Post-Quantum Cryptography:
We have the algorithms, what next?

Emma Morrison University of St Andrews em406@st-andrews.ac.uk

University of St Andrews

Why do we need Post-Quantum Cryptography?

Conventional computers only allow bits to be in one of two states: 0 or 1. All of our previous algorithms are designed using this principle. Quantum computers, however, are composed of qubits (quantum bits), which can be in multiple states at once: a superposition. Small proof-of-concept quantum computers have been built, and benefits are already being seen, for example in medical imaging. We can also design algorithms to run on quantum computers, taking advantage of the properties of qubits. One of these is Shor's algorithm, which computes the prime factorisation of a number far quicker than the best conventional algorithms. RSA is a cryptographic system used on the internet for exchanging keys. An RSA key pair can theoretically be broken in minutes on a suitably powerful quantum computer using Shor's algorithm. Therefore, once quantum computers can run Shor's algorithm on numbers of the size used in RSA it will no longer be secure.

What is Post-Quantum Cryptography (PQC)?

Post-quantum cryptography is the family of encryption systems that can be used with conventional computers and are not vulnerable to attack from quantum computers.

What are the case studies?

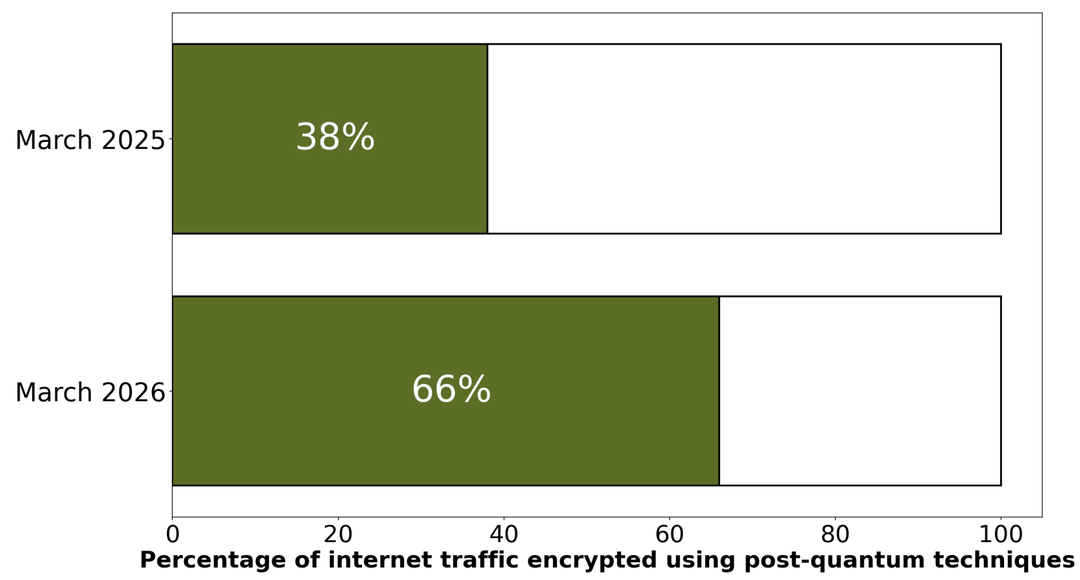
DES (Data Encryption Standard): DES was NIST's* symmetric-key encryption standard until the early 2000s. Throughout the late 1990s, as computers increased in speed, it was broken multiple times on various different systems, resulting in its deprecation.

The Y2K Bug: This was a date representation issue that was predicted to cause widespread problems at the turn of the millennium. Every line of code on every computer system had to be checked, costing hundreds of billions of dollars [1].

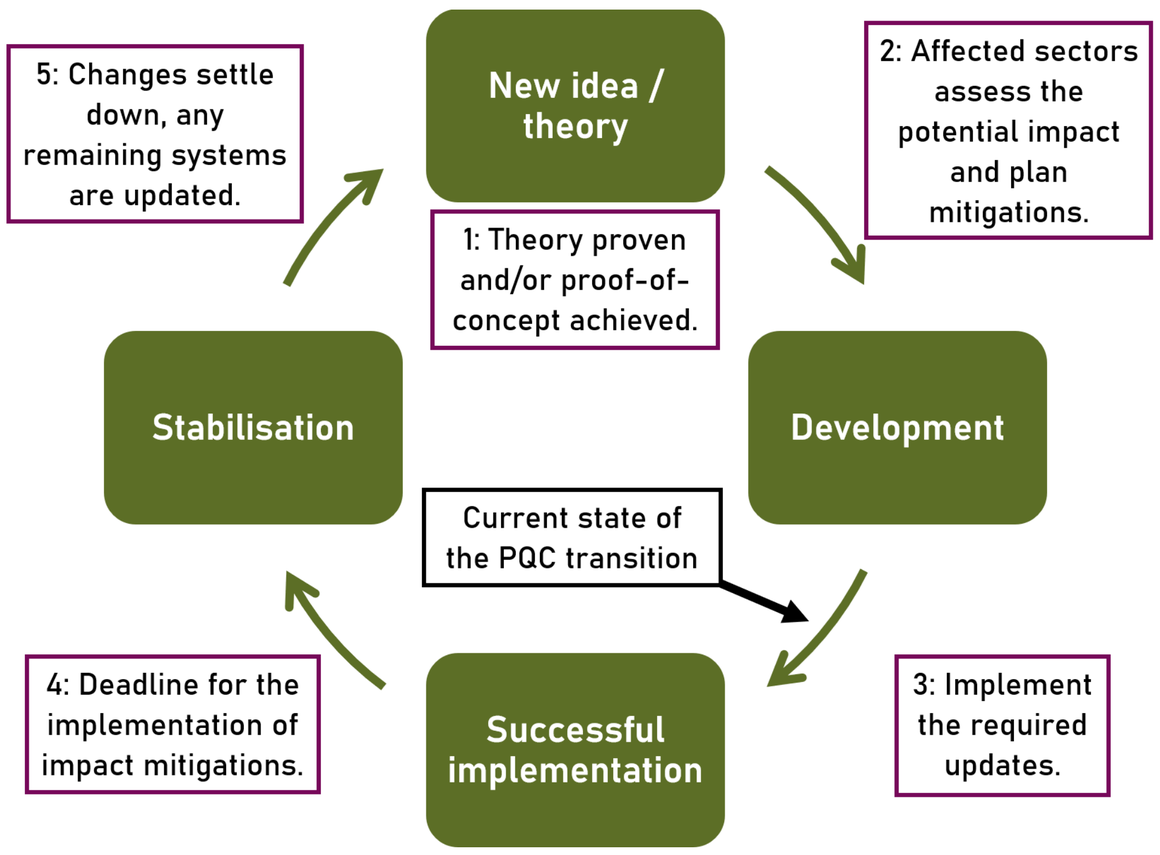
*US National Institute of Standards and Technology

Where are we now?

The proportion of internet traffic encrypted using PQC has increased in the past year [2], which is promising, but there is still a large amount of traffic unprotected, and therefore at risk for "store now, decrypt later" attacks.



The Cycle Of Cryptographic Development



1: Once computers were fast enough to break DES, it was provably no longer secure, so there was no "proof-of-concept" stage. However, RSA's vulnerabilities are entirely hypothetical until a sufficient implementation of Shor's algorithm is achieved.

2: NIST updated their standards to replace DES, just as they have for PQC.

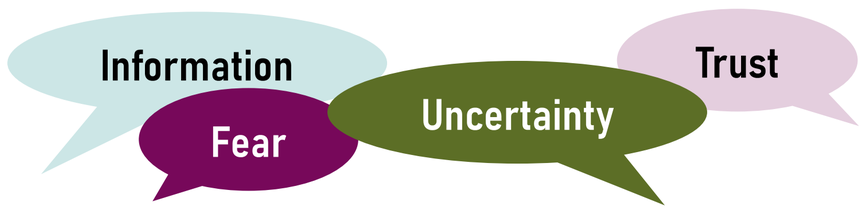
3: The uncertainty in the capabilities of quantum computers in the near future means that organisations need to be able to adapt quickly. This could be especially difficult for smaller organisations. Training programmes and a focus on lower-cost implementations of updates are some possible solutions [3].

4: The timing for this deadline is currently very uncertain, and some academics believe that quantum computers will never be able to break RSA.

5: Even if the initial transition is successful, the stabilisation phase may be very short if the initial success leads to a cascade of new algorithms or engineering improvements which create new vulnerabilities. Furthermore, if the number of people that are able to do security audits on quantum technology is low, problems in systems might slip through the cracks. Once quantum computers become more widely accessible, attackers will also be able to look for new exploits, and defensive capabilities need to be able to keep up.

The Impact of Public Opinion on Next Steps

- There were fears when DES was brought in as a standard that the NSA (US National Security Agency) had built a backdoor into it. This appears not to be the case, but the Snowden leaks revealed that the NSA had put a backdoor into a new system for pseudo-randomness that they then recommended for adoption [4]. These memories may contribute to a lack of trust in organisations such as the NSA during the transition to PQC.
- After Y2K, some people thought the issue had been a hoax set up by the companies that were offering services to help fix the problem. These opinions stemmed from the fact that there were far fewer system failures than predicted by many analysts [1]. Unfortunately the "ideal solution" in the PQC transition is similarly anti-climactic, in a perfect world the majority of internet users shouldn't know that anything has changed. This provides a seamless transition, but it makes it hard to know if your data is protected.
- The internet is involved in almost every aspect of our lives, from commerce to logistics to entertainment. A breakdown of trust in the organisations responsible for technology or a perceived increased risk of attacks could make people reluctant to do things like online banking.
- Keeping the public informed about new developments will be key in maintaining trust in organisations and systems.



References

[1] Manion, M., & Evan, W. M. (2000). The Y2K problem and professional responsibility: a retrospective analysis. *Technology in Society*, *22*(3), 361-387.

[2] Cloudflare (2026, March 1). Cloudflare Radar: Post-quantum encryption adoption, https://radar.cloudflare.com/post-quantum?dateRange=52w

[3] Okika, N., Nwatuzie, G. A., Olarinoye, H. S., Nwaka, A. A., Igba, E., & Dunee, R. (2025). Assessing the Vulnerability of Traditional and Post-Quantum Cryptographic Systems through Penetration Testing and Strengthening Cyber Defenses with Zero Trust Security in the Era of Quantum Computing.

[4] Landau, S. (2015). NSA and Dual EC_DRBG: Déjà Vu All Over Again?. *The Mathematical Intelligencer*, *37*(4), 72-83.