Basic Cryptography

Security through obscurity is a *fallacy*!

- *substitution cipher* ~ Cesarean cipher
- *XOR cipher* - XOR with some repeated "combinator"
- *diffusion* - small change in plaintext → large change in ciphertext
- *confusion* - key/cleartext doesn't relate in simple way to ciphertext
- *non-repudiation* - proves that a user performed an action
- *plaintext* - data that is to be encrypted
- *cleartext* - data that has not yet been encrypted

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

Four basic protections of crypto:

- Authenticity
- Confidentiality
- Integrity
- Non-Repudiation

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-1	160b	Weak
SHA-2	128 (9 r), 192 (11 r), 256 (13 r)	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 Cypto, Shared Key Crypto

Algorithm	Type	Length	Traits
DES	Block	56b Key	Not Secure
3DES	Block	Can use 3 keys	3 rounds of DES
AES	Block	128b plaintext, 192, 256	NIST in 2000, Secure
RC-4 + BR Rivest	Stream	56b, 128b Key	Voice, Video, Streaming
Blowfish	Block	64b blocks, 32-448 keys	No significant weakness
IDEA	Block	64b blocks, 128b Key	8 Rounds, EU

DES - Data Encryption Standard

AES - Advanced Encryption Standard

IDEA - International Data Encryption Algorithm

Asymmetric Key Cypto

Public Key Crypto

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

- *perfect forward secrecy* - random public keys for each session

Key Exchange

Diffie-Hellman

- DH
  - Uses same keys each time
  - agree on large prime number and related integer
- 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 & other crypto services, built in motherboard / hardware
  - HSM - onboard keygen and storage