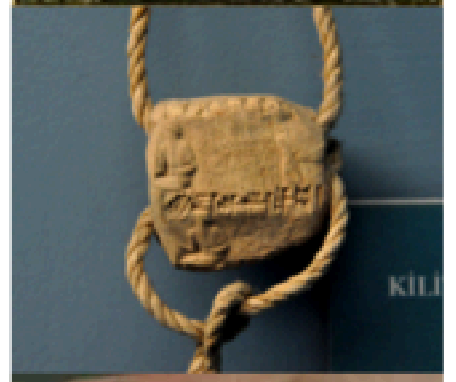
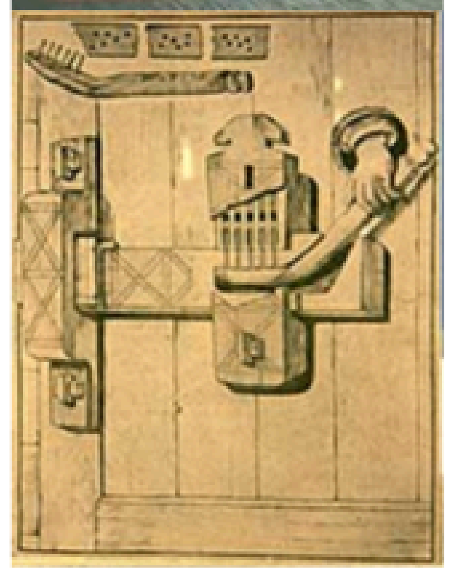
Our first attempts at security involved putting large boulders in front of our caves to keep intruders out. This worked great, until someone figured out how to move them. This started us on the repetitive journey throughout history to **find the better lock.**

Who Moved My Rock?

Post-Quantum Cryptography and its Impact on Higher Education



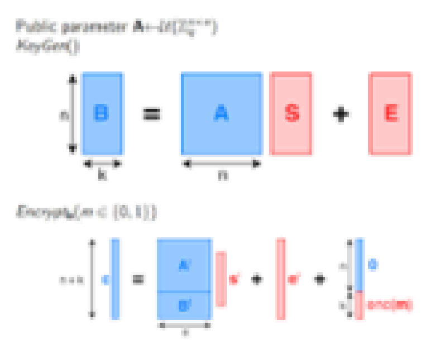


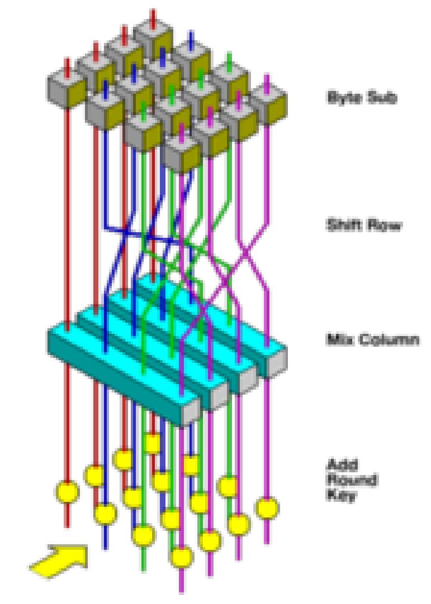
Problem: Quantum computers combined with Shor's Algorithm can lead to significant improvements in factoring large composite numbers to their prime factors. This has the **potential for making current cryptographic protocols obsolete and easily broken.**

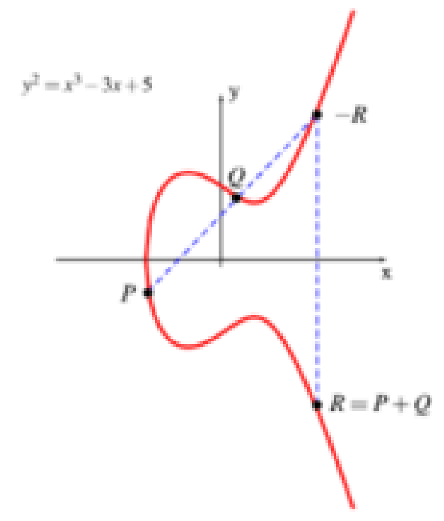
Challenge: What can we do about it? NIST has been working on standardizing Quantum-Safe Cryptography (QSC) for over a decade (timeline below). The final candidates are being scrutinized and should be ready in 2024. **Don't panic**; continue to focus on your current security program. Just stay informed, and **be ready for the changes that are coming**.

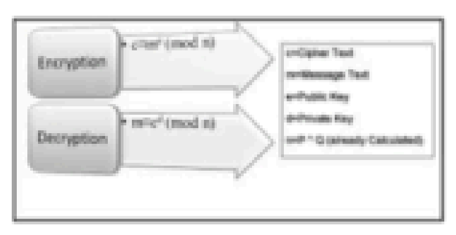
Next Steps: We have been here before. We have replaced many cryptographic protocols in the past, like DES, RC4, MD5, SHA-1, etc. Our cryptographic libraries are ready to utilize new Quantum-Safe Cryptography (QSC) once the NIST standards are complete. As a community, we should continue the discussion to determine our next steps.

?









1977

Rivest, Shamir, and Adleman designed the RSA algorithm which uses the idea that prime factorization is difficult.

1994

Peter Shor designs an algorithm that can factor integers into its prime counterparts quickly by utilizing a quantum computer with a large number of qubits.

2001

IBM shows that Shor's algorithm can work on a quantum computer with 7 qubits. It was able to factor 15 into 3 x 5.

2009

NIST publishes a survey for protocol designers. The survey says, "it does not appear inevitable that quantum computing will end cryptographic security as we know it."

2012

NIST formally begins the Post Quantum Cryptography Project.

Prime factorization of 21 into 3 x 7 was achieved.

2015

NIST holds 1st PQC Workshop.

NSA states that transitioning to quantum resistant algorithms is in the not too distant future.

2016

NIST publishes 1st report on PQC (8105). Deadlines for submissions of round one due in 2017.

2019

NIST holds 2nd PQC Workshop.

Attempt to factor 35 into primes fails due to accumulating errors.

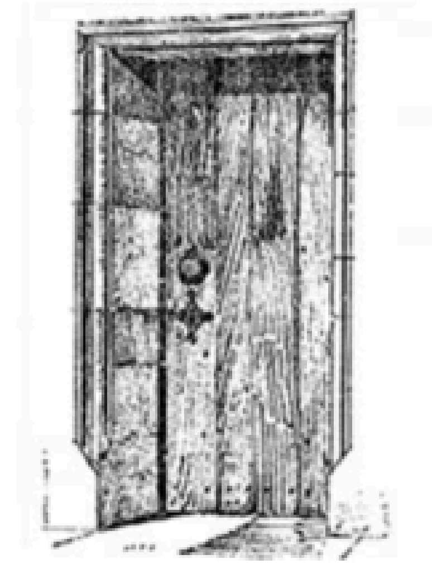
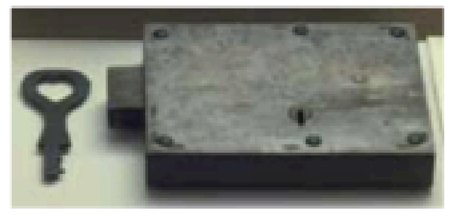
2021 & 2022

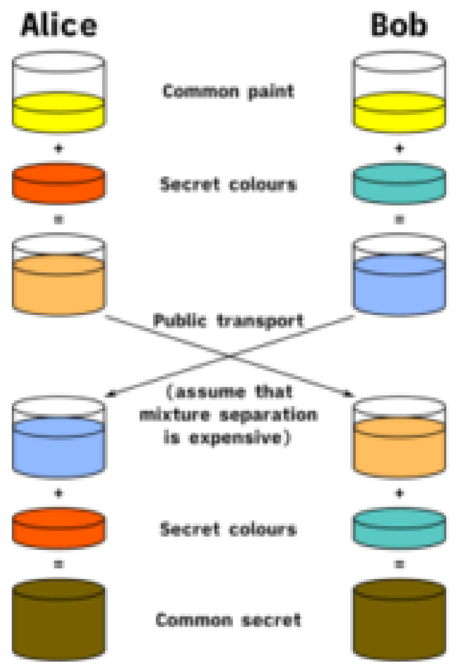
NIST holds 3rd & 4th PQC Workshop.

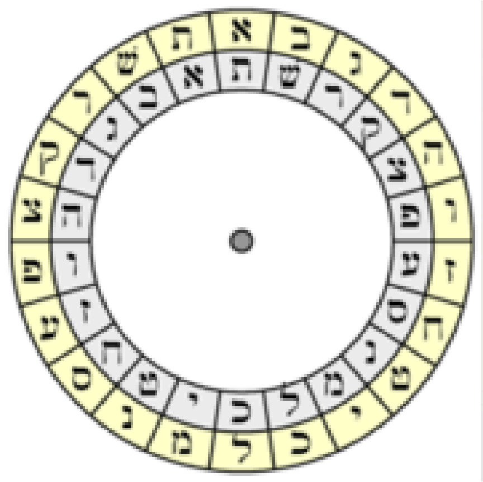
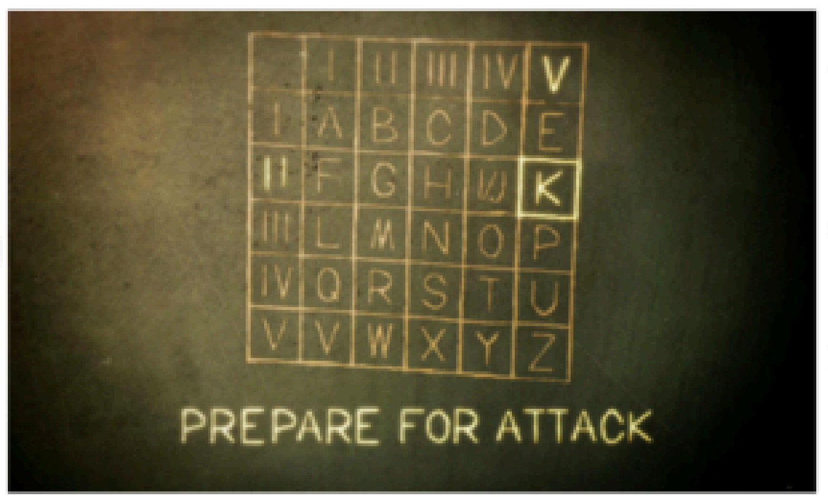
Draft standards made, algorithms selected for QSC (CRYSTALS-KYBER, CRYSTALS-DILITHIUM, FALCON, SPHINCS+).

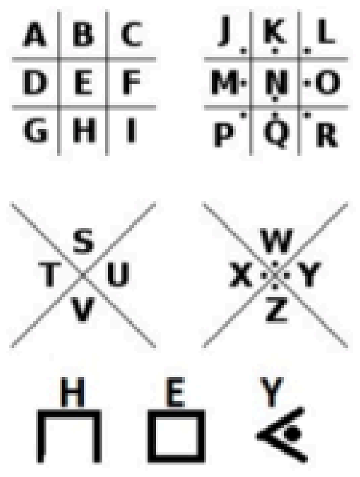
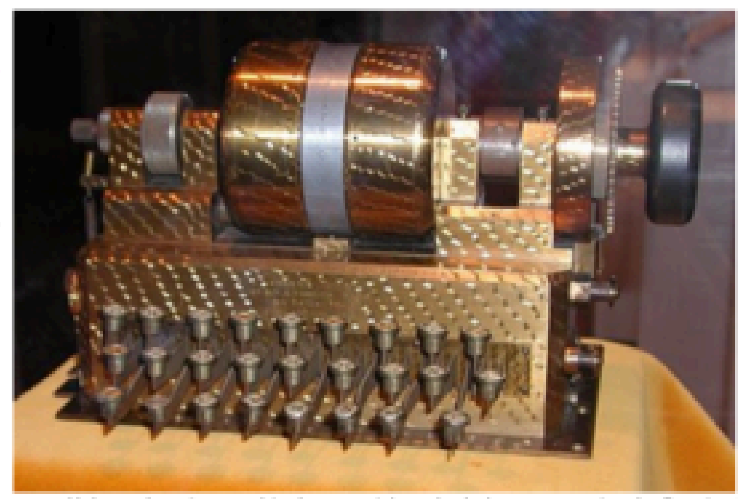
2024

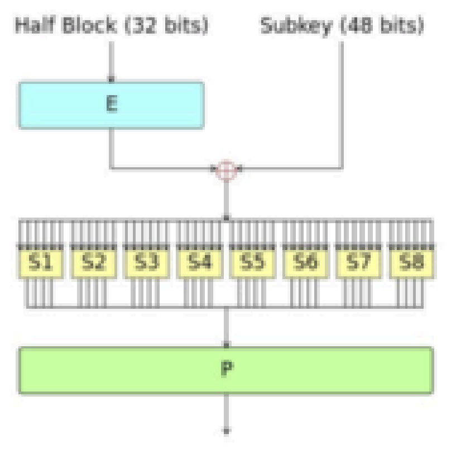
NIST announced that it will integrate the four selected post-quantum algorithms into U.S. encryption standards





Author: Brian Epstein <bepstein@ias.edu> Institute for Advanced Study © 2023 https://security.ias.edu