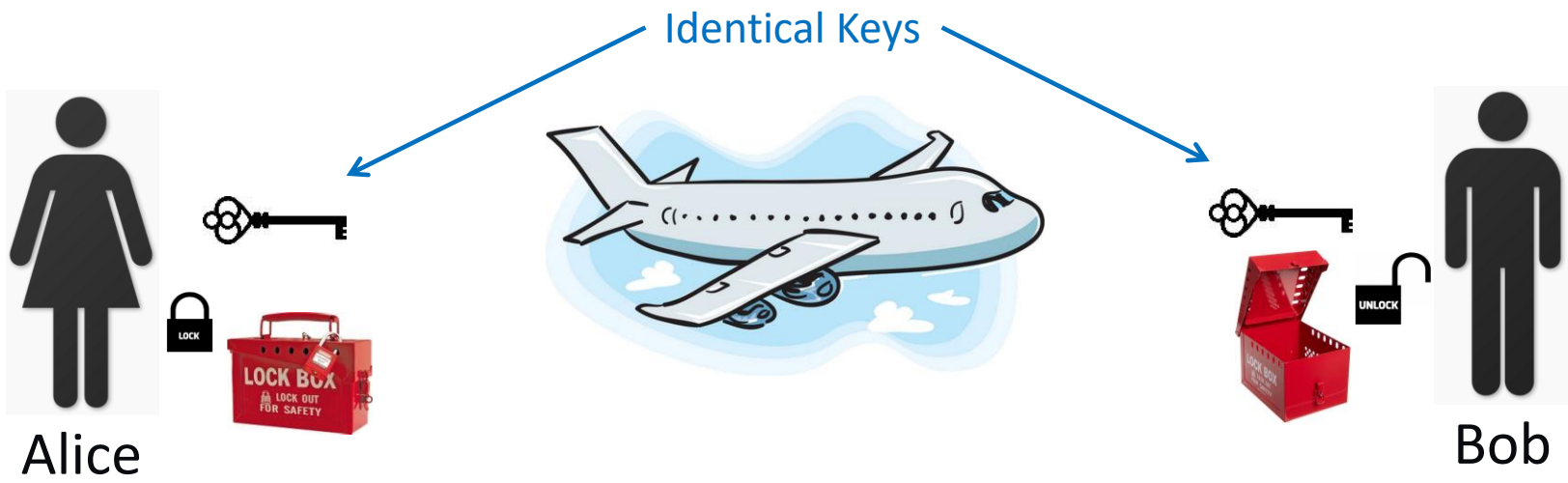
Symmetric Cryptography Primer

Presenter: Chris Kim – Senior Embedded Solutions Engineer

MICROCHIP

Symmetric Cryptography

- **Other terms for symmetric key you may encounter are:**
  - Secret-key, Shared-Key, Single-key and Parent Key
- **It is a methodology where both sides use the same secret**
  - Example: using identical keys to lock and unlock a lock-box



Key Establishment is Important

Also often referred to as “Key Exchange”

- **There are several methodologies of key establishment**
  - This method is called “Key Transport”
    - Alice and Bob know and trust each other
    - Alice securely “transports” a copy of the secret key to Bob
      - Bob is assured it is genuine and trusted based on his knowledge and trust in Alice

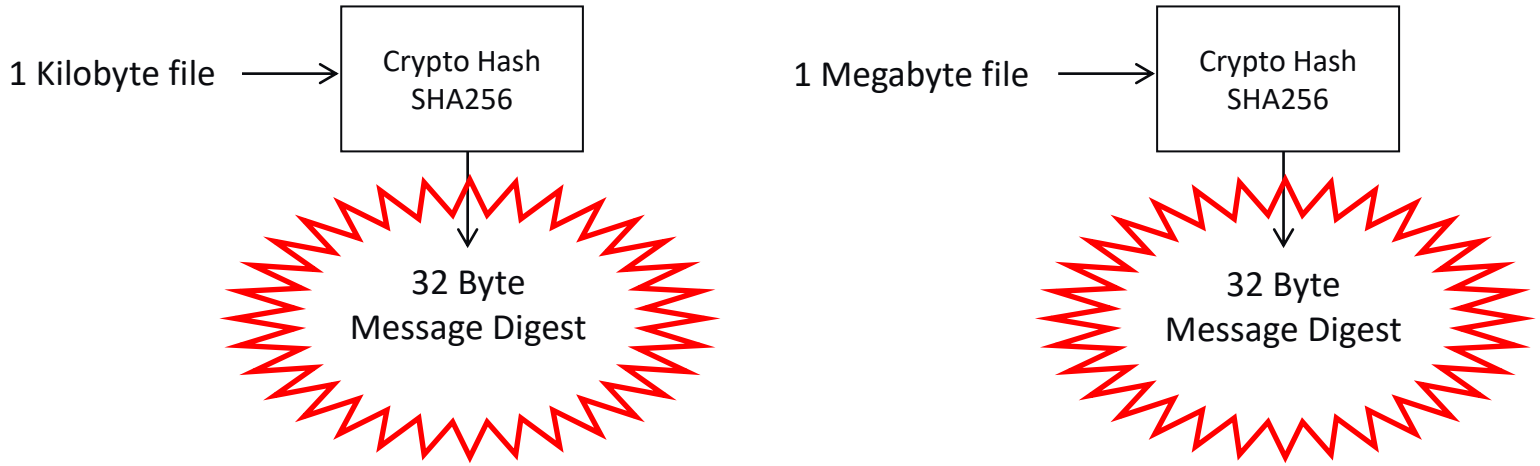
This is the simplest form of key establishment. There are other, more advanced forms of Key Establishment which can handle the case of Alice and Bob being strangers and somehow need to establish trust in each other.

The Keys Must Remain Secure

- **The vulnerability is the confidentiality of the key**
  - Are there other copies of the keys Alice didn't know about?
  - Was the exchange secure?
    - Keys delivered in this way need to be given under "relative security" so nobody else can gain any knowledge about the key
  - Does Bob value the key to the same degree as Alice?
  - Is there someone Alice or Bob trusts with the key, but shouldn't?
- **Secret key can be extremely secure, but great care must go into protecting the Shared Key**
  - Secret keys are "need to know" data
  - The number of copies should be aggressively managed

Hash: A Fundamental Building Block of Cryptography

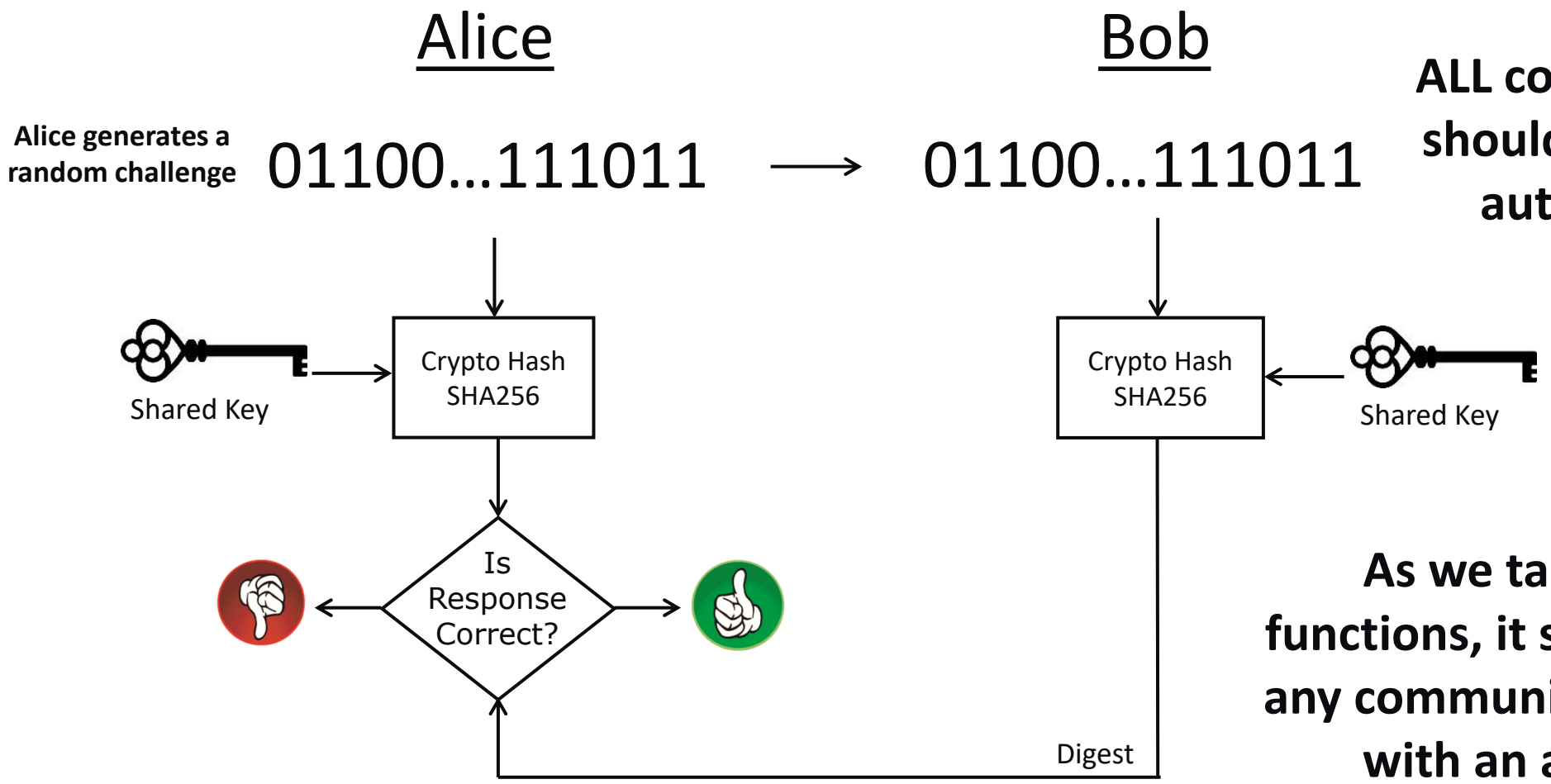
- **A crypto hash uses a strong irreversible mathematical transformation**
  - Characteristics of a strong crypto hash:
    - Easy to compute the digest
    - Infeasible to regenerate the original message
    - Infeasible to modify a message without changing the digest
    - Infeasible to find different messages with the same digest
      - Output is called a “Message Digest” and is a fixed length
    - SHA256 outputs a 32 byte digest no matter the size of input



Hash Used in Symmetric Authentication

Alice wants to authenticate a connection with Bob

Alice and Bob know and trust each other and have copies of an identical secret key

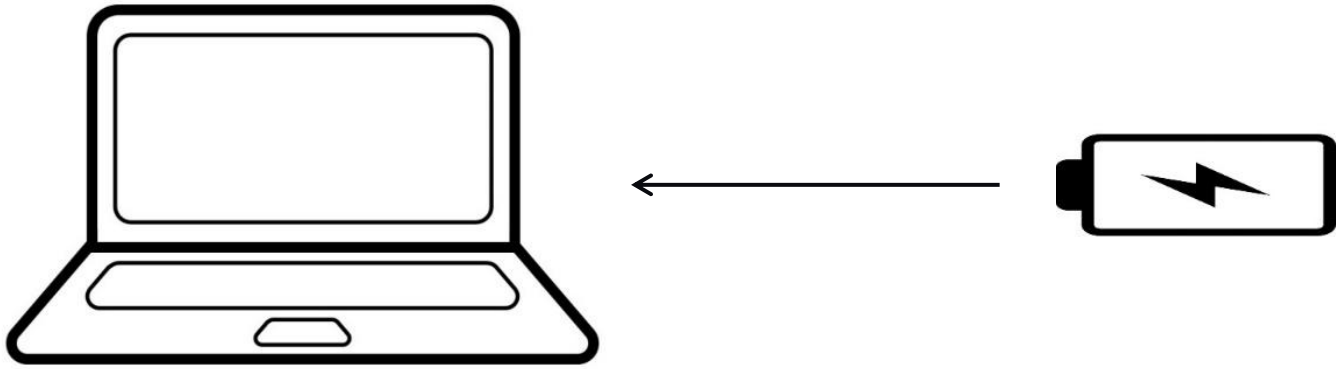


ALL communications should start with an authentication

As we talk about other functions, it should be assumed any communication first started with an authentication

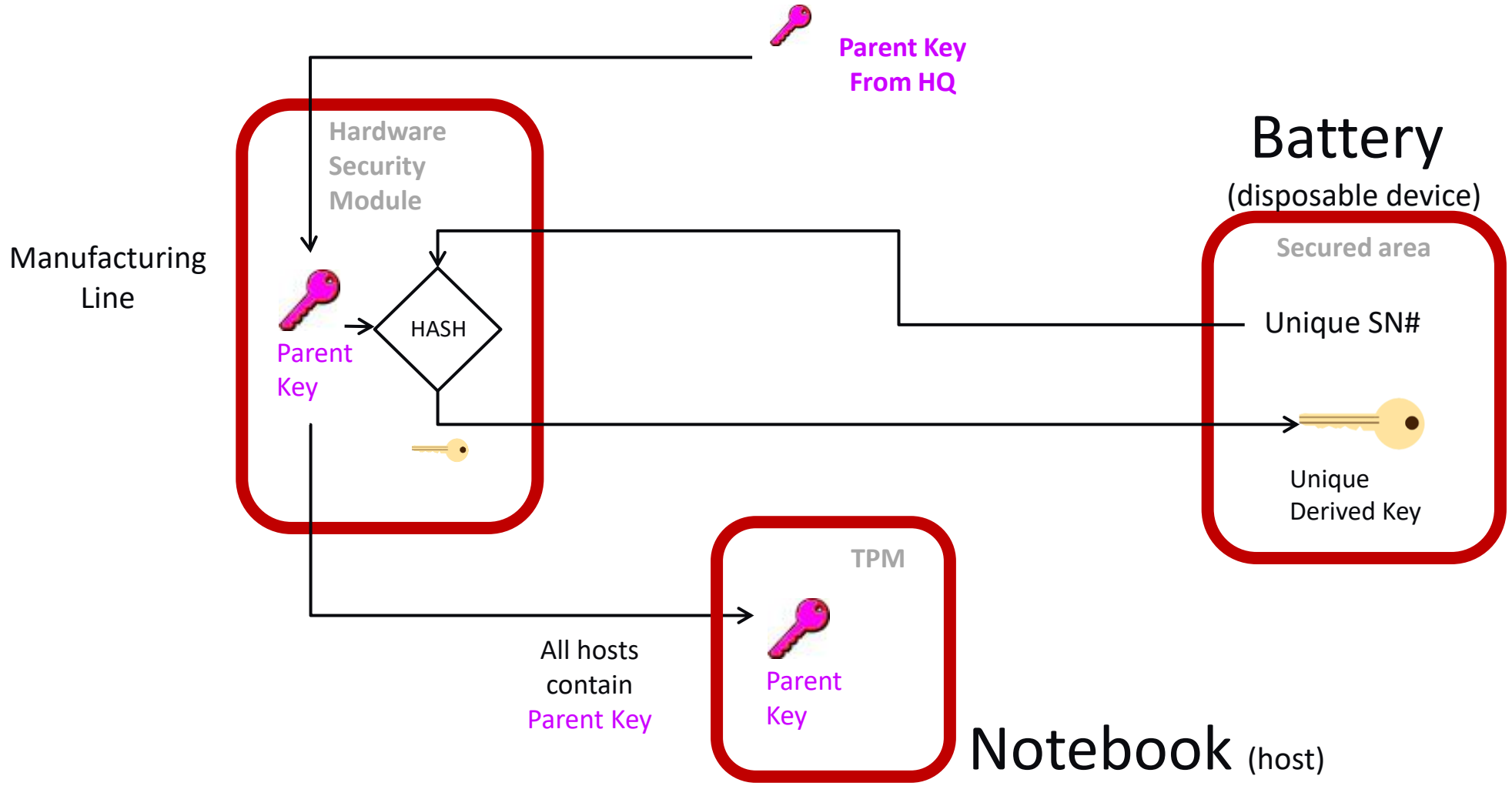
How Symmetric Authentication Would Be Implemented In a Real-World System

For Example: Authenticating a Battery



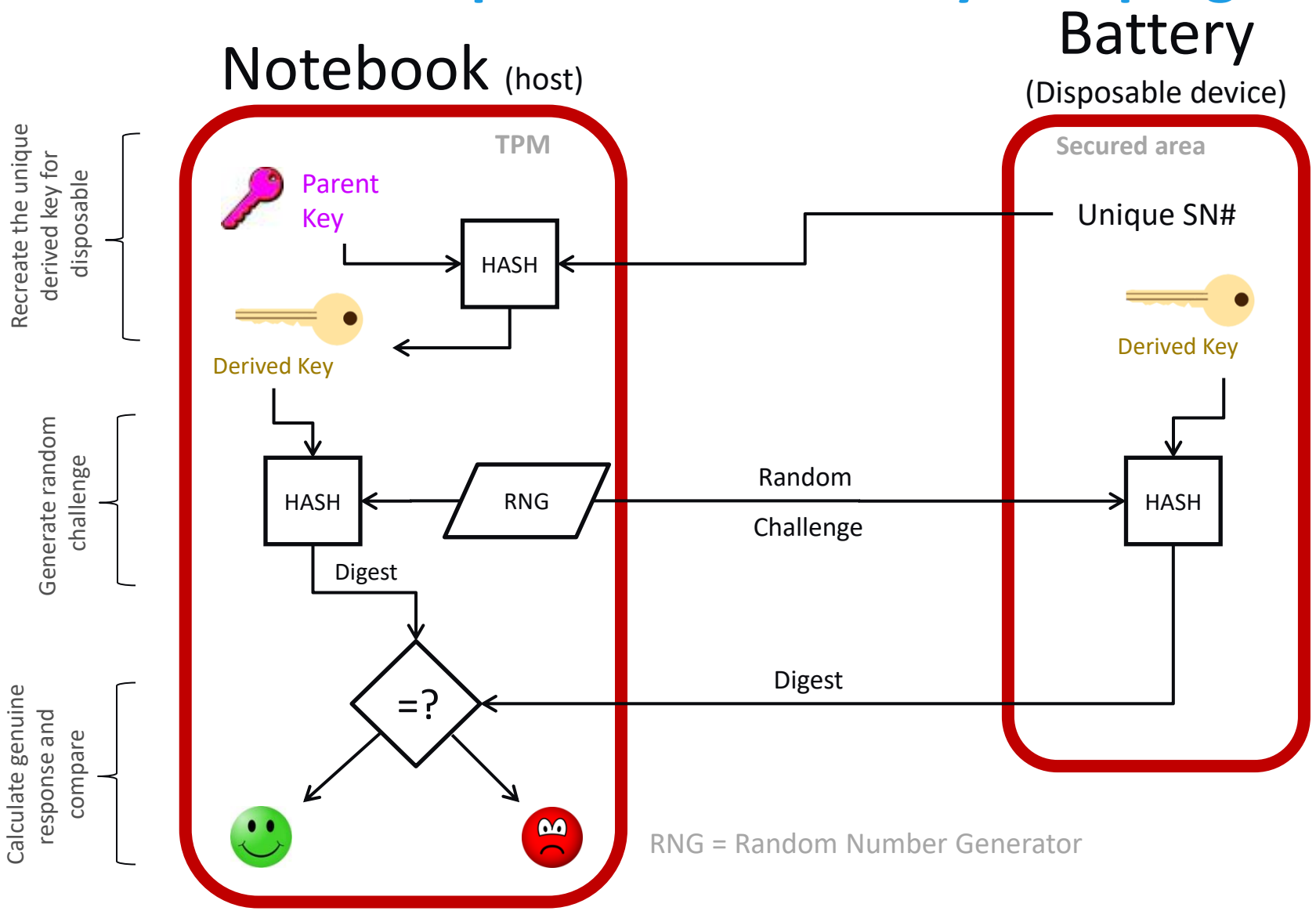
How to Provision a Disposable Device

How both disposables and hosts are prepared in the factory



The Authentication Process

The end user receives a replacement battery and plugs it in



MICROCHIP

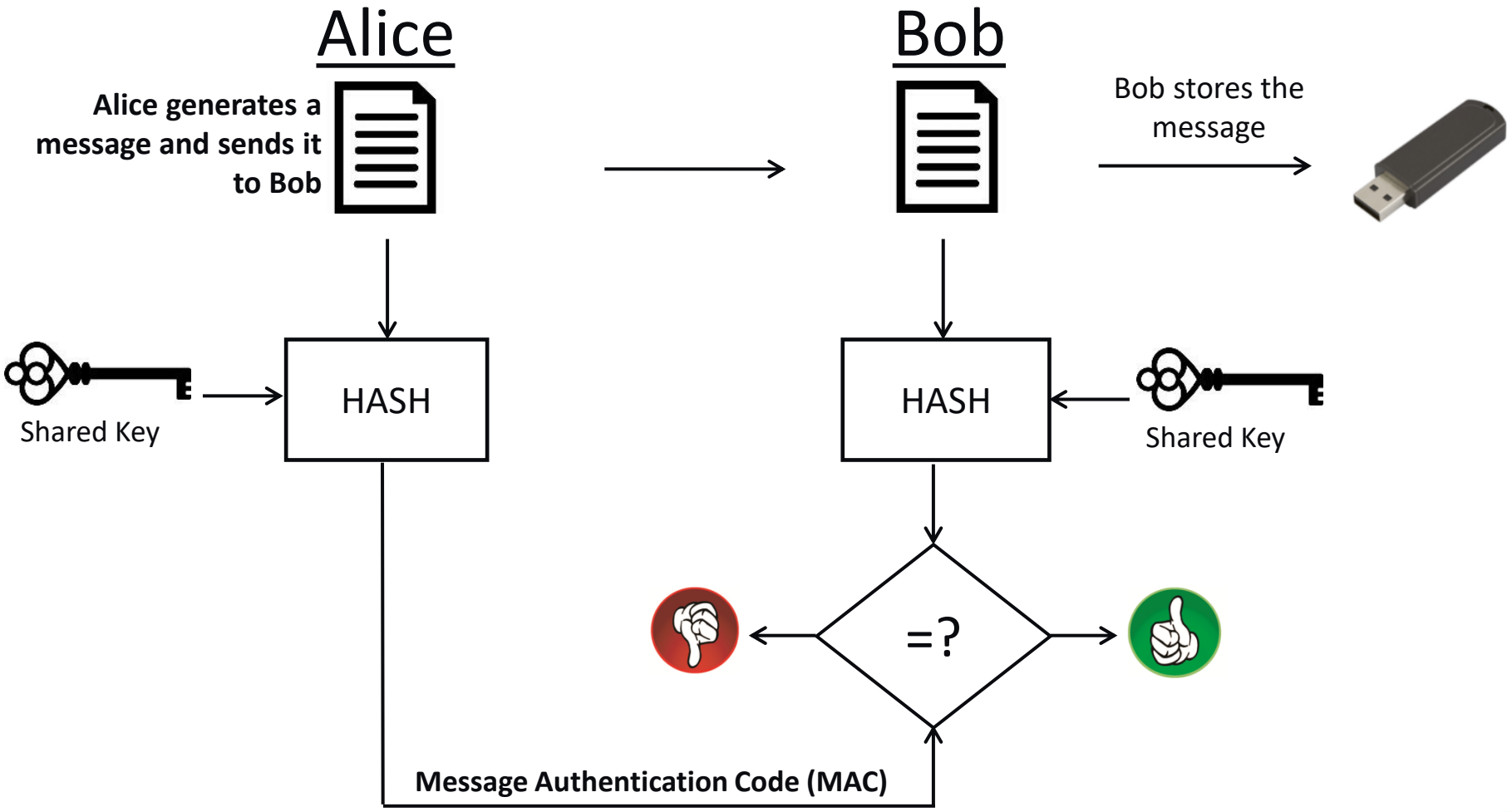
That Was “Identity Authentication”

Now Let's Use Hash for “Message Authentication”

Symmetric Message Authentication

Bob wants authentication of a message from Alice

Alice and Bob know and trust each other and share a secret key



MICROCHIP

Symmetric Cryptography to Generate Session Keys

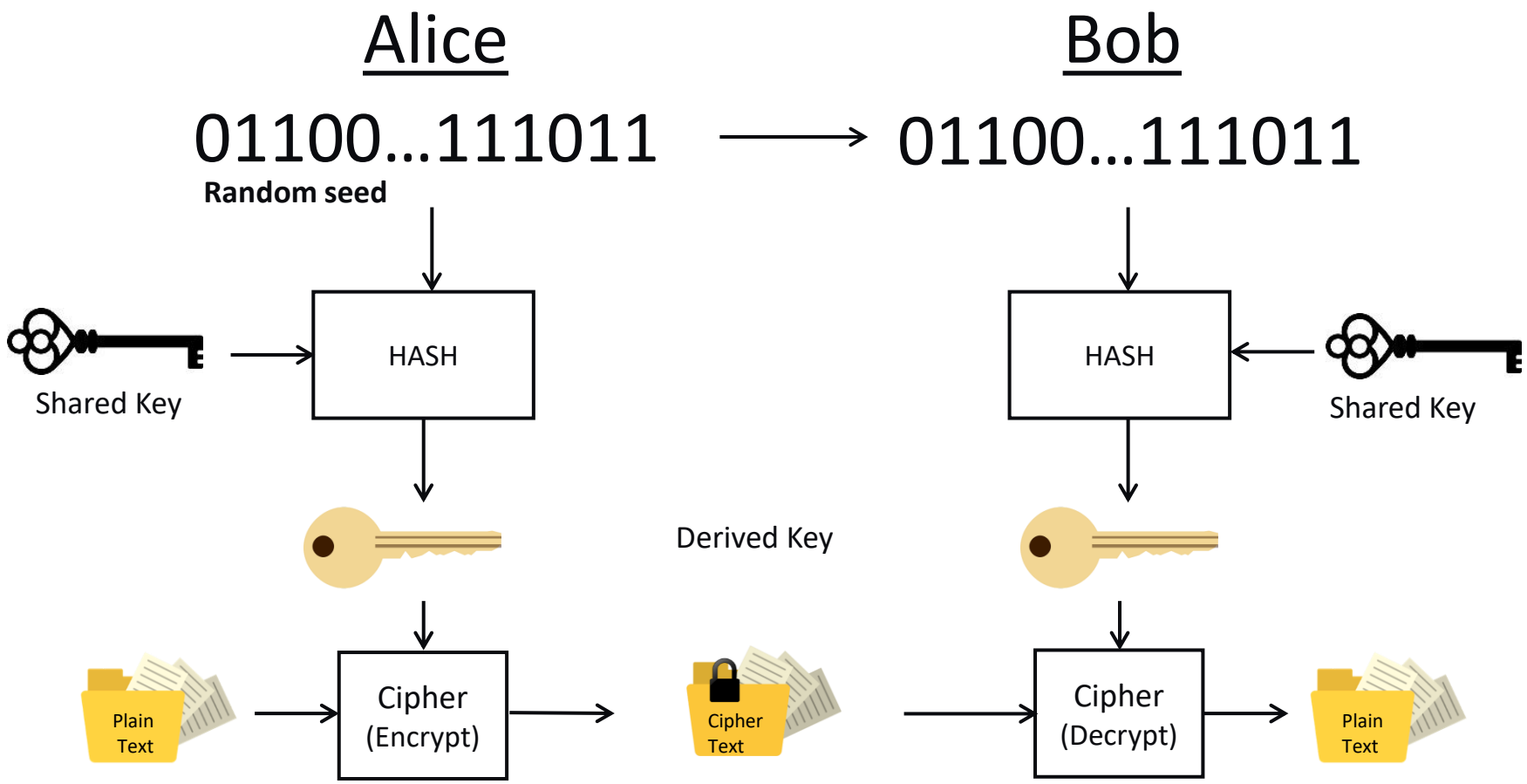
What are Session Keys?

Session keys are used with a cipher to obfuscate messages and/or data

- **To encrypt we use a cipher, which needs a Key(s)**
  - A cipher is a math function which uses a unique key to uniquely obfuscate input (cleartext), turning it into unreadable output (ciphertext)
  - There are many types of ciphers
    - Advanced Encryption Standard (AES), Data Encryption Standard (DES), Triple Data Encryption Standard (3DES), Blowfish, Twofish, International Data Encryption Algorithm (IDEA), ChaCha20, etc.
    - Ciphers also have modes of operation, like AES-CBC (Cipher Blocking Chaining) or AES-GCM (Galois Counter Mode)
- **A critical mass of ciphertext with the same key has vulnerabilities**
  - This is known as “key exhaustion”
  - Temporary keys are used and frequently changed to thwart these vulnerabilities
    - Hence the term “session keys” – a “session” can be any length of time
      - A session could be every message transmission or a full day or a week of transmissions
      - Or a single transmission could consist of multiple sessions
        - Military communications often change keys many times each second during a single message transmission

Symmetric Cryptography for Session Keys

Alice wants to send Bob a secret message
Alice and Bob have previously shared an identical secret key



MICROCHIP

Summary

- What is symmetric cryptography
- The simplest form of key establishment – “key transport”
- What a hash function does
- How identity authentication is accomplished using symmetric cryptography
- How message authentication is accomplished using symmetric cryptography
- What a cipher is and why we shouldn’t always use the same key
- What a session key is and how to spawn one using symmetric cryptography

Thank You