

# Cybersecurity

## Common Cryptography Use Cases



# Finding the balance

- Low power devices
  - Portable electronics (mobile phone, tablet, etc...)
  - Elliptical curve cryptography is very common
- Low latency
  - Time constraints
  - Stream ciphers are commonly used for their speed
- High resiliency
  - Functions capable of resuming normal operations after disruption
  - Hashing can help protect the data



# Use cases

- Supporting Confidentiality
  - Keeping the data private
  - This is the backbone of all cryptography
- Supporting Integrity
  - Important during transfers
  - Data has not been altered
  - Hash functions can be used to support integrity
- Supporting Obfuscation
  - Protect from casual observer
  - Changing names to mask their use
  - Changing the order of a PIN code to make more difficult



# Use cases

- Supporting Authentication
  - Protecting a password
  - Allowing validation
- Supporting Non-Repudiation
  - Verifying data has been sent/received
  - Private keys help with this
- Resource vs. security constraints
  - Essential step when planning cryptography implementation
  - Constant battle happening

