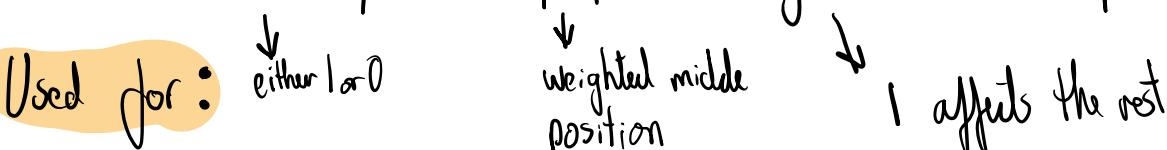


Summarise Crypto techniques

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, entanglement and collapse


Used for : ↓ either 1 or 0 ↓ weighted middle position → 1 affects the rest
- 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

- World's biggest Quantum 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 analytics 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 or reversed.

- Used for Cryptocurrency

- Potential Uses :

- Finance
- Online Voting
- ID management Systems
- Data Storage
- Notarization

(Security by Obscurity)

Steganography

CoverText = The medium / container that holds the hidden message

- Technique to conceal messages within a cover 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 Steganography:

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