Cybersecurity

Quantum Cryptography and Ephemeral Keys

Quantum

- The least amount of any physical entity required for an interaction

- Quantum Communications
  - Field of applied quantum physics
  - Related to quantum information and quantum teleportation
  - Protects against eavesdropping

- Quantum Computing
  - Uses quantum phenomena to perform computations
  - Computer that can do quantum computing is known as a quantum computer

Quantum Cryptography

- The science of using quantum phenomena to perform cryptography
  - Tasks that were thought to be impossible with classic cryptography

- Post-quantum cryptography
  - Cryptographic algorithms thought secure against attacks orchestrated by a quantum computer

Ephemeral Keys

- Cryptographic key that is generated with each execution of a key
  - Ephemeral can be defined as lasting a very short amount of time

- Opposite of static key
  - A static key is used for a long period of time

CYB=R.ORG