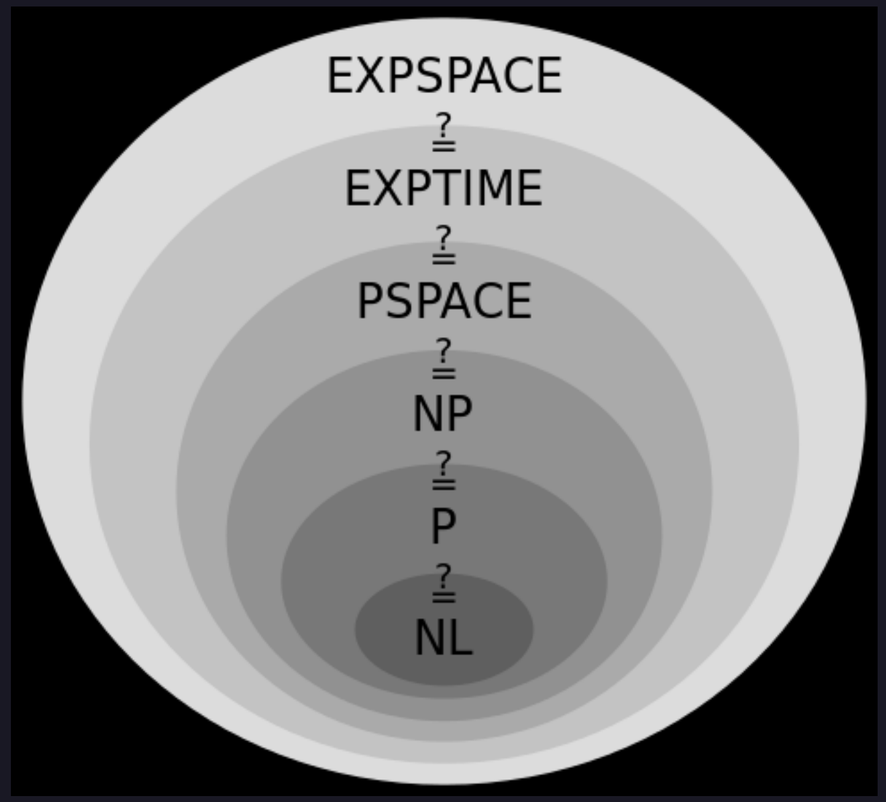


```
11111101  00000011
00000010  00000001
00000000  00000010

11111100  00000011
11111101  00000001
00000001  11111100
```

c	a	t
01 10 00 11	01 10 00 01	01 11 01 00

COMO FAZER UM PROTOCOLO?



Em geral, busca-se um problema matemático que seja considerado “difícil”, até para uma máquina, de forma em que a quebra da criptografia demore um tempo impraticável.

Na prática, problemas tipo "NP" (fácil de testar uma resposta que já se saiba, difícil de achar solução em tempo hábil).

SIMÉTRICA VERSUS ASSIMÉTRICA

Na simétrica, utiliza-se a mesma chave para criptografar e decifrar. Na assimétrica, chaves diferentes.

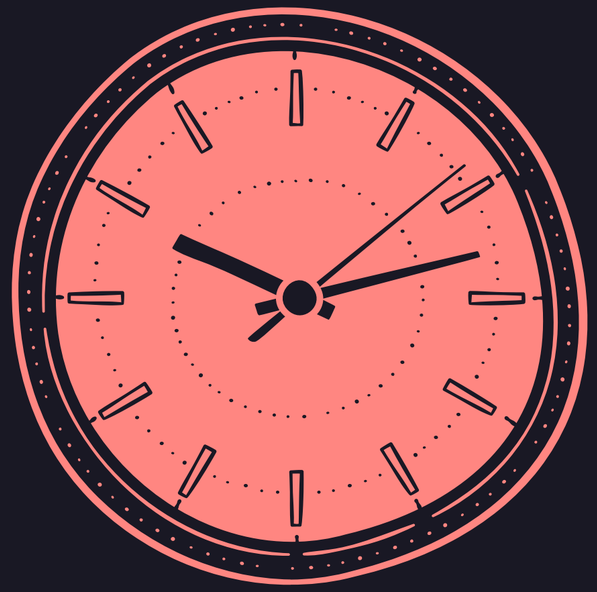
A Assimétrica é mais segura, mas a simétrica funciona melhor para grandes fluxos de informação (ex: AES)

DOIS PROBLEMAS NP IMPORTANTES

- Logaritmo discreto de curva elíptica (ECDLP)
- Fatoração em primos

São problemas diferentes, mas ambos envolvem aritmética modular.

RELEMBRANDO: ARITMÉTICA MODULAR



$x = y \pmod N$

Exemplo:
$15 = 3 \pmod N$
(15 horas = 3horas, nossos relógios seguem aritmética mod 12)

Relacionado a operação de módulo (%), que retorna o resto de uma divisão inteira.

Exemplo: 15 % 4 = 3

ALGORITMO DE SHOR

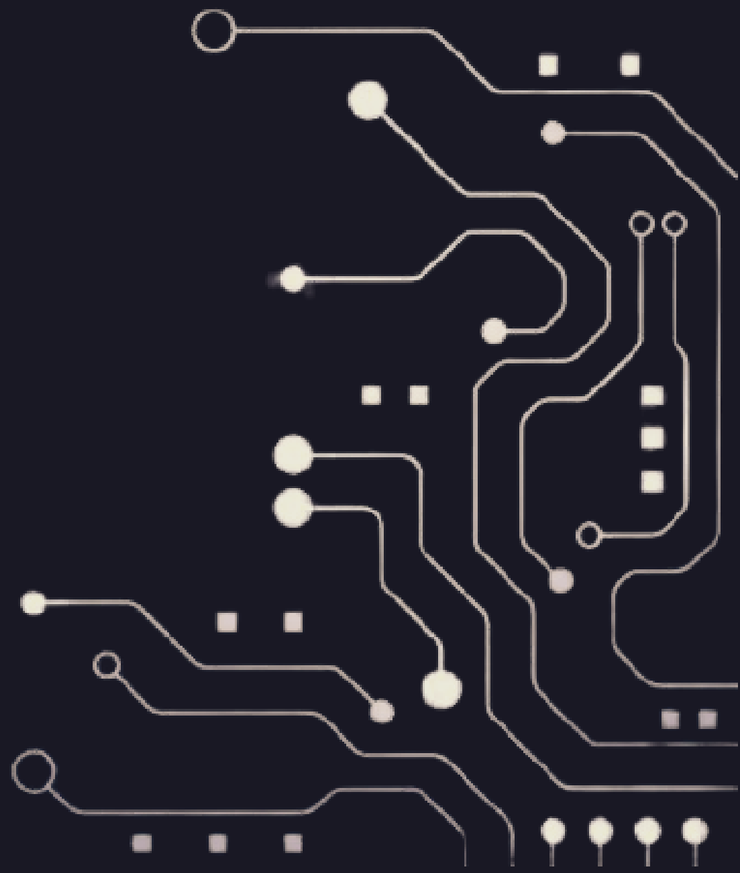
ALGORITMO DE SHOR

O algoritmo de Shor resolve mais rapidamente o problema de fatoração de primos.

O problema consiste na decomposição de um número em multiplicação de números que sejam primos, e não há forma rápida de fazer isso.

Essa é a base pra criptografia RSA, uma das mais importantes criptografias assimétricas atuais.

PASSOS DO ALGORITMO DE SHOR



Passos do algoritmo de Shor

Dado um número N que queremos fatorar, os passos do algoritmo são

1. Escolher um número a < N que seja coprimo de N:

$$\mathrm{MDC}(N, a) = 1.$$

2. Encontrar a ordem r. A ordem é definida como o menor número natural que satisfaça:

$$a^r = 1 \bmod N$$

3. Se r for ímpar ou

$$a^{r/2} = -1 \bmod N,$$

escolhe-se outro número.

4. Se r for par, temos que

$$\{\mathrm{MDC}(a^{r/2} + 1), \mathrm{MDC}(a^{r/2} - 1)\}$$

São dois divisores não-triviais de N.

N = 15

1. Escolher um número a < N que seja coprimo de N: vamos escolher $a = 13$.
2. Encontrar a ordem r, tal que

$$13^r = 1 \mathrm{mod} 15$$

Vamos testar diferentes valores de r:

$$13^1 = 13 \mathrm{mod} 15$$
$$13^2 = 4 \mathrm{mod} 15$$
$$13^3 = 7 \mathrm{mod} 15$$
$$13^4 = 1 \mathrm{mod} 15$$
$$13^5 = 13 \mathrm{mod} 15$$
$$13^6 = 4 \mathrm{mod} 15$$
$$\ldots$$

Vemos que r = 4 satisfaz a condição.

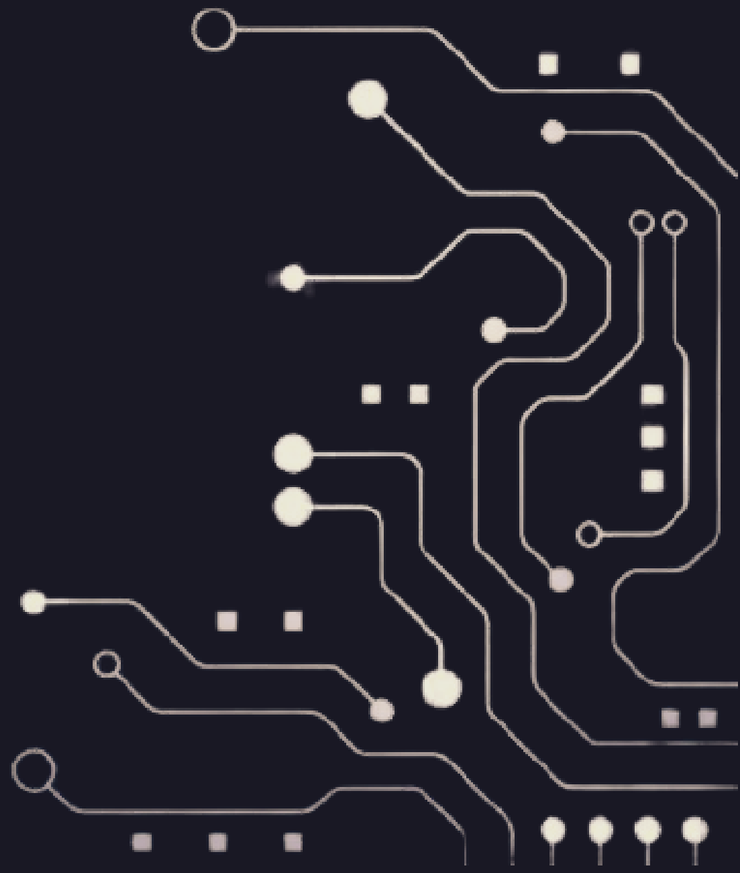
3. Temos que

$$\{\mathrm{MDC}(13^{4/2} + 1), \mathrm{MDC}(13^{4/2} - 1)\}$$
$$= \{5, 3\}$$

São dois divisores não-triviais de 15.

VERSÃO QUÂNTICA

- Quantum Phase Estimation (QPE)
- Quantum Fourier Transform (QFT)



Obrigada!

Perguntas?