The Impact of Quantum Computing on Cryptography

Tara O’Kelly

Introduction to Cryptography

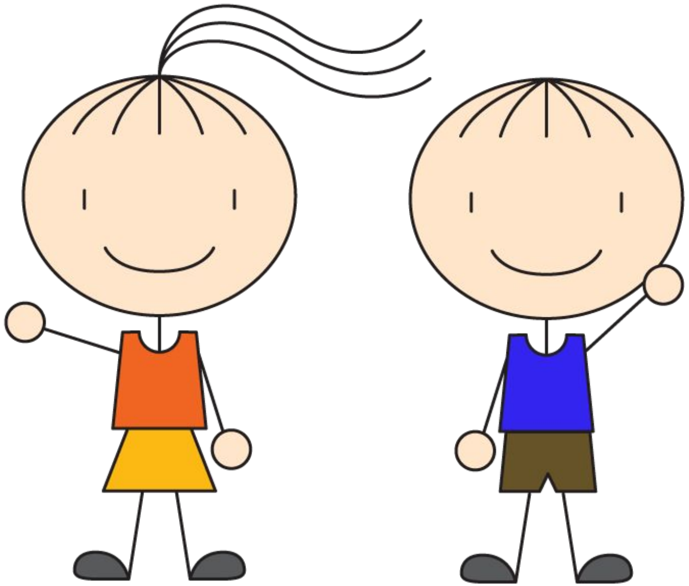
Confidentiality

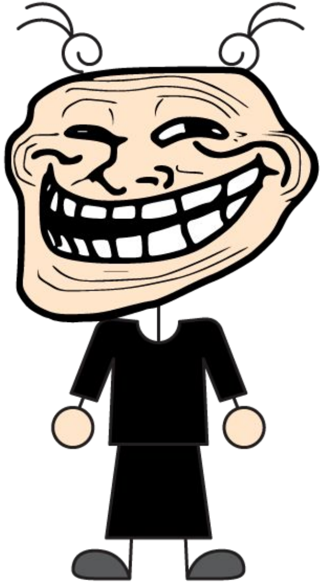
Integrity

Authenticity

Non-repudiation

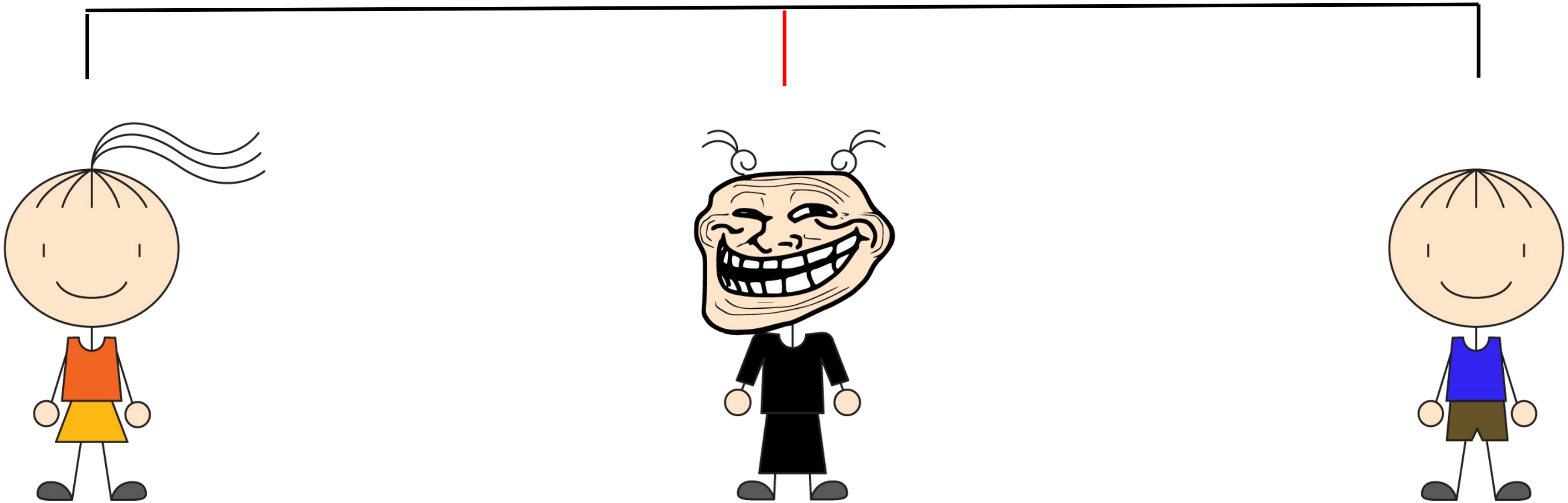
Meet Alice, Bob and Eve



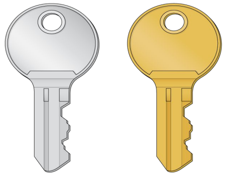


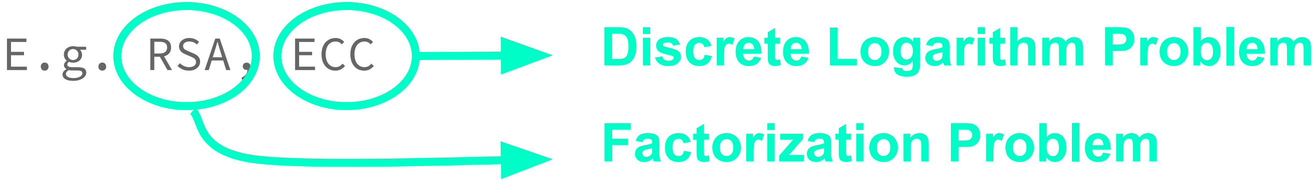
Symmetric Key Encryption

E.g. AES



Asymmetric Key Encryption

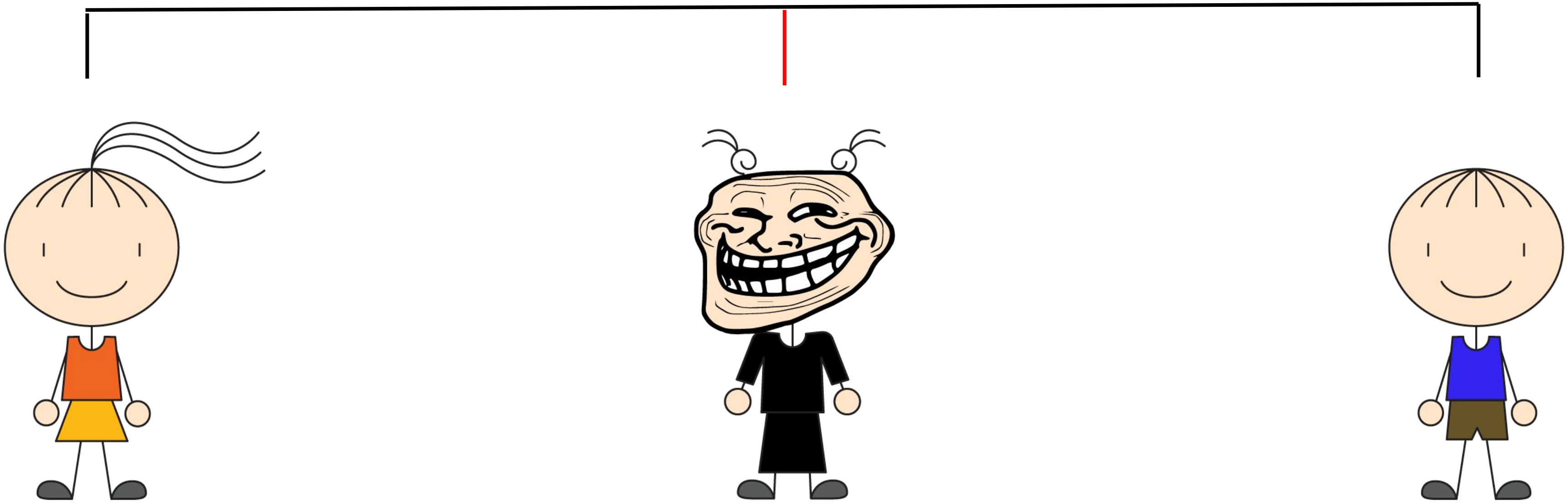




E.g. RSA, ECC

Discrete Logarithm Problem

Factorization Problem



Quantum Algorithms

Shor's Algorithm

Factorization

Discrete Logarithm Problem

C:

$$O(c^N)$$

Q:

$$O(N^c)$$

Grover's Algorithm

Unordered Search

C:

$$O(N)$$

Q:

$$O(\sqrt{N})$$

Impact On Current Cryptographic Systems

Symmetric cryptography

AES	Encryption	Damaged	Grover
GMAC	MAC	No impact	Grover
SHA	Hash Function	Damaged	Grover

Asymmetric cryptography

RSA	Encryption/Signature	Broken	Shor
ECC	Encryption	Broken	Shor
DSA	Signature	Broken	Shor
ECDSA	Signature	Boken	Shor

Security Implications

~~Confidentiality~~

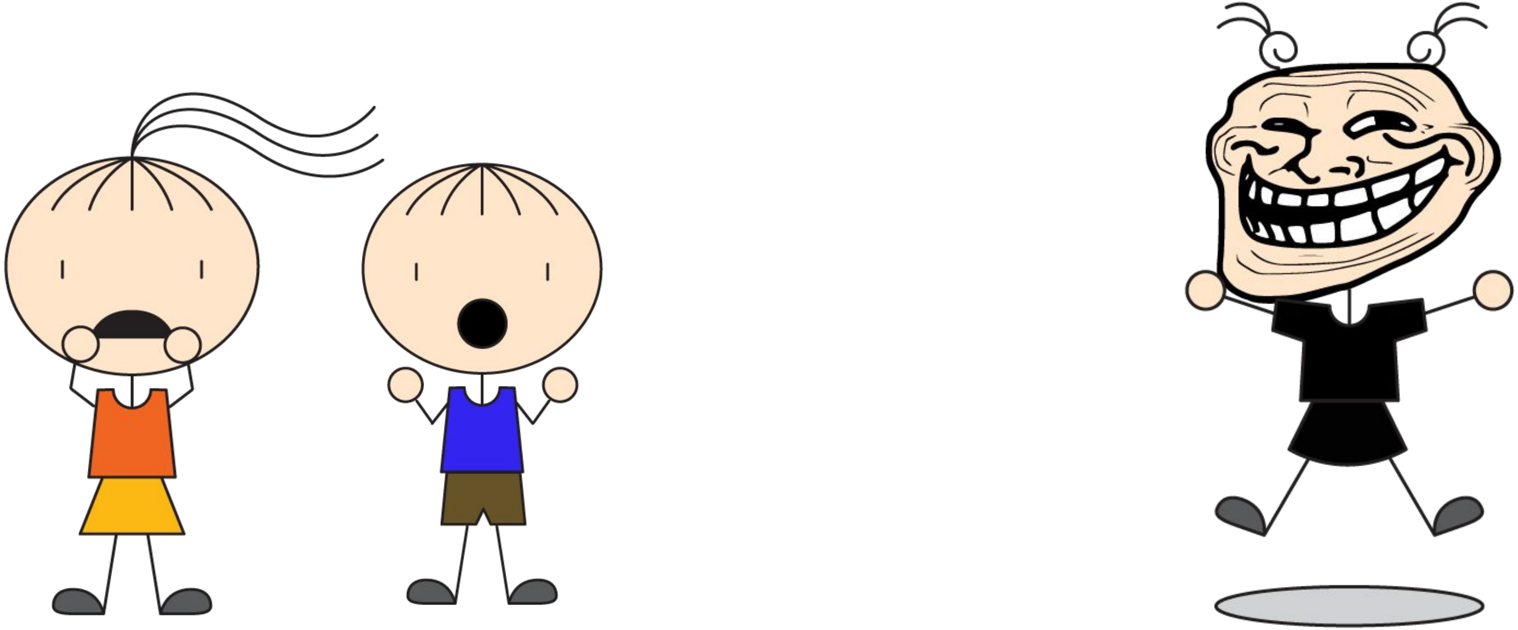
~~Integrity~~

~~Authenticity~~

~~Non-repudiation~~

So When Will Quantum Computers Arrive?

… They're already here



Post-Quantum Cryptography

Classical Solutions

- Code-based encryption
- Lattice-based encryption/signatures
- Multivariate-quadratic equation signatures
- Hash-based signatures

Quantum Solutions

- Quantum Key Distribution (QKD)

Will We be Prepared on Time?