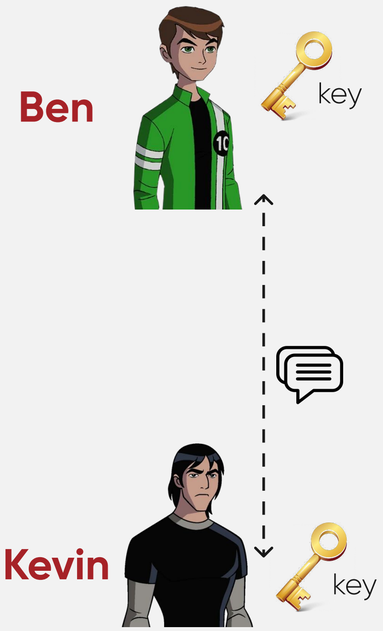
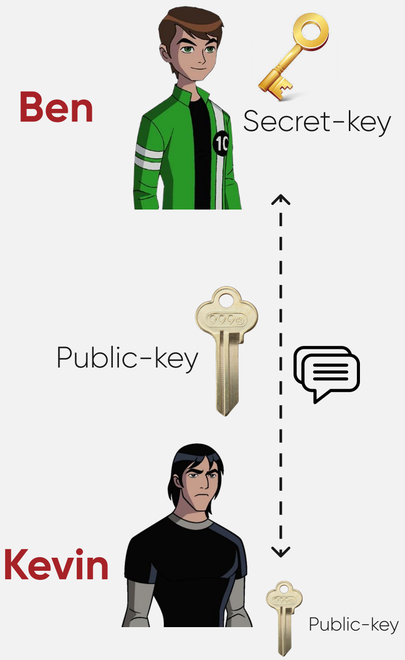
Post-Quantum Cryptography

Private-Key Cryptography

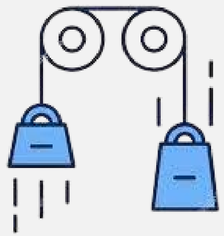


Public-Key Cryptography

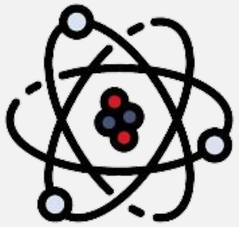


But Quantum Computers can break existing Public-Key crypto-schemes

~Peter Shor

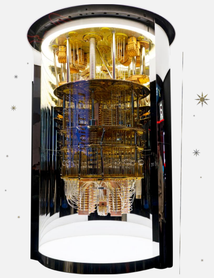


Classical Physics
(17th Century)



Quantum Physics
(20th Century)

Classical Computers
(20th Century)

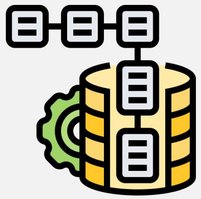


Quantum Computers
(In Progress)

- Does this mean security on internet is broken?
- Not yet, Quantum Computers are still in their very early stages.
- So why do we even need to worry?

Lots of funding and research towards building quantum computers

Takes a long time to deploy any cryptographic primitive on the internet. (10+ years)



Harvesting Attacks :
Attackers can store sensitive ciphertexts now, and use future quantum computers to decrypt them.

Post Quantum Cryptography :
Design cryptosystems that are resilient/ safe against quantum computing attacks.

~Shankh Gupta
CSE Dept.