Levantamento e análise de complexidade de técnicas de criptografia pós quântica

Daniel Boso

Direções ...

Criptografia Clássica

- Definições
- Criptografia Simétrica
- Criptografia Assimétrica
- Hash
- Assinatura Digital

Criptografia Pós Quântica

- Code-based cryptography
- Hash-based cryptography
- Lattice-based cryptography
- Multivariate Polynomial Cryptography

Criptografia Clássica

Definições

Autenticação: propriedade de ser genuíno e capaz de ser verificável e confiável.

Controle de Acesso: provê proteção contra o uso não autorizado de recursos.

Confidencialidade de Dados: preservar restrições autorizadas sobre acesso e divulgação de informação, incluindo meios para proteger a privacidade de indivíduos e informações privadas.

Definições

Integridade de Dados: prevenir-se contra a modificação ou destruição imprópria de informação.

Não Repúdio: oferece proteção contra negação, por parte de uma das entidades envolvidas em uma comunicação, de ter participado de toda ou parte dela.

“Conjunto de técnicas baseadas na matemática e aplicadas por meio da informática que utilizam métodos distintos com o objetivo de ocultar dados antes dos observadores não autorizados, mediante o uso de um algoritmo e ao menos uma chave.”

- *Federico Pacheco*

Criptografia Simétrica

Texto Claro: mensagem original.

Algoritmo de Encriptação: realiza diversas substituições e transformações no texto claro.

Chave Secreta: serve como entrada para o algoritmo. O algoritmo produzirá uma saída diferente, dependendo da chave usada no momento.

Criptografia Simétrica

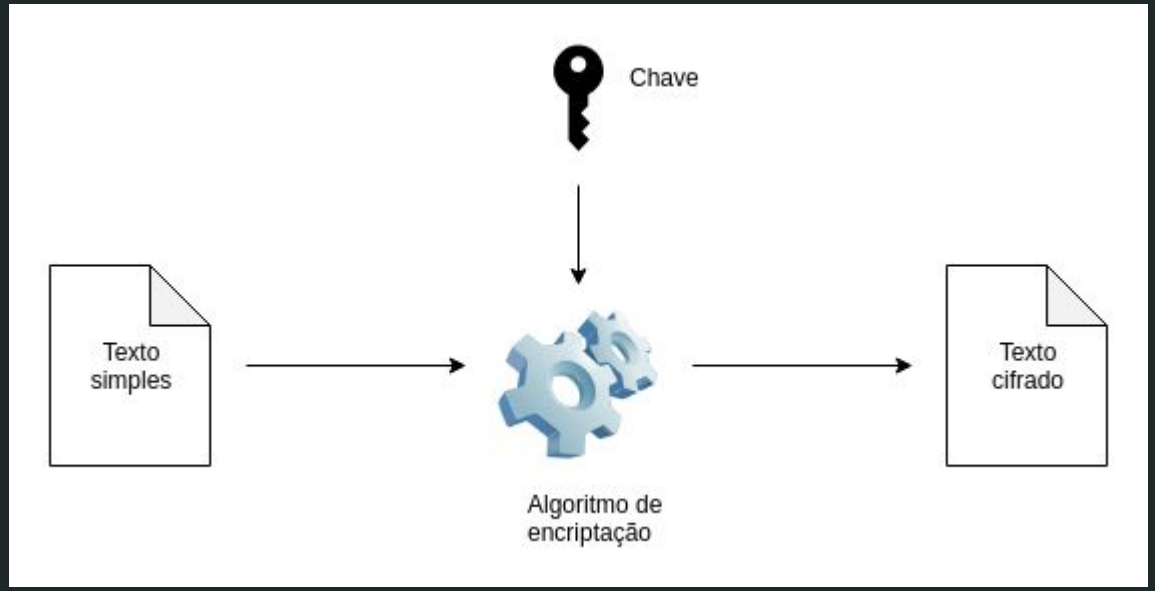
Texto Cifrado: mensagem embaralhada produzida pelo algoritmo.

Algoritmo de Decriptação: basicamente é o algoritmo de encriptação executado de modo inverso.

Criptografia Simétrica

São tipicamente projetadas para minimizar a computação necessária para criptografar e descriptografar dados e consequentemente podem ser implementadas de tal maneira a operar em altas velocidades.

Esquema de ciframento



Criptografia Assimétrica

Texto Claro: é a mensagem ou os dados legíveis.

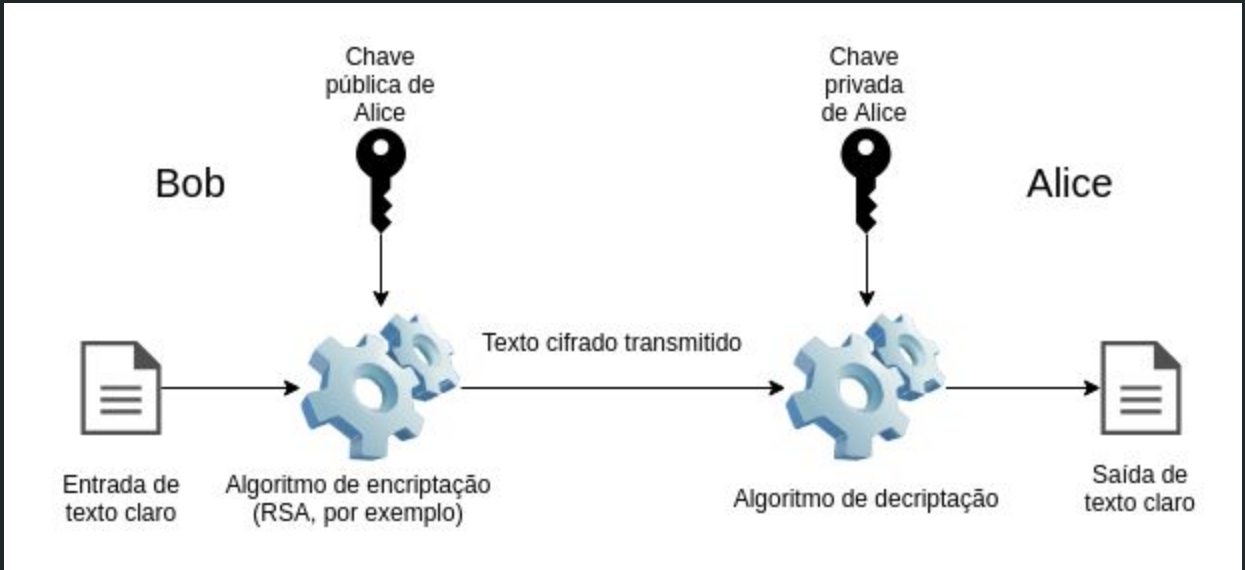
Algoritmo de Encriptação: realiza várias transformações no texto claro.

Chaves pública e privada: é um par de chaves que foi selecionado de modo que, se uma for usada para encriptação, a outra é usada para decriptação.

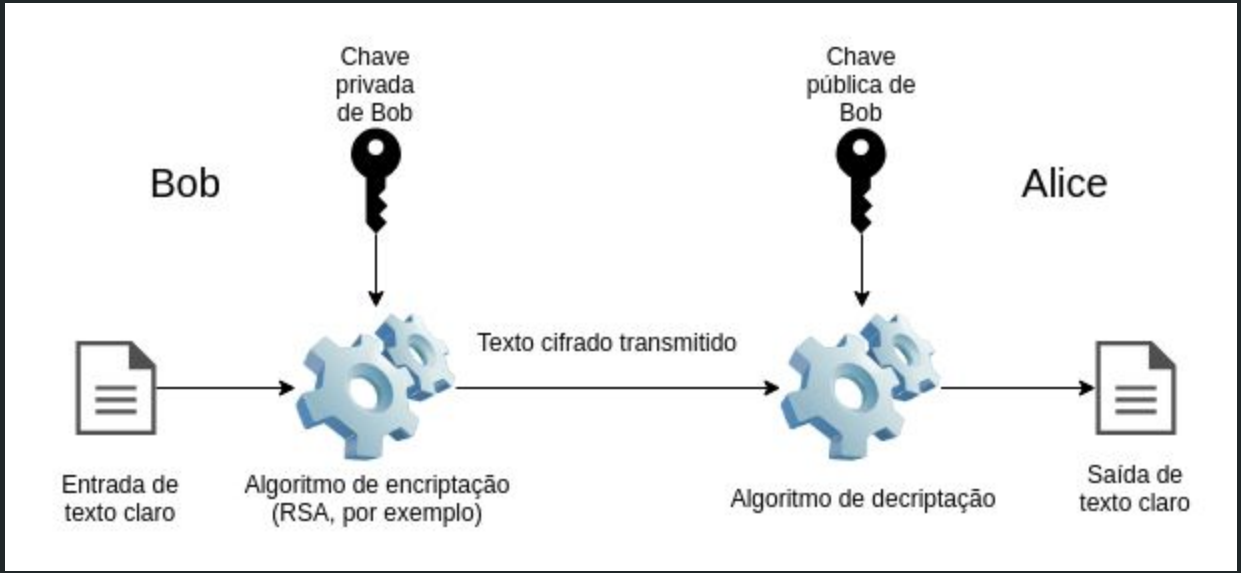
Texto Cifrado: mensagem embaralhada, produzida como saída.

Algoritmo de Decriptação: recebe o texto cifrado e a chave correspondente

Ciframento utilizando chave pública



Ciframento utilizando chave privada



Hash

Resistência à pré-imagem: dado um código hash aleatório, é computacionalmente inviável encontrar uma segunda entrada que dá o mesmo hash.

Resistência à segunda pré-imagem: dado uma entrada para uma função de hash, é computacionalmente inviável encontrar uma segunda entrada que dá o mesmo código hash

Hash

Resistência à colisão: É computacionalmente inviável encontrar duas entradas que resultam no mesmo hash.

Indistinguível de aleatório: é impossível para um atacante dizer a diferença entre a função hash e uma função escolhida completamente ao acaso de todas as funções com as mesmas características de entrada/saída como a função de hash.

Hash

O objetivo principal é funcionar como uma representação reduzida de uma entrada. Uma boa função de hash tem a propriedade de que os resultados da aplicação da função a um grande conjunto de entradas produzirá saídas que são distribuídas por igual e aparentemente de modo aleatório.

O papel das funções de hash na criptografia como um bloco construtor é absolutamente vital. Um grande número de esquemas criptográficos usam uma função de hash em algum ponto, e na maioria dos casos o uso de uma função de hash fraca destrói a segurança do esquema todo.

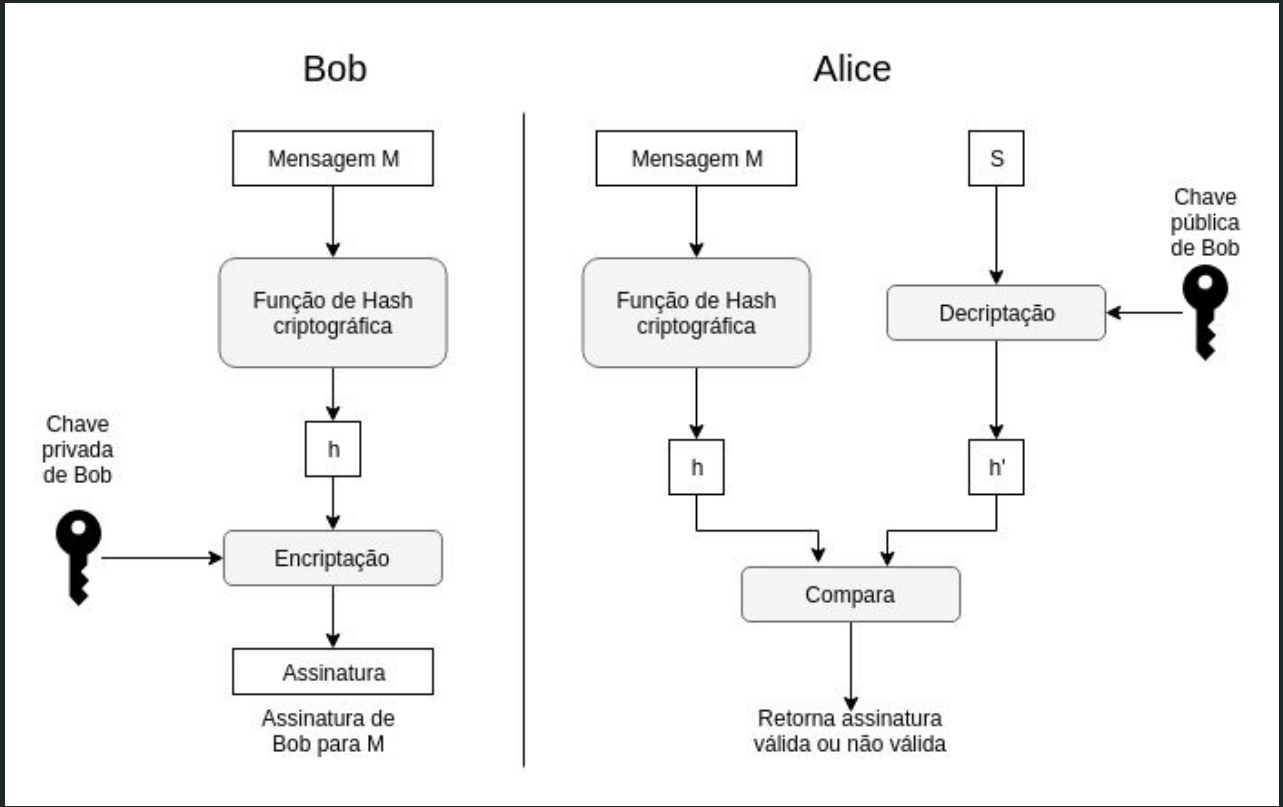
Assinatura Digital

Foram primeiro previstas no final da década de 1970.

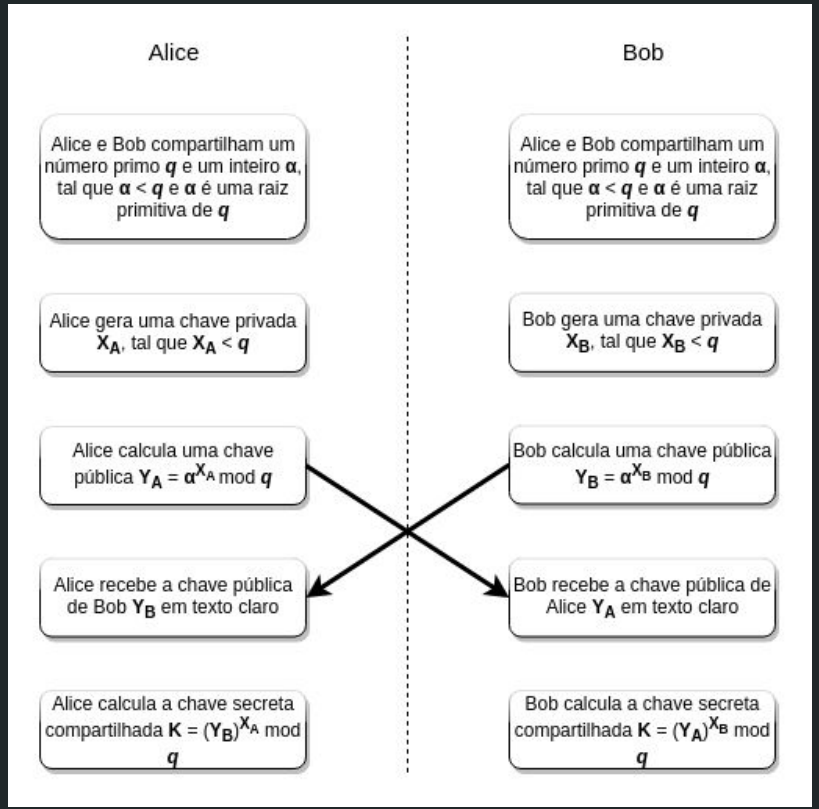
Foram projetadas para prover todas as vantagens de uma **assinatura de contrato da vida real** em um cenário digital, permitindo que as pessoas negociem contratos sob vastas distâncias rapidamente.

Uma assinatura digital deve garantir que o **dado ou contrato não é mudado depois que foi assinado** e que **o assinante não pode repudiar sua assinatura.**

Processo de Assinatura Digital



Um exemplo: Troca de Chaves - Diffie-Hellman



Criptografia Pós Quântica

“A ideia de criptografia pós quântica foi ***primeiramente proposta nos anos de 1970*** *por Stephen Wiesner e Charles H. Bennet da IBM e Gilles Brassard da Universidade de Montreal. Esta,* ***desafia a linha divisória de problemas tratáveis e intratáveis****. O exemplo mais significante para isso é algoritmos quânticos eficientes para quebrar sistemas de criptografia na qual são acreditados serem seguros para computadores clássicos.”*

Seu objetivo: *Desenvolver sistemas criptográficos que sejam seguros contra computadores clássicos e quânticos, e possam interoperar com protocolos de comunicação e redes existentes hoje.*

Code-based Cryptography

Robert McEliece, em 1978 propôs o primeiro esquema.

São sistemas de criptografia que um código de correção de erro C.

Esta primitiva pode consistir em adicionar um erro para uma palavra de C ou na computação de uma síndrome relativamente a uma matriz de teste de paridade de C.

A maioria sofre por terem tamanho de chaves muito grande.

Code-based Cryptography

Segurança clássica, 128 bits.

Códigos de dimensão k = 3.376. Tamanho n = 4.096. t = 60 erros.

O tamanho da chave pública é de 303.840 bytes.

Para a mesma segurança contra adversários quânticos, o tamanho deve aumentar por um fator de 2 e o tamanho de chave por um fator de 4.

Chave pública na ordem de 1MB !

Code-based Cryptography

Uma variante do McEliece chamada MDPC-McEliece.

Utiliza códigos QC-MDPC.

Tamanho de chave pública na ordem de 4KB.

Adequado para troca de chaves de sessão.

Code-based Cryptography

Segurança: a decodificação genérica é difícil na média e a chave pública é difícil de distinguir de uma matriz aleatória. Estes problemas não podem ser resolvidos eficientemente. São intratáveis.

Hash-based Cryptography

Criadas por Ralph Merkle em 1979.

Requerem apenas uma função de sentido único.

Considerada uma das mais importantes, segundo Buchmann.

Sua segurança até mesmo contra ataques quânticos é bem entendida.

Usam funções de hash criptográficas.

Segurança: depende da resistência de colisão de uma função de hash.

Lattice-based Cryptography

Baseadas na dificuldade de resolver problemas envolvendo reticulados, o mais básico na qual é o problema de caminho mínimo.

Tentativas de resolver problemas de reticulados por algoritmos quânticos foram feitas desde o algoritmo de Shor.

Lattice-based Cryptography

Periodicidade, que é usada no algoritmo de fatoração de Shor e relacionada a algoritmos quânticos, não parece ser aplicável para problemas de reticulados.

Não há algoritmo quântico de tempo polinomial que aproxima problemas de reticulados dentro dos fatores polinomiais.

Lattice-based Cryptography

Segurança: resolver problemas envolvendo reticulados, o mais básico, na qual é o problema do caminho mínimo.

Multivariate Polynomial Cryptography

Estudo de sistemas de criptografia de chave pública onde a função de sentido único toma a forma de um mapa polinomial quadrático sobre um corpo finito.

Oferecem o benefício de assinaturas curtas e geralmente eficientes.

São rápidos em relação a outros tipos de esquemas de assinatura.

Chaves públicas podem ser grandes.

Multivariate Polynomial Cryptography

Segurança: resolver conjuntos de equações não lineares sobre um corpo finito e está relacionado a estrutura de polinômios ideais.

Técnica	Uso
Code-based Cryptography	Criptografia de chave pública
Hash-based Cryptography	Sistema de assinatura
Lattice-based Cryptography	Estabelecimento de chaves
Multivariate Polynomial Cryptography	Sistema de assinatura

Técnica	Algoritmo	Chave pública	Chave Privada
Code-based Cryptography	McEliece	1MB	?
	QC-MDPC	4KB	?
Hash-based Cryptography	?	?	?
Lattice-based Cryptography	?	?	?
Multivariate Polynomial Cryptography	Rainbow	45KB	31KB

Técnica	Algoritmo	Complexidade
Code-based Cryptography	McEliece	?
	QC-MDPC	?
Hash-based Cryptography	?	?
Lattice-based Cryptography	?	?
Multivariate Polynomial Cryptography	?	?