

## Basic Cryptography

Security through obscurity

- *substitution cipher* ~ Cesarean cipher
- *XOR cipher* - XOR with some repeated “combinator”
- *diffusion* - small change in plaintext → large change in ciphertext
- *confusion* - key doesn't relate in simple way to ciphertext
- *non-repudiation* - proves that a user performed an action

Resource vs. Security Constraint

- low-power devices need security
- crypto needs to work for devices with low-latency
- Energy, Latency, Security all fight in a trifecta

thus, there needs to be *high resiliency* in crypto

## Crypto Algorithms

- Stream Cipher - one character and replaces with another
- Block Cipher - entire block at a time
- Sponge Function - expansion of plaintext to larger ciphertext

## Hashing

- Fixed Size
- Unique
- Original
- Secure

Algorithm	Length	Traits
MD5	512b	Collisions, Weak
SHA-2	128, 256, 512	Secure
SHA-3		Latest SHA, Low-Power
RIPEMD	128, 256, 320	Parallel
HMAC		Shared Key

RIPEMD - Race Integrity Primitives Evaluation Message Digest

## Symmetric Key Crypto

Private Key Crypto, Shared Key Crypto

Algorithm	Length	Traits
DES	56b Key	Block Cipher
3DES	Can use 3 keys	3 rounds of DES

Algorithm	Length	Traits
AES	128b plaintext	NIST in 2000, Secure
Rivest		
Blowfish	64b blocks, 32-448 keys	No significant weakness
IDEA	64b blocks, 128b Key	8 Rounds, EU

DES - Data Encryption Standard

AES - Advanced Encryption Standard

IDEA - International Data Encryption Algorithm

## Asymmetric Key Crypto

Public Key Crypto

Algorithm	Traits
RSA	Prime Numbers, 1997 MIT, Most Common
ECC	Elliptic Curve, Less Power, Smaller Keys
DSA	Digital Signatures

## Key Exchange

Diffie-Hellman

- DH Ephemeral
- Elliptic Curve DH

## Attacks

- Knowledge of underlying plaintext language - i.e. English
- Distribution of characters - tons of E, little use of Q
- Null ciphertext - null value padding
- Management Frames - TCP/IP has a structure
- Collision Attack
- Birthday Attack

## File System Encryption

- EFS - Microsoft Windows Encrypting File System - NTFS
- Full Disk Encryption - BitLocker
- Hardware Encryption - trusted platform module, hardware security model
  - password-protected flash drives
  - self-encrypting drives (SED)
  - TPM - true random numbers, built in motherboard
  - HSM - onboard keygen and storage