Criptografia e Criptografia pós quântica

Bryan, Esdras, Ramon, Gustavo Mota e Jonathan

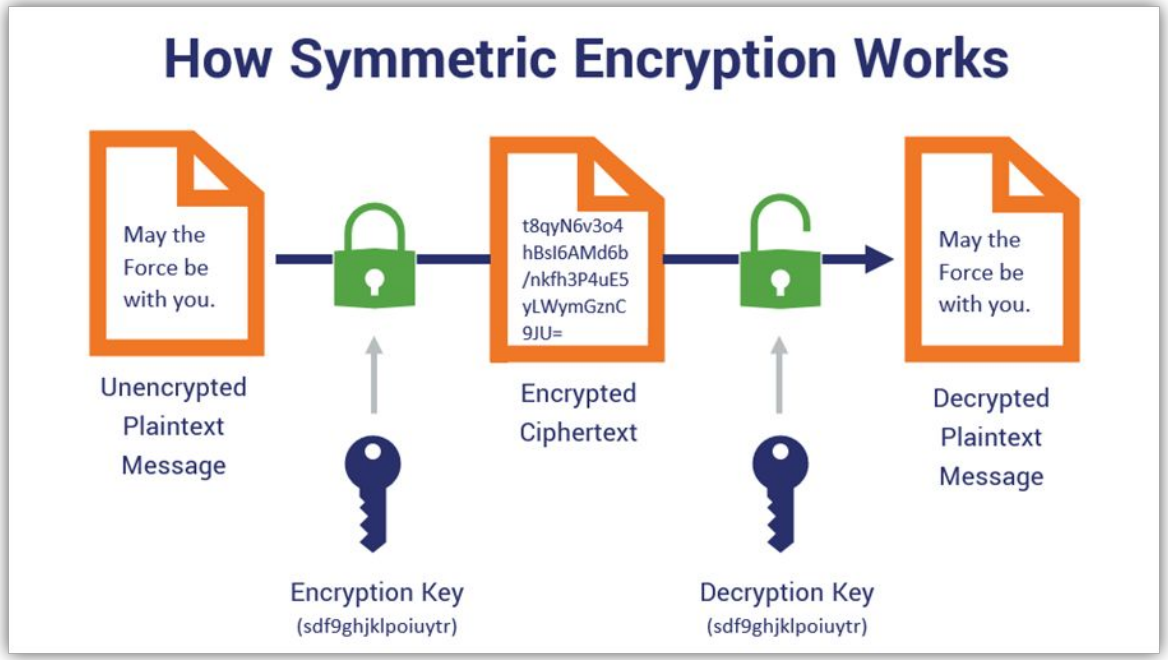
O que é a Criptografia?

Criptografia em segurança virtual é a conversão de dados de um formato legível em um formato codificado. Os dados criptografados só podem ser lidos ou processados depois de serem descriptografados.

A criptografia é um elemento fundamental da segurança de dados. É a forma mais simples e mais importante de garantir que as informações do sistema de um computador não sejam roubadas e lidas por alguém que deseja usá-las para fins maliciosos.

Como ela é executada ?

Ela funciona ao embaralhar dados em um código secreto que só pode ser desbloqueado com uma chave digital exclusiva.



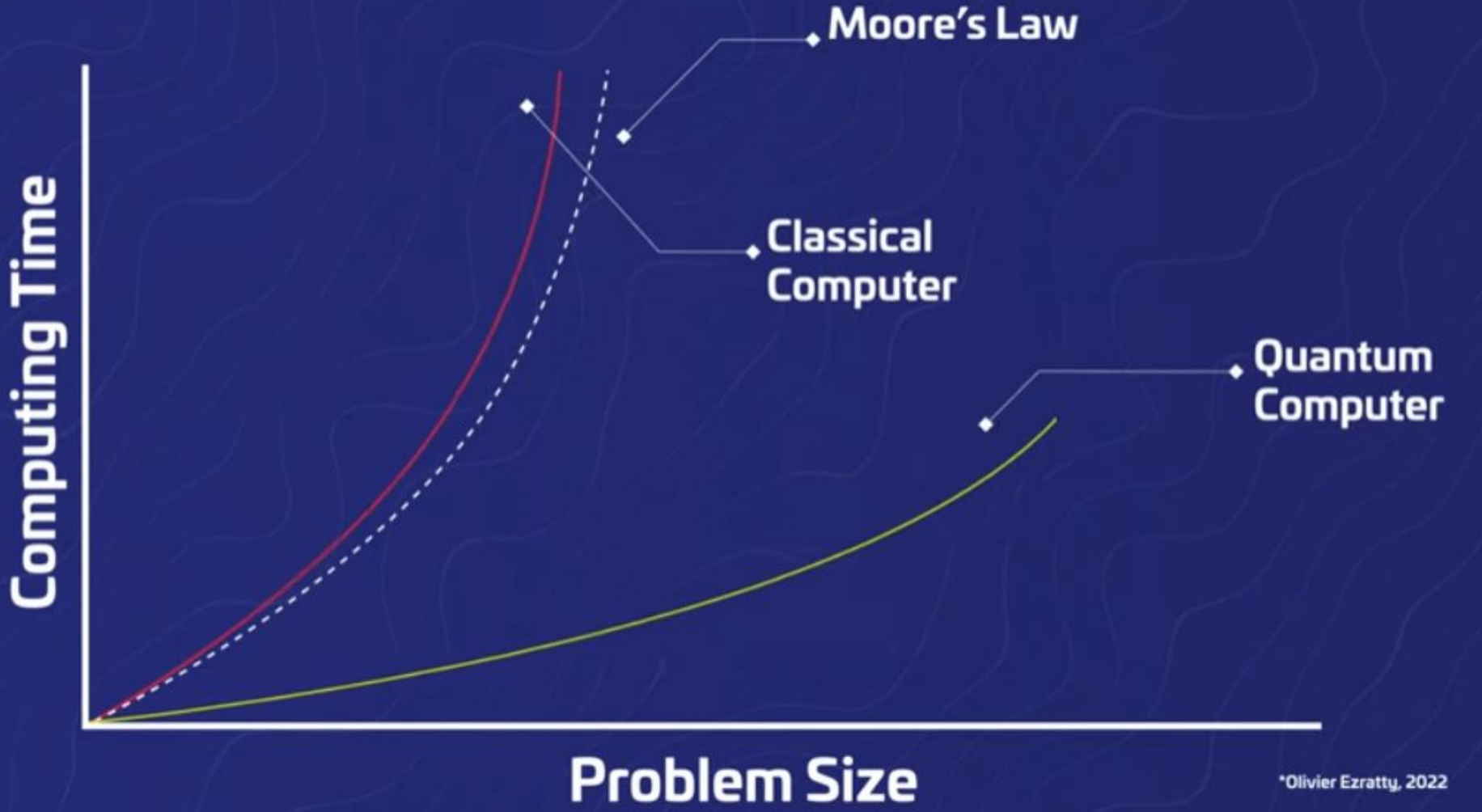
Como evitar uma quebra na Criptografia?

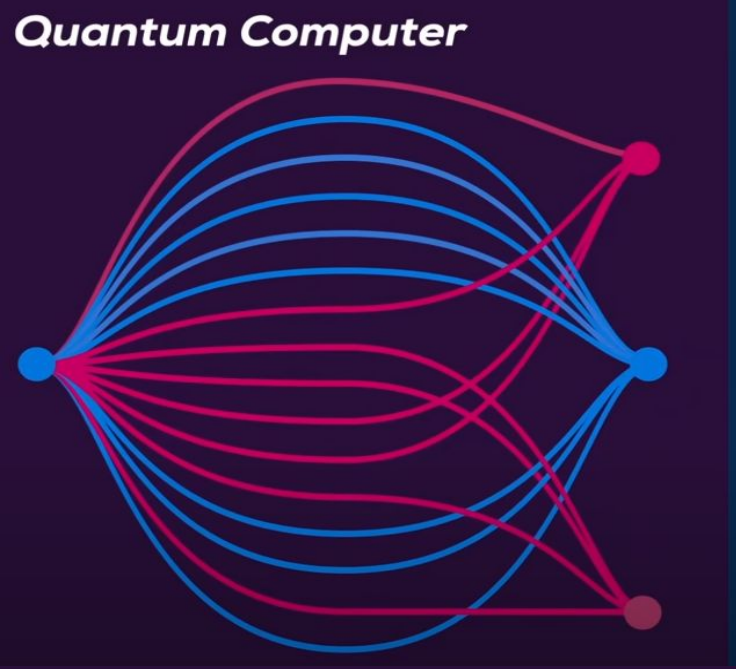
A quebra de criptografia é vista como impossível ou muito demorada, podendo levar anos. No entanto, essa perspectiva pode mudar com a introdução dos computadores quânticos.

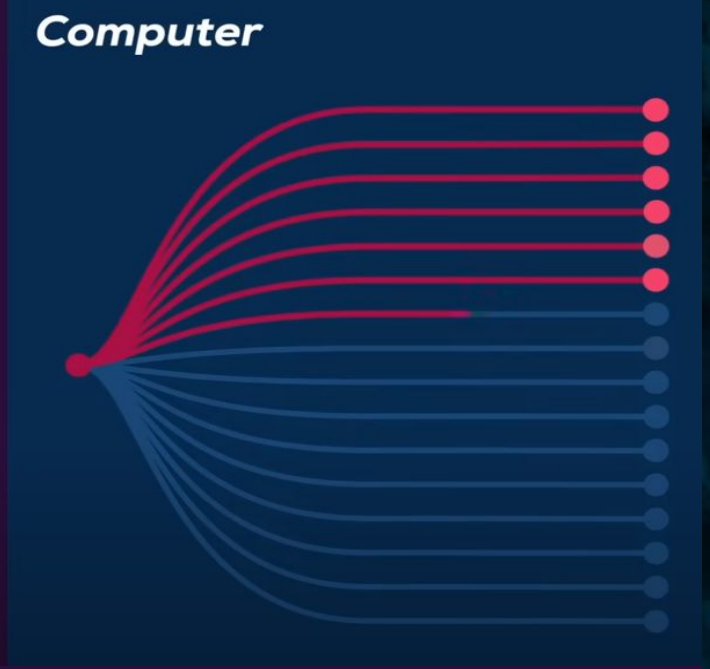
Como a criptografia será afetada com a chegada dos computadores quânticos?

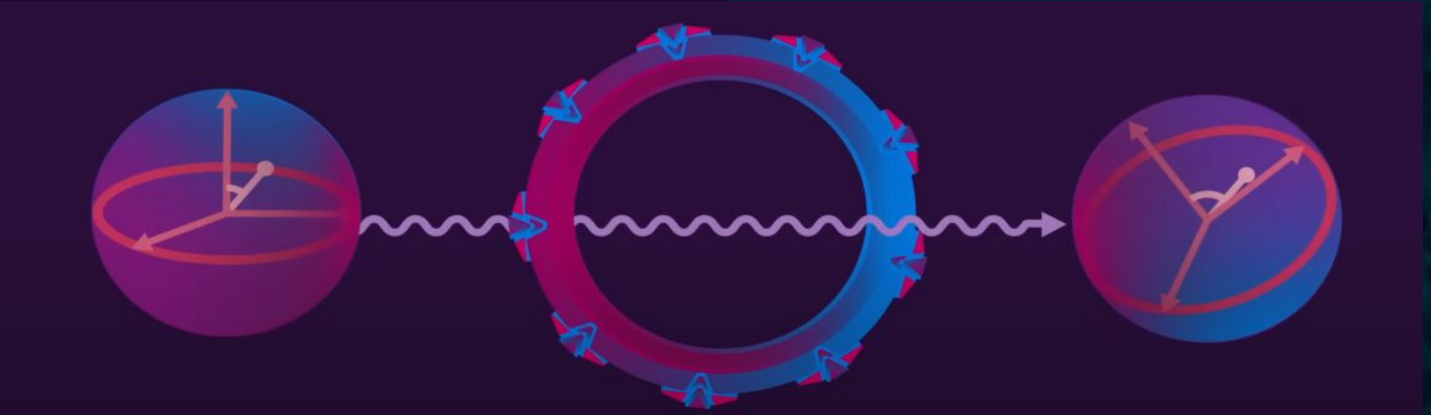
É possível usar algo como o Algoritmo de Shor, que explora a mecânica quântica, para simplificar a fatoração de números em seus componentes principais (números primos), algo essencialmente inviável para computadores comuns quando os números são muito grandes.

isso afeta diretamente na confidencialidade da criptografia de chave pública, e outros algoritmos similares, tornando ela num controle de segurança inútil.


Moore's Law
Classical Computer
Quantum Computer
Computing Time
Problem Size
*Olivier Ezratty, 2022







FUNDAMENTOS

<Qubits>

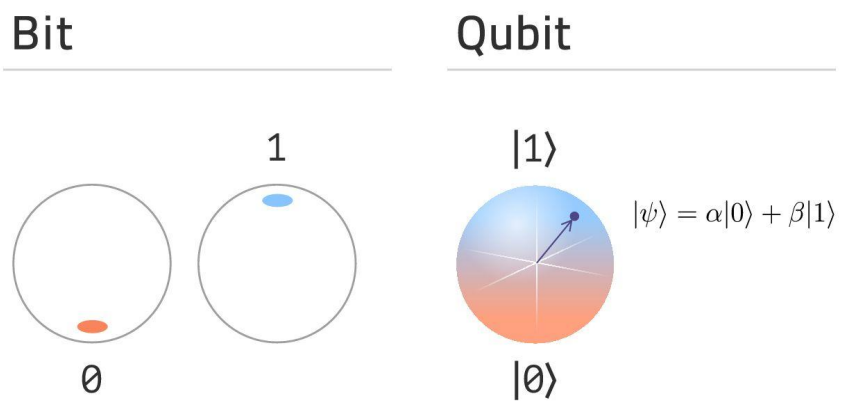
<Superposição>

<Emaranhamento quântico>

<Portas Quânticas>

Computadores Quânticos

- Definição: Sistemas criptográficos seguros contra ataques de computadores quânticos.
- Motivação: Computadores quânticos podem quebrar algoritmos criptográficos tradicionais, como RSA e ECC.



Criptografia Pós-Quântica

- Definição: Sistemas criptográficos seguros contra ataques de computadores quânticos.
- Motivação: Computadores quânticos podem quebrar algoritmos criptográficos tradicionais, como RSA e ECC.

Tipos de Criptografia Quântica

Criptografia de Lattice:

- Baseada em problemas matemáticos relacionados à geometria de reticulados.
- Exemplos: NTRUEncrypt, Kyber.

Códigos de Corpo de Extensão:

- Baseados em problemas de decodificação de código em corpos finitos. Exemplos: McEliece, BIKE.

Algoritmos de contra medidas Pós Quantica

- **NTRUEncrypt**
- **Kyber**
- **Saber**
- **SIKE (Supersingular Isogeny Key Encapsulation)**

SNDL (Store Now Decripty Later)

Usado por algumas nações e outros indivíduos. SNDL tem a intenção de armazenar dados criptografados para futuramente os descriptografar com computadores quânticos