Summarise Crypto techniques

Quantum and Post Quantum

Quantum Computing

- Is able to utilize a huge number of state Variables represented as Qubits.

- When 1 Qubit is read, it collapses to either 0 or 1. So do all the other entangled qubits.

- Quantum bits (qubits), Superposition, entanglment and collapse

↓ either 1 or 0

↓ weighted middle position

↓ 1 affects the rest

Used for:

- factoring problem (RSA encryption)

- Discrete logarithmic problems (ECC)

- Communications
  - Tamper-evident key distribution

Post Quantum

- Anticipating challenges to current cryptographic Implementations, where the attacker has access to many Qubits.

↳ Quantum - based cryptanalysis

- Worlds biggest Quantom Computer has 50 Qubits.

Cryptographic agility

- The ability to update specific algorithms used across a range of security devices without interrupting the flow of business

Light weight Cryptography

- Used in low power devices

Homomorphic encryption

- Supports data analytis done by third party Companies while keeping the Information Encrypted.

Block Chain

- Expanding list of transactional records (blocks)
- Each block is linked by hashing all the previous blocks and adding that hash to the new block
- Public ledger

- Record of transactions
- P2P transactions are public
- Transactions Can not be deleted of reversed.

- Used for Crypto Currency

- Potential Uses:
  - Finance
  - Online Voting
  - ID mangment systems
  - Data Storage
  - Notarization

(security by Obscurity)

Stegnography

Covertext = The medium / Container that holds the hidden message

- Technique to Conceal messages within a covert text.
- Use file data that can be manipulated without Introducing Obvious artifacts.
  - Image
  - Audio
  - Video

  } change the least significant bits when hiding message

Uses for Stegnography:

- Provide integrity or non-repudiation (Real / Fake)
  (show that something was printed at a particular time) → e.g money
- Used to create Covert channels (hiding messages in TCP packets)
- C2C
- Exfilterating Data covertly
- Bypass protection mechanisms (DLP's)
  ↳ Data loss prevention