

Selected Constructive and Destructive Approaches to Post-Quantum Cryptography

Gustavo Souza Banegas

Technische Universiteit Eindhoven
gustavo@cryptme.in

November 12, 2019

Cryptography 101



Cryptography 101



Alice



Bob



Communication Problem

Oof.. Lazy drawing skills



Communication Problem



Communication Problem



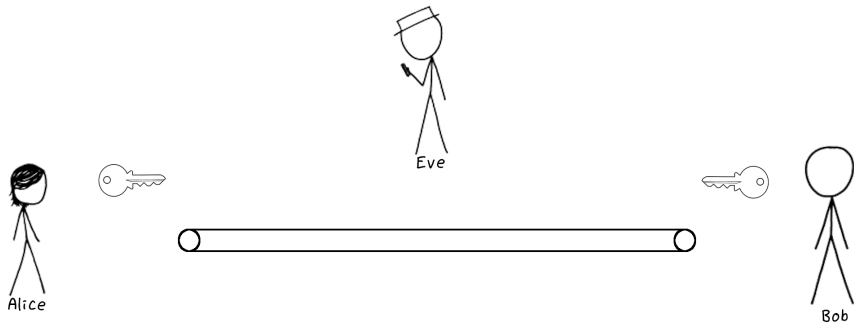
Communication Problem



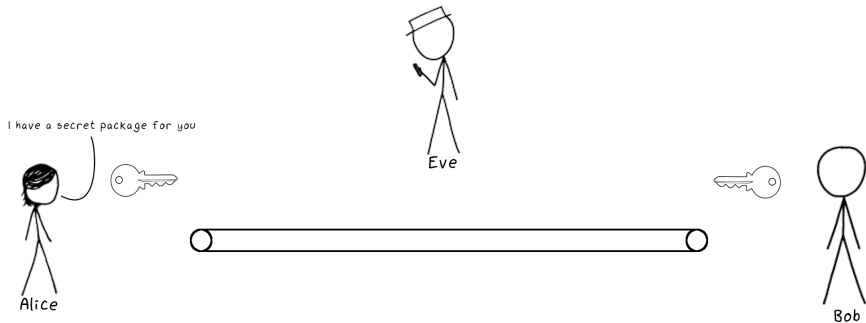
Communication Problem



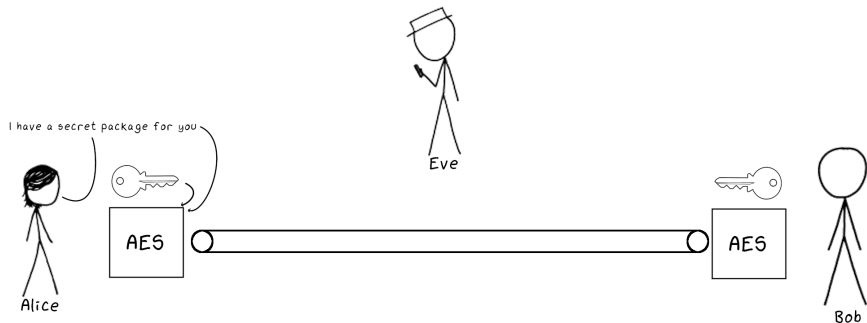
Communication Problem



Communication Problem



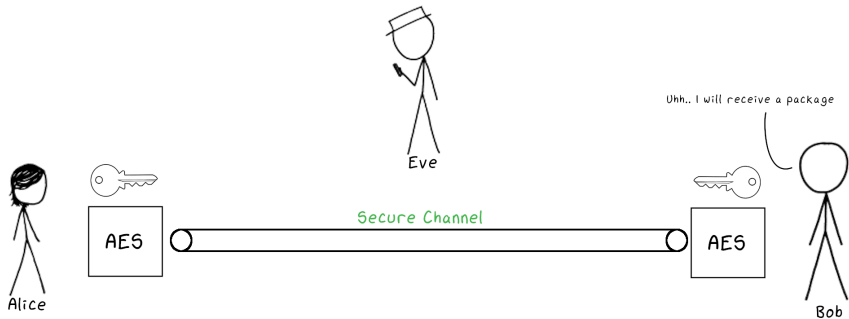
Communication Problem



Communication Problem



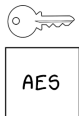
Communication Problem



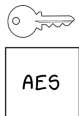
Communication Problem



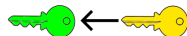
Communication Problem



Communication Problem



Communication Problem



Communication Problem



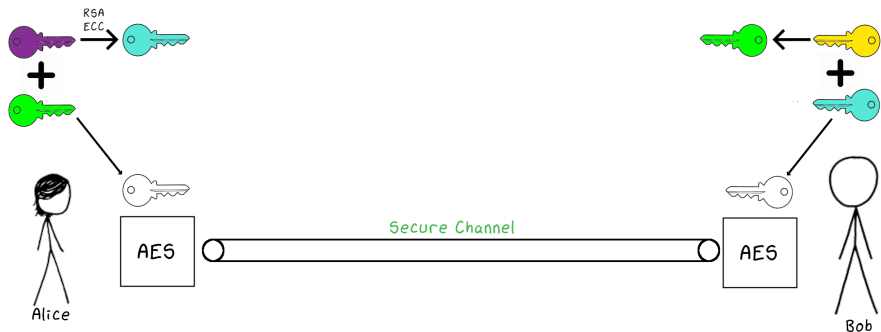
Communication Problem



Communication Problem



Communication Problem



Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:

Secret Key

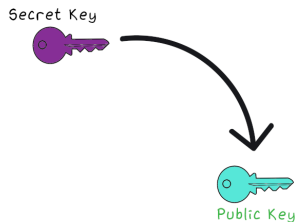


Public Key



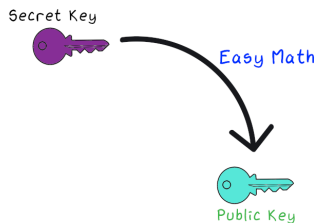
Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



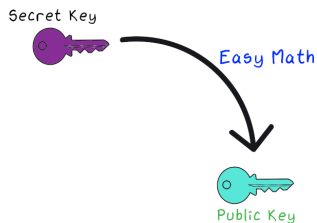
Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



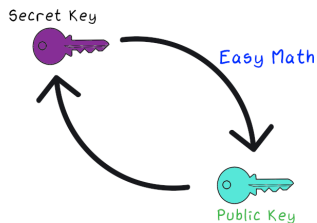
Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



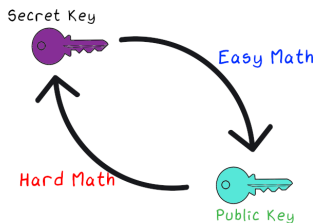
Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



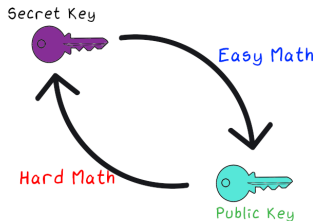
Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:

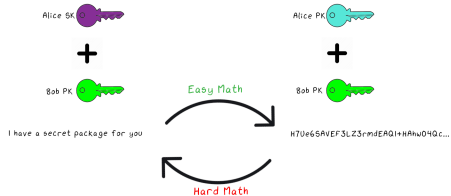
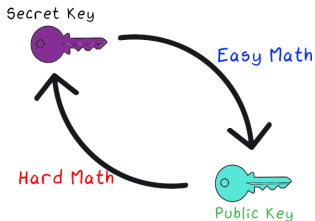


*Factoring is hard.
Let's go shopping*



Mathematics behind Cryptography

In a nutshell, cryptography desires certain properties to be secure:



Quantum Computer and Quantum Algorithms



Quantum Computer and Quantum Algorithms



Quantum computers mean cryptography needs to change, and soon

As quantum computing gains momentum with practical quantum computers due to come online as early as next year, concerns about post-quantum cryptography are pushed to the forefront.

By [Peter Loshin](#), Technology Editor

INNOVATION

How Peter Shor's Algorithm Dooms RSA Encryption to Failure

In 1994, Peter Shor created an algorithm for a theoretical computer that solved a nearly impossible problem. Now that technology is catching up, Shor's algorithm guarantees the end to RSA Encryption.

By [John Loeffler](#)



Post-Quantum Cryptography

**We can make
cryptography
secure with**



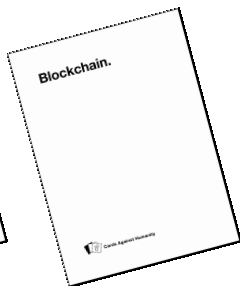
Post-Quantum Cryptography

**We can make
cryptography
secure with**



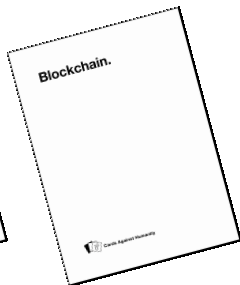
Post-Quantum Cryptography

We can make
cryptography
secure with



Post-Quantum Cryptography

We can make
cryptography
secure with



Post-Quantum Cryptography



Post-Quantum Cryptography



Post-Quantum Cryptography

Is this enough to make
cryptography secure?



Post-Quantum Cryptography

Is this enough to make
cryptography secure?



Post-Quantum Cryptography

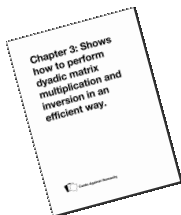
Is this enough to make
cryptography secure?



- ▶ Evaluate the current cryptoschemes for mistakes;
- ▶ Check if the current parameters are secure;
- ▶ Use quantum cryptanalysis:
 - ▶ Check how to use quantum algorithms;
 - ▶ Estimate how big a quantum computer needs to be to run a quantum algorithm;
 - ▶ Develop new quantum algorithms.



Post-Quantum Cryptography



Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.



Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.



Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.

Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.

Chapter 5: Shows that implementation matters and shows how to use a side-channel attack in code-based schemes. Later on, the chapter proposes a countermeasure.

Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.

Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.

Chapter 5: Shows that implementation matters and shows how to use a side-channel attack in code-based schemes. Later on, the chapter proposes a countermeasure.

Chapter 6: Shows a reaction attack that exploits the decoding failure rate and then recover the key.

Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.

Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.

Chapter 7: The basic explanation of quantum algorithm and quantum cryptanalysis

Chapter 5: Shows that implementation matters and shows how to use a side-channel attack in code-based schemes. Later on, the chapter proposes a countermeasure.

Chapter 6: Shows a reaction attack that exploits the decoding failure rate and then recover the key.

Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.

Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.

Chapter 7: The basic explanation of quantum algorithm and quantum cryptanalysis

Chapter 8: How to build AES circuit in a quantum computer.

Chapter 5: Shows that implementation matters and shows how to use a side-channel attack in code-based schemes. Later on, the chapter proposes a countermeasure.

Chapter 6: Shows a reaction attack that exploits the decoding failure rate and then recover the key.

Post-Quantum Cryptography

Chapter 3: Shows how to perform dyadic matrix multiplication and inversion in an efficient way.

Chapter 4: Shows that it is possible to create a cryptosystem using Generalized Srivastava codes.

Chapter 7: The basic explanation of quantum algorithm and quantum cryptanalysis

Chapter 8: How to build AES circuit in a quantum computer.

Chapter 5: Shows that implementation matters and shows how to use a side-channel attack in code-based schemes. Later on, the chapter proposes a countermeasure.

Chapter 6: Shows a reaction attack that exploits the decoding failure rate and then recover the key.

Chapter 9: Build a quantum circuit for finding preimages when AES is used as a hash function.

Post-Quantum Cryptography



Selected Constructive and Destructive Approaches to Post-Quantum Cryptography

Gustavo Souza Banegas

Technische Universiteit Eindhoven
gustavo@cryptme.in

November 12, 2019

