Selected Constructive and Destructive Approaches to Post-Quantum Cryptography

Gustavo Souza Banegas

Technische Universiteit Eindhoven
gustavo@cryptme.in

November 12, 2019

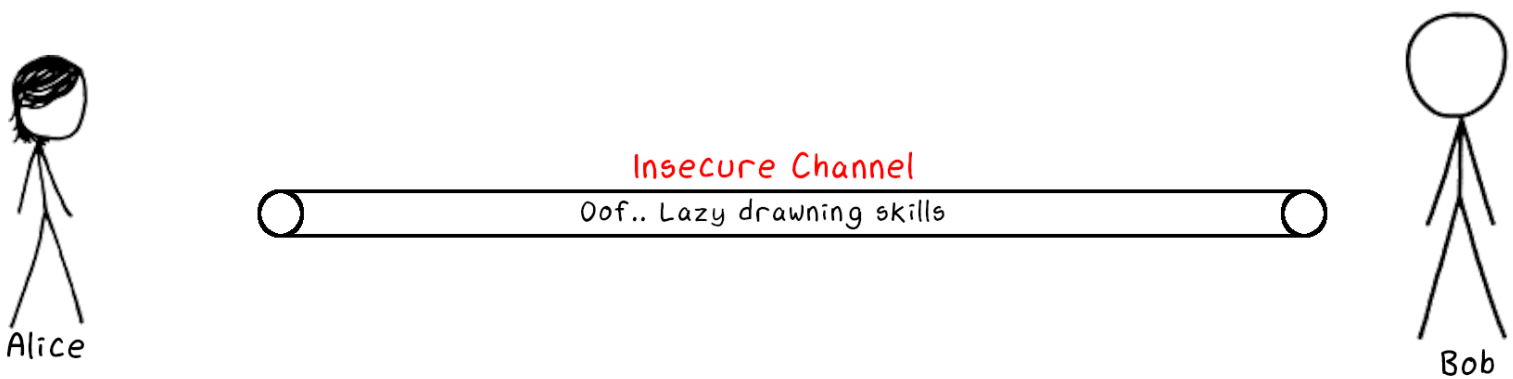
Defense Against Committee

Cryptography 101

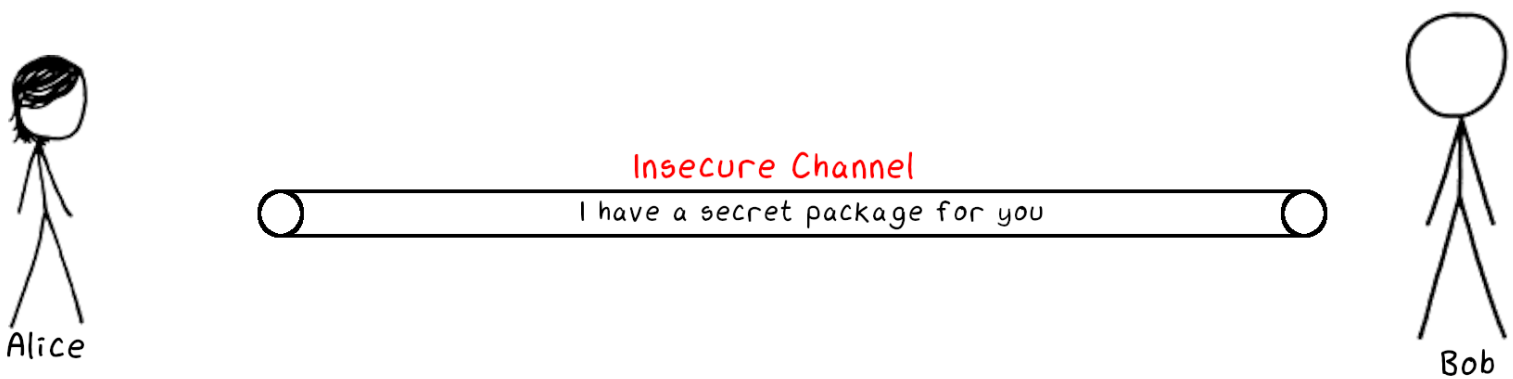
Cryptography 101

Communication Problem

Communication Problem



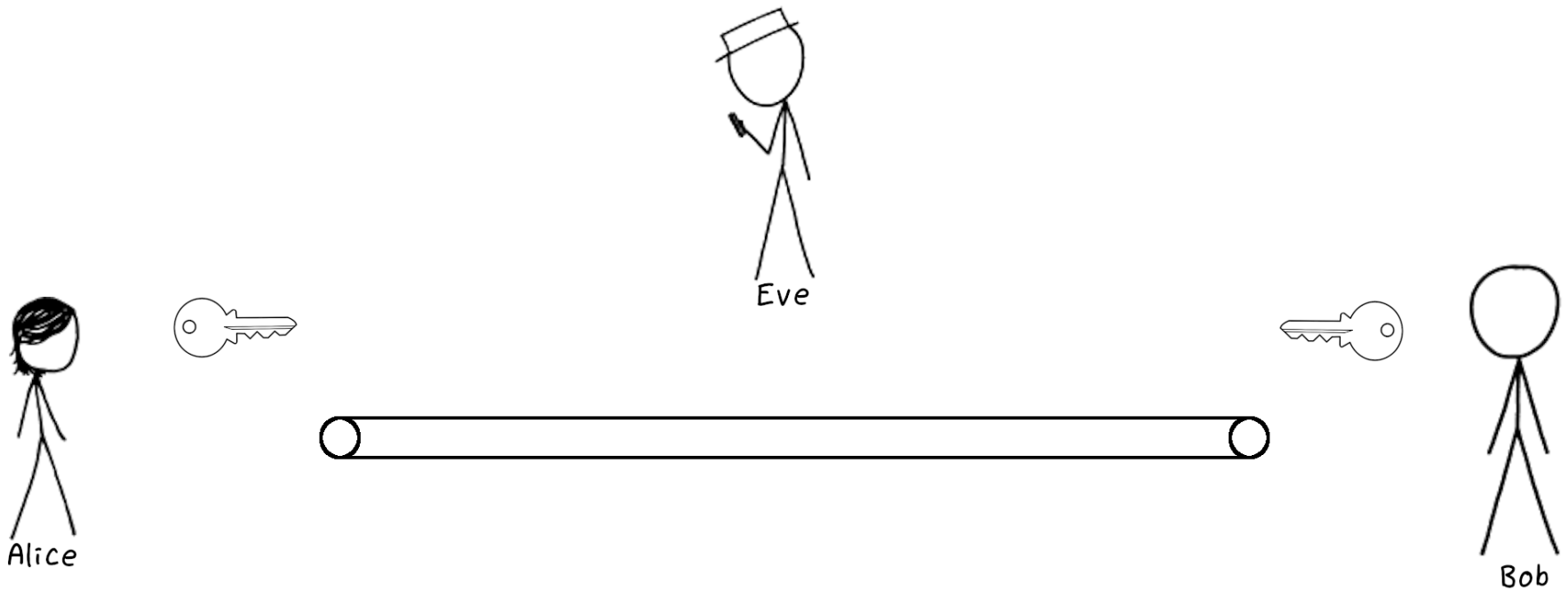
Communication Problem



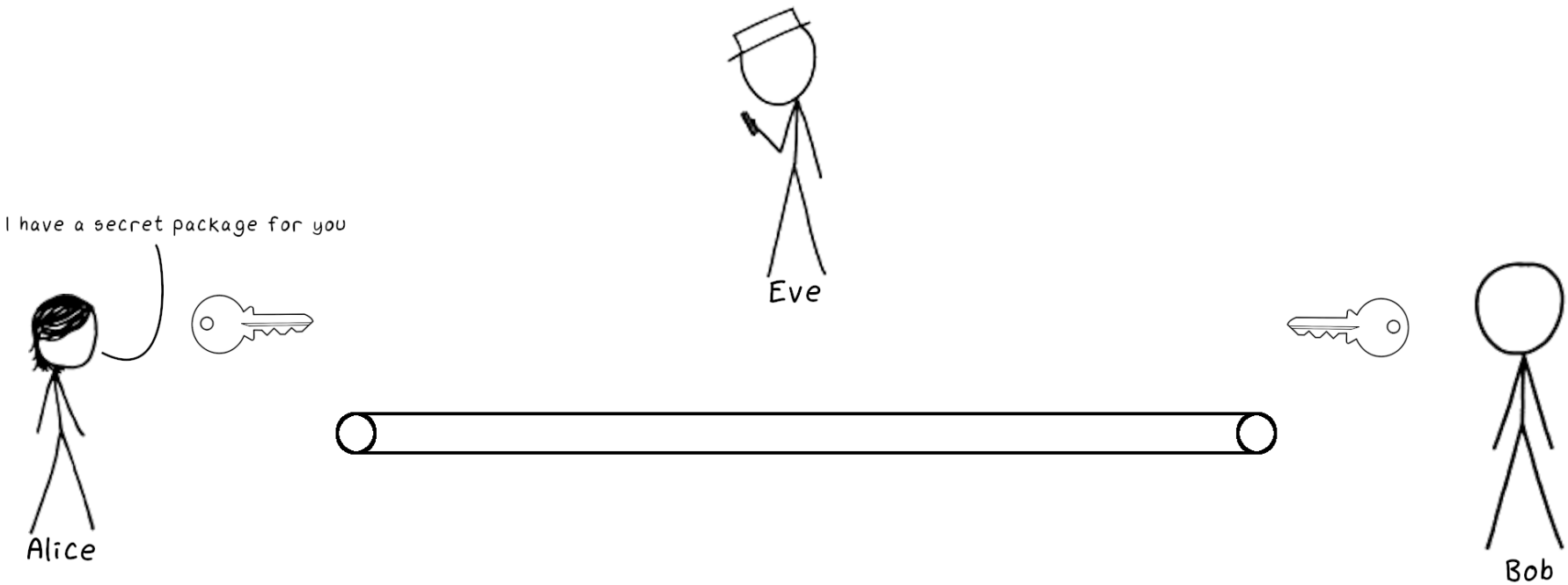
Communication Problem

Communication Problem

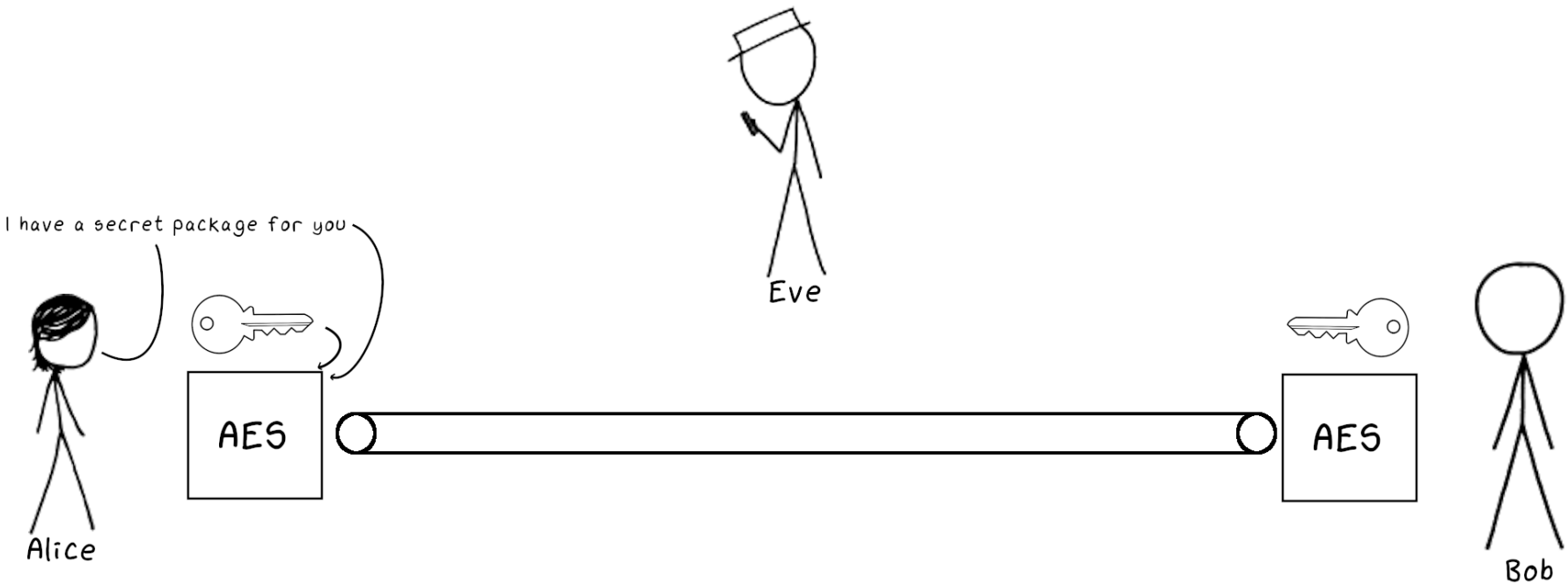
Communication Problem



Communication Problem

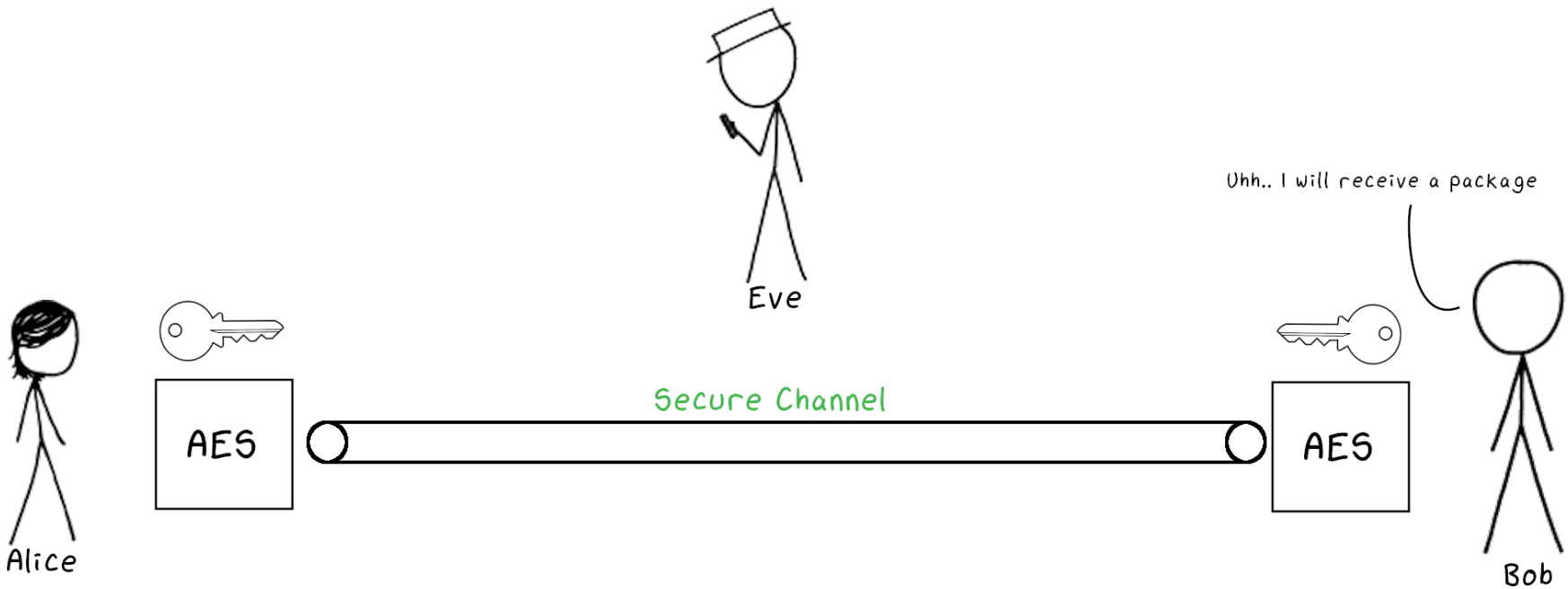


Communication Problem



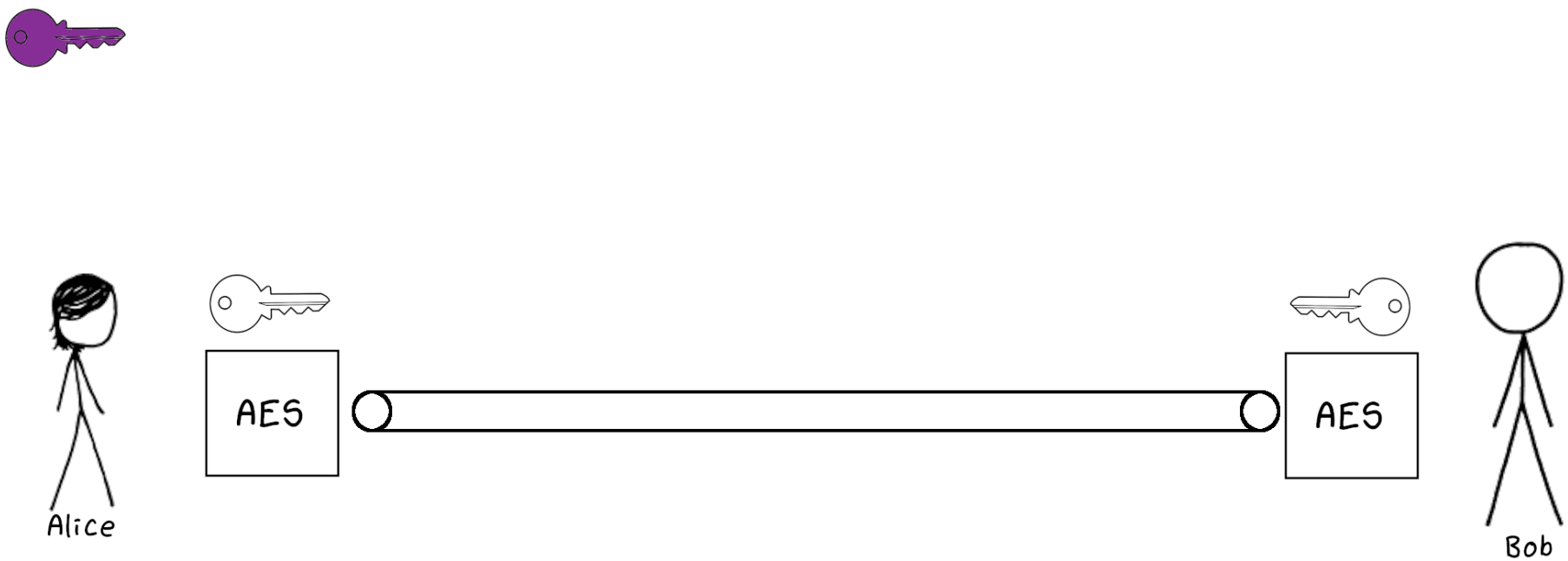
Communication Problem

Communication Problem

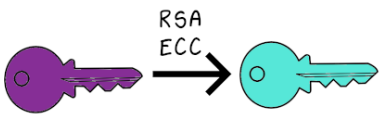


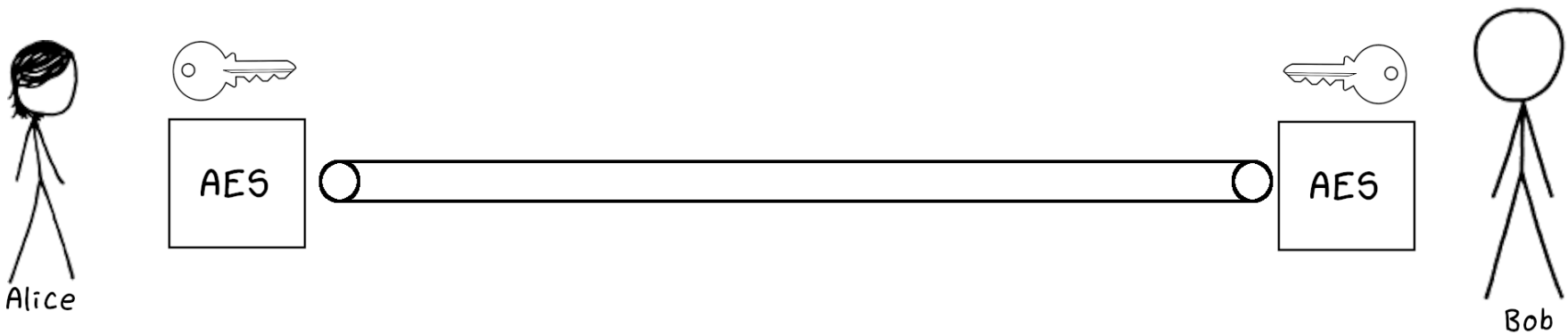
Communication Problem

Communication Problem



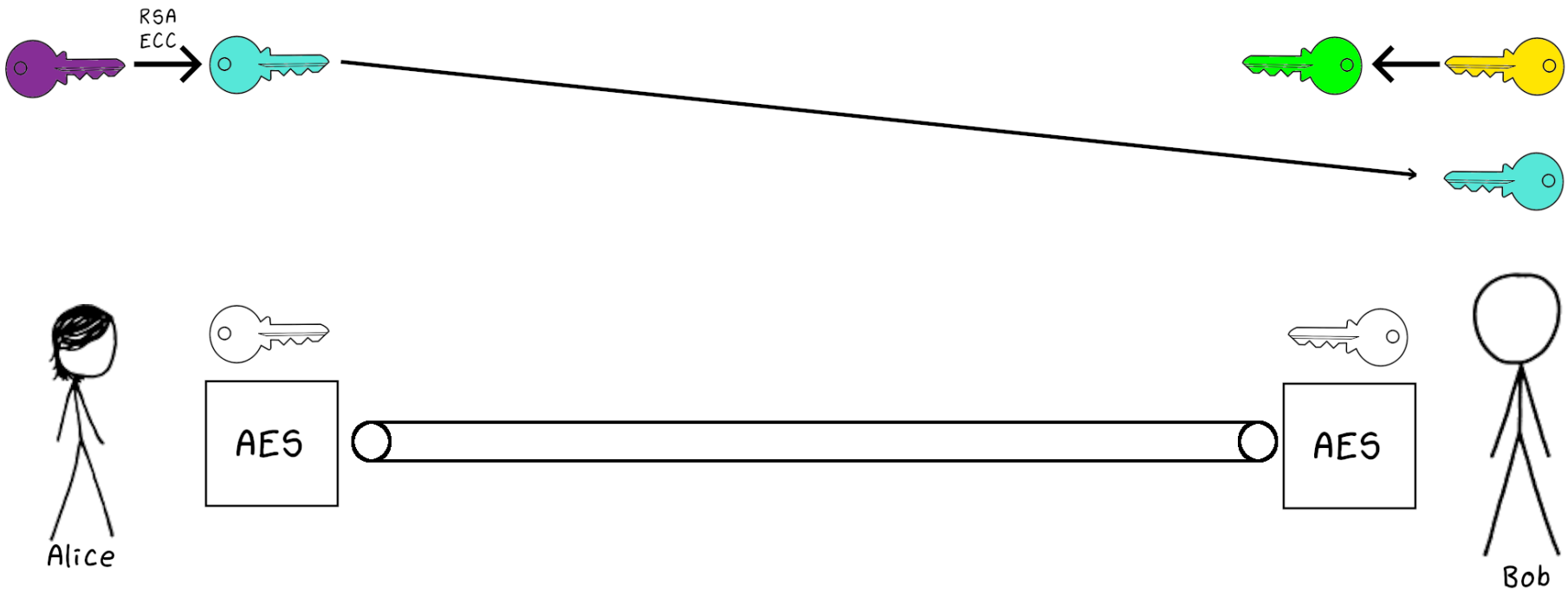
Communication Problem





Communication Problem

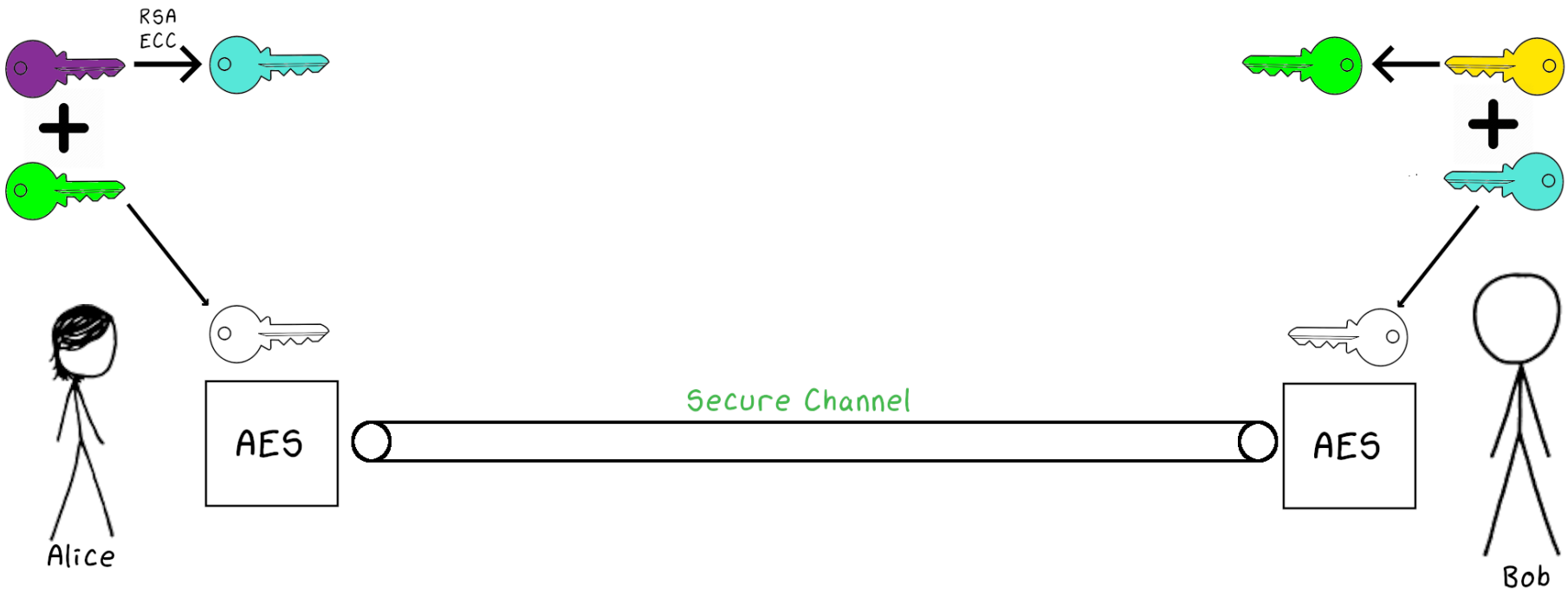
Communication Problem



Communication Problem

Communication Problem

Communication Problem



Mathematics behind Cryptography

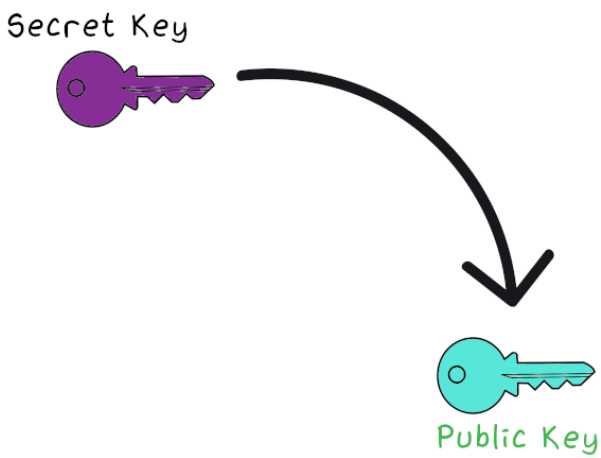
In a nutshell, cryptography desires certain properties to be secure:

Mathematics behind Cryptography

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

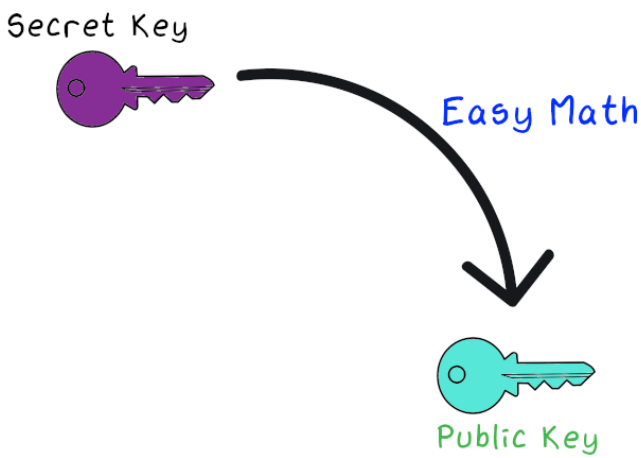
Mathematics behind Cryptography

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



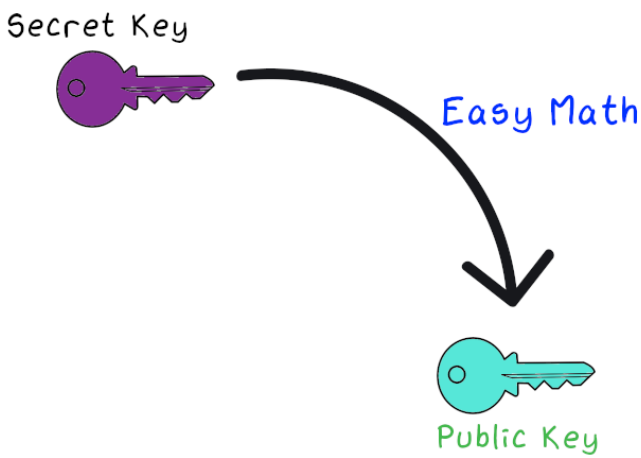
Mathematics behind Cryptography

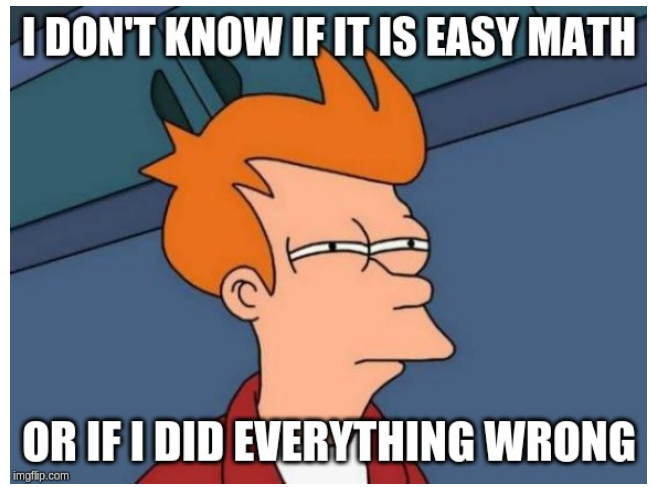
In a nutshell, cryptography desires certain properties to be secure:



Mathematics behind Cryptography

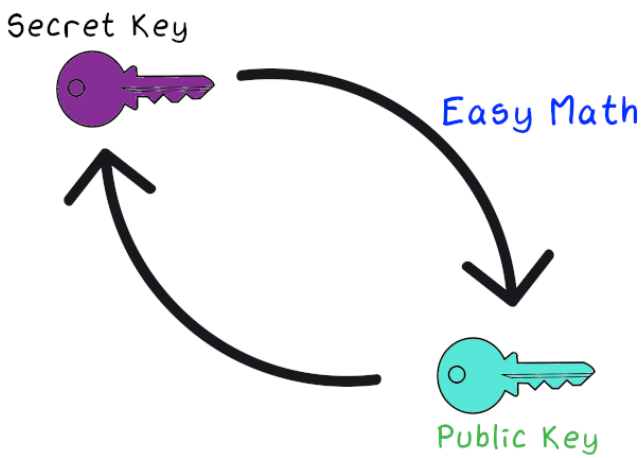
In a nutshell, cryptography desires certain properties to be secure:





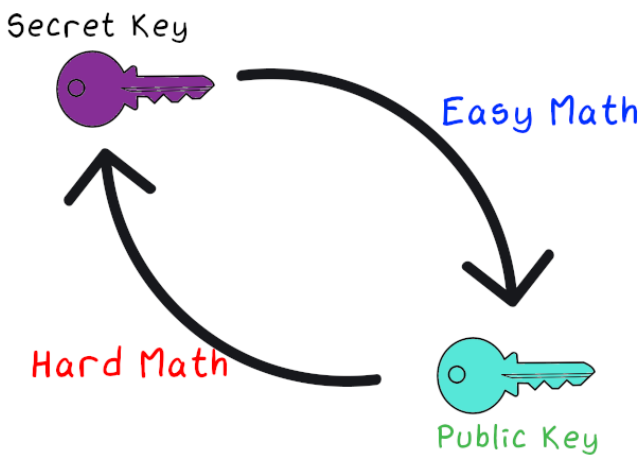
Mathematics behind Cryptography

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



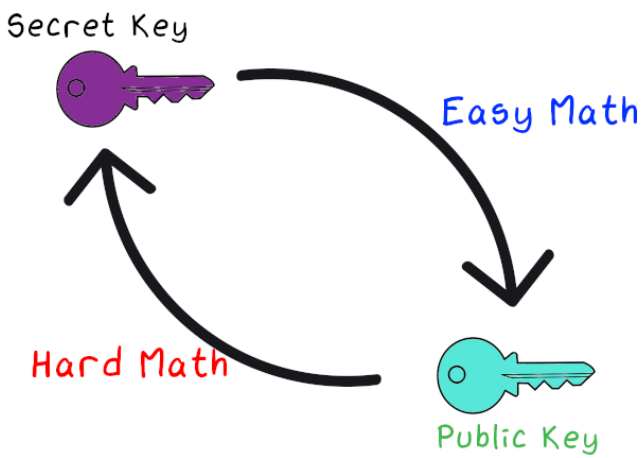
Mathematics behind Cryptography

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



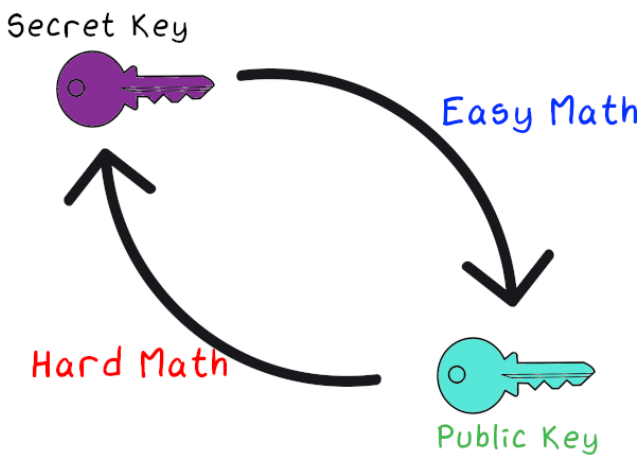
Mathematics behind Cryptography

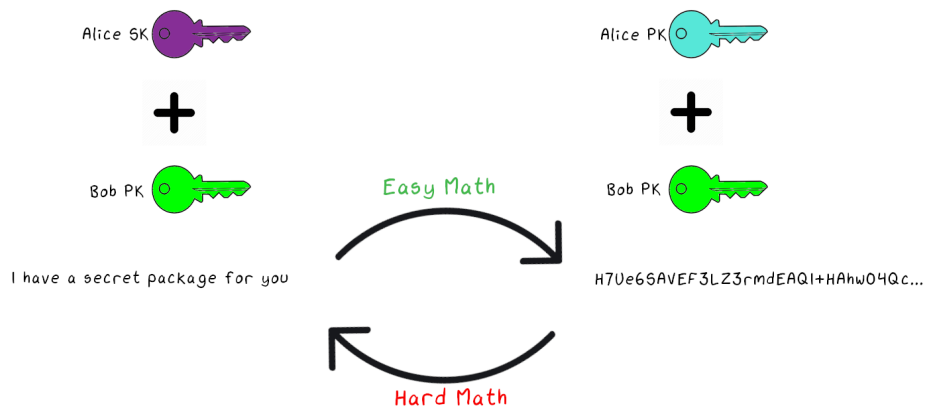
In a nutshell, cryptography desires certain properties to be secure:



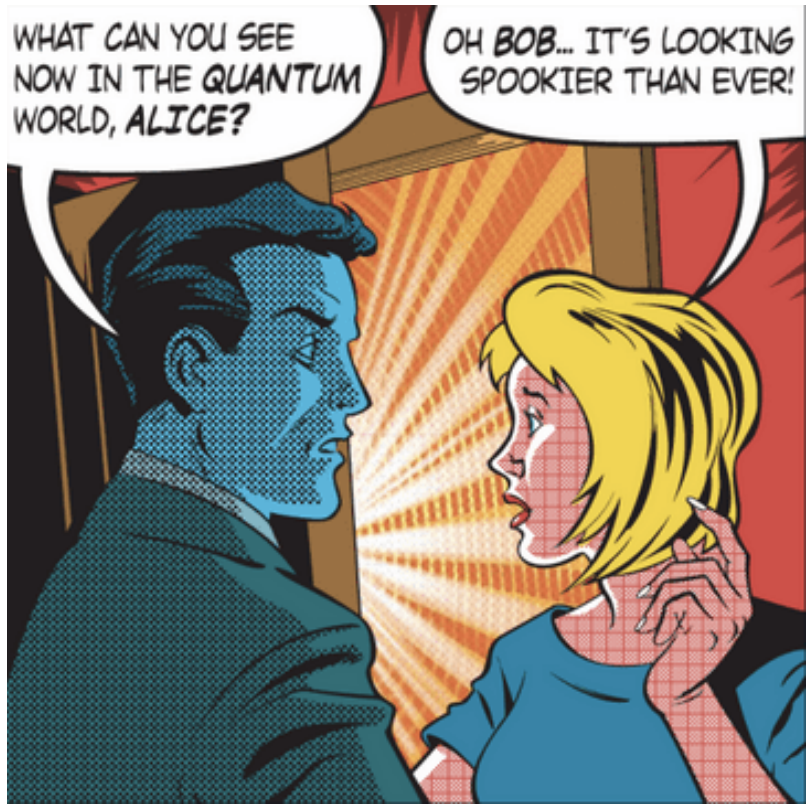
Mathematics behind Cryptography

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





Quantum Computer and Quantum Algorithms



Quantum Computer and Quantum Algorithms

Quantum Leap Into Time And Space Closer To Reality
National Geographic · 15 hours ago

Quantum leap in computing as Google claims 'supremacy'
Jordan Times · 2 days ago

EVALUATE

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

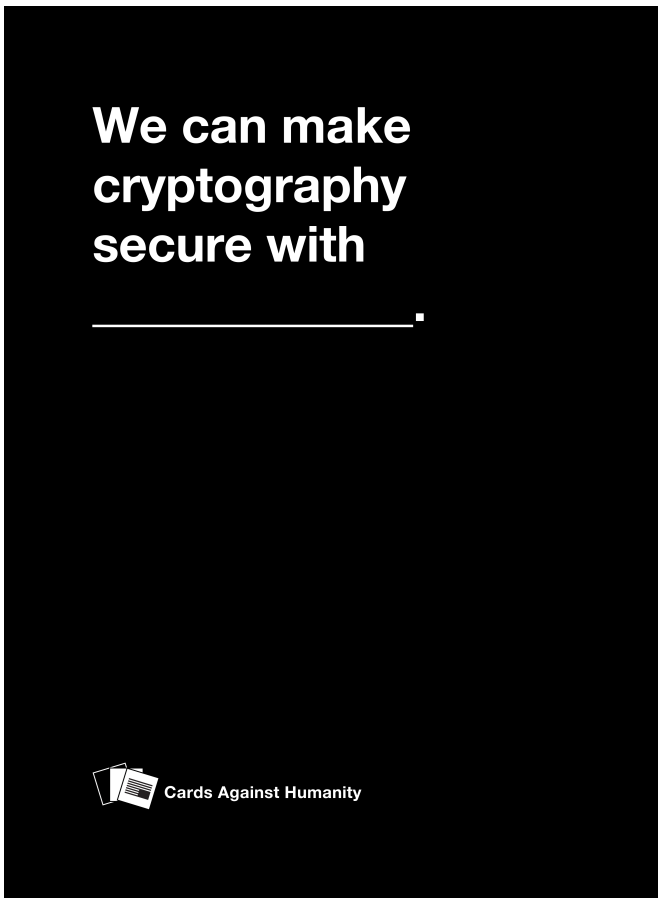
INNOVATION

How Peter Shor's Algorithm Dooms RSA Encryption to Failure

In 1994, Peter Shor created an algorithm for a theorical 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



Post-Quantum Cryptography

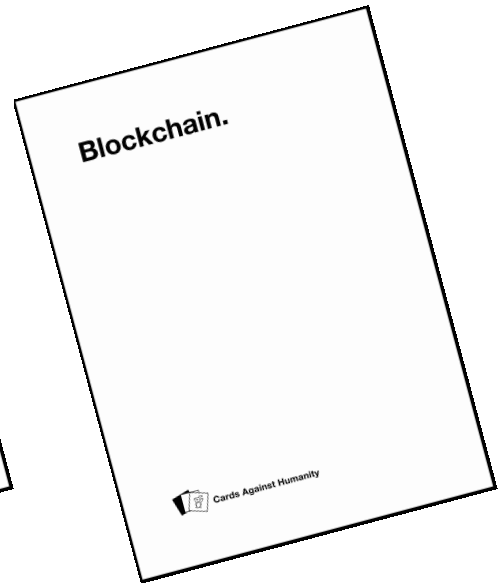
We can make cryptography secure with _____.

Cards Against Humanity

Post-Quantum Cryptography

We can make cryptography secure with _____.

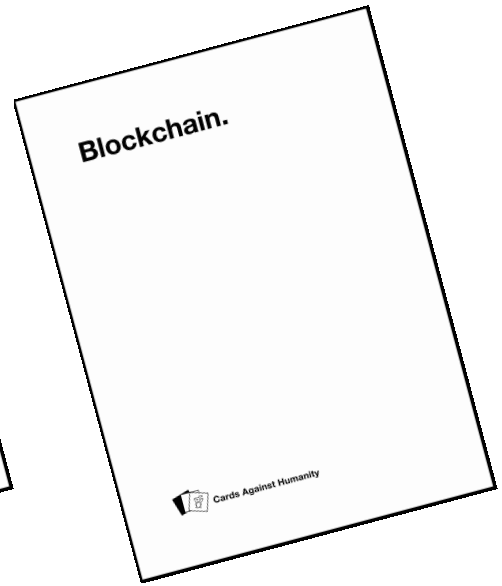
Cards Against Humanity



Post-Quantum Cryptography

We can make cryptography secure with _____.

Cards Against Humanity



Defense Against Committee

Post-Quantum Cryptography

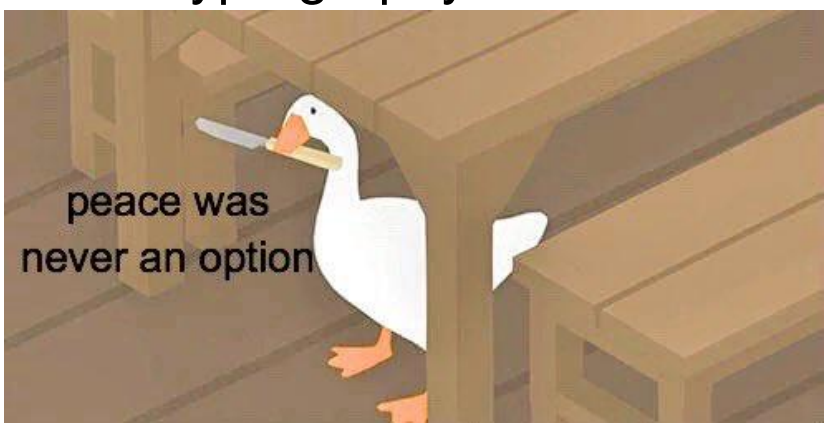
Post-Quantum Cryptography

Post-Quantum Cryptography

Is this enough to make cryptography secure?

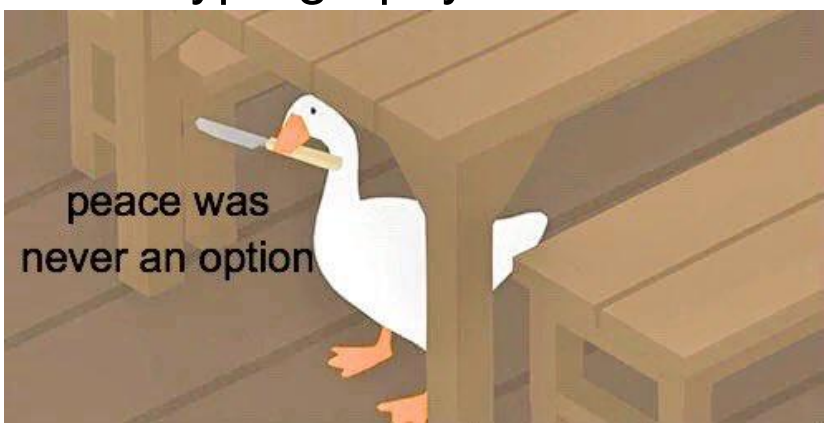
Post-Quantum Cryptography

Is this enough to make cryptography secure?



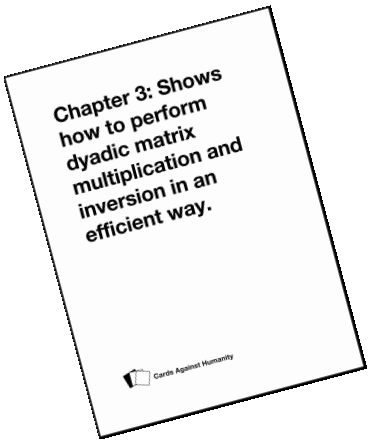
Post-Quantum Cryptography

Is this enough to make cryptography secure?

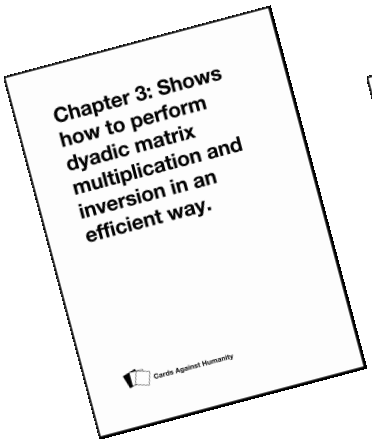


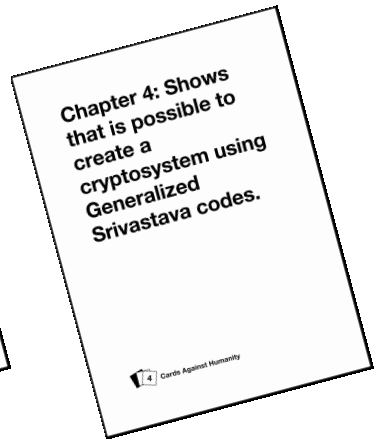
- Evaluate the current cryptoschemes for mistakes;
- Check if the current parameters are secure;
- Use quantum cryptanalysis:
  - Check how to use quantum algorithms;
  - Estimate how big a quantum computer needs to be to run a quantum algorithm;
  - Develop new quantum algorithms.

Post-Quantum Cryptography

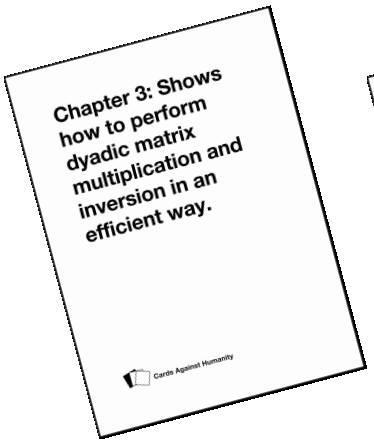


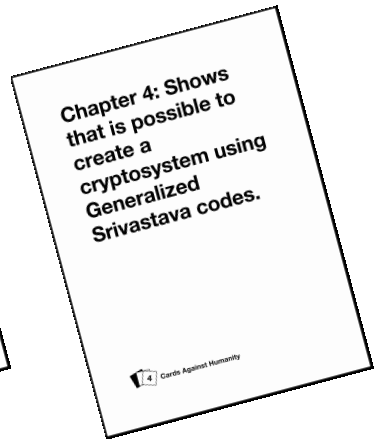
Post-Quantum Cryptography

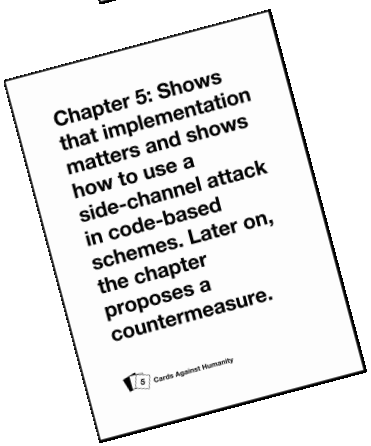




Post-Quantum Cryptography

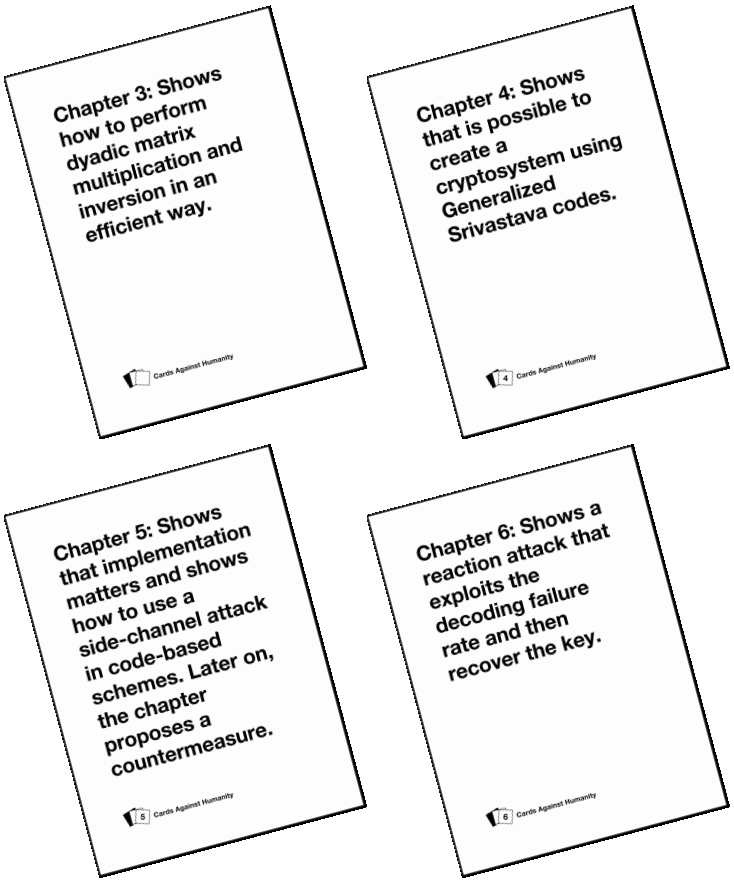






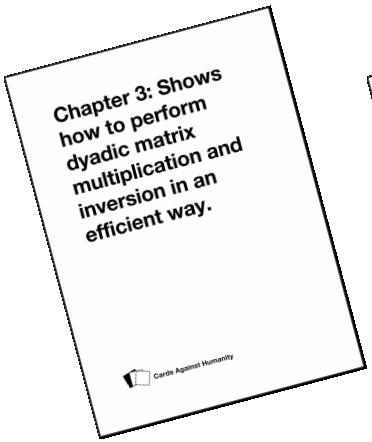
Defense Against Committee

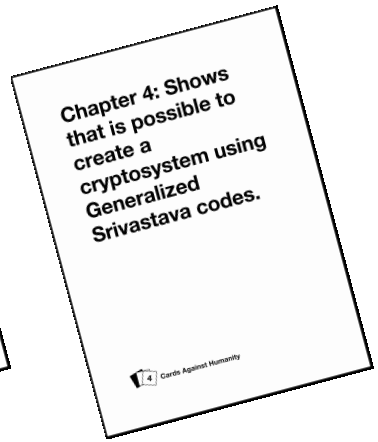
Post-Quantum Cryptography

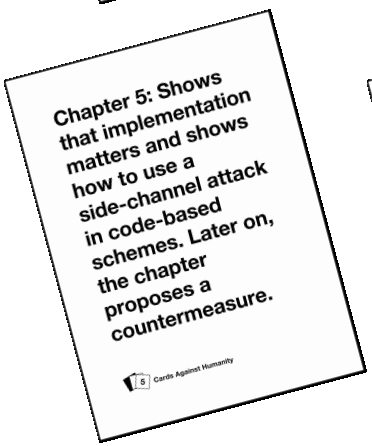


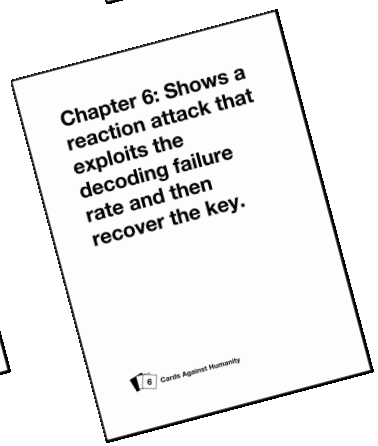
Post-Quantum Cryptography

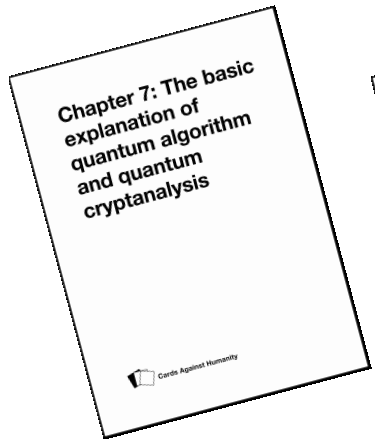
Post-Quantum Cryptography

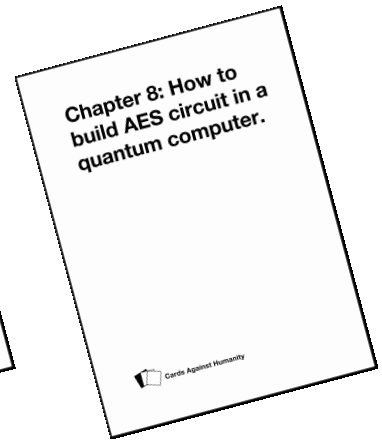






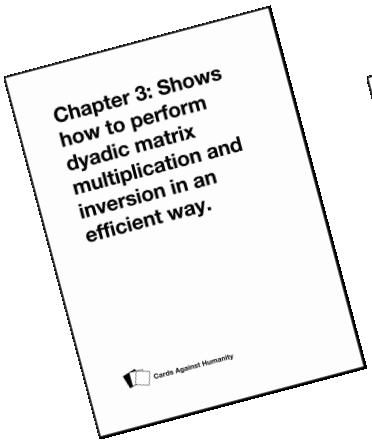


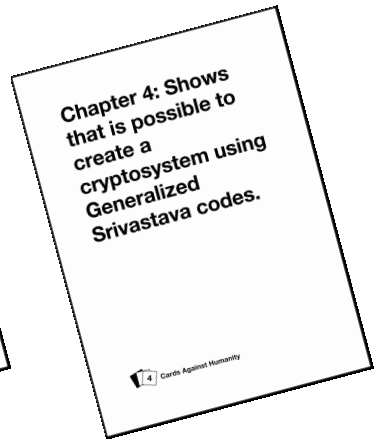


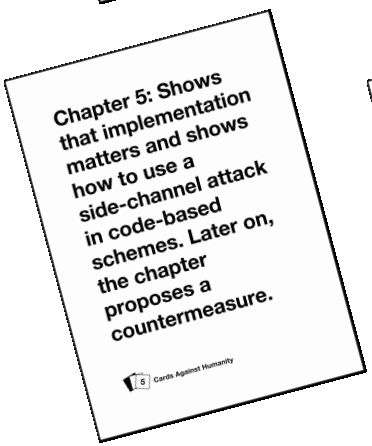


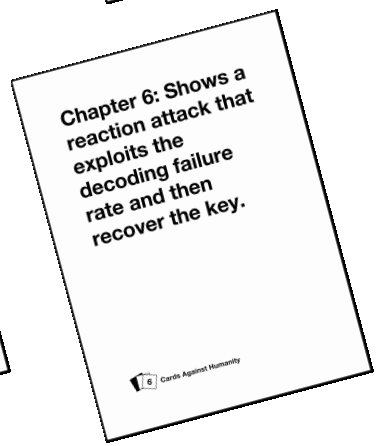
Defense Against Committee

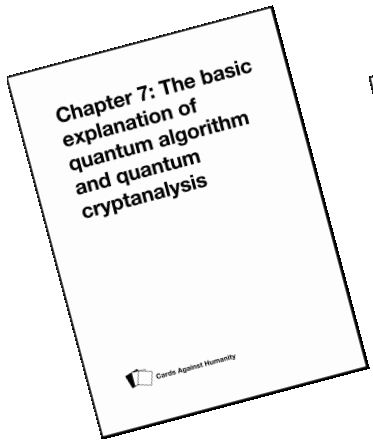
Post-Quantum Cryptography

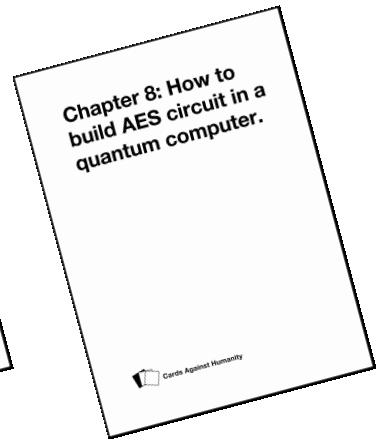












Defense Against Committee

Post-Quantum Cryptography

Selected Constructive and Destructive Approaches to Post-Quantum Cryptography

Gustavo Souza Banegas

Technische Universiteit Eindhoven
gustavo@cryptme.in

November 12, 2019

Defense Against Committee