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
  - private keys are never seen by others, if so, they're revoked
  - "actions that are signed cannot be repudiated by the holder"; *they* signed it
- *plaintext* - data that is to be encrypted
- *cleartext* - data that has not yet been encrypted
- *ephemeral keys* - keys used only once
- *perfect forward secrecy* - key derived from another isn't compromised, if the parent is
- *differential cryptanalysis* - compares plaintext to ciphertext to determine the key
- *linear cryptanalysis* - uses a simplified cipher to generate new ciphertext from plaintext, and compares to actual ciphertext to better estimate key
- *key stretching* - the act of increasing the keyspace of a cipher, usually through multiple rounds
- *key exchange* - the act of sharing a secret key - implementations can use asymmetric encryption to share, or derive it with DH
- *Rainbow Tables* - lookup table for hashed data - salting renders them ineffective

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	128b, 512b block	Collisions, Weak
SHA-1	160b, 512b block	Weak
SHA-2	224b, 256b, 384b, 512b	Secure
SHA-3	arbitrary	Latest SHA, Low-Power
RIPEMD	128, 160, 256, 320	Parallel
HMAC		Shared Key

RIPEMD - Race Integrity Primitives Evaluation Message Digest

Symmetric Key Crypto

Private Key Cypto, Shared Key Crypto

- comparatively fast
- few computational requirements

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
RC4 + BR	Stream	56b block, 128b Key	Voice, Video, Streaming, weak IV, used in WEP
Blowfish	Block	64b blocks, 32-448 keys	16 rounds, No significant weakness
Twofish	Block	128b blocks, -256b keys	Stronger than Blowfish
IDEA	Block	64b blocks, 128b Key	8 Rounds, EU

DES - Data Encryption Standard

AES - Advanced Encryption Standard

IDEA - International Data Encryption Algorithm

Block	Stream
More Memory	Faster
Stronger	Difficult to make Correct
High diffusion	Low Diffusion
Resistant to insert / modify	Susceptible to insert / modify

Block	Stream
Susceptible to error propagation	Resistant to error propagation
Grants authenticity or integrity	Can't prove authenticity or integrity
3DES, AES	A5, RC4

Modes of Operation

What if two blocks have the same plaintext? You would see the same blocks of ciphertext

- Electronic Code Book (ECB)
  - Simplest, each block is encrypted separately
- Cipher Block Chaining (CBC)
  - XOR with previous block, IV for first cipher
  - Cannot be parallelized
- Cipher Feedback Mode (CFM)
- Output Feedback Mode (OFM)
- Counter Mode (CTR / CTM)
  - generates nonce for each block
  - encrypts nonce, then XOR with plaintext
  - Can be parallelized
- Galois Counter Mode (GCM)
  - CTM with Galois mode of authentication
  - Can be parallelized
  - 802.1ad 802.1AE
  - AES-GCM and GMAC recognized by NIST

Asymmetric Key Cypto

Public Key Crypto

Algorithm	Functions	Traits
RSA	Encryption, Signatures	Prime Numbers, 1997 MIT, Most Common
ECC	Encryption, Signatures	Elliptic Curve, Less Power, Smaller Keys
DSA (ElGamal)	Signatures	Digital Signatures, U.S. Fed Standard
PGP/GPG	Encryption, Signatures	Symantec, uses both Asymmetric and Symmetric
Diffe-Hellman	Key Exchange	Doesn't Encrypt

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

Diffie-Hellman

- DH Groups
  - the keyspace, basically
- DH
  - Uses same keys each time
  - agree on large prime number and related integer
- DH Ephemeral
  - aka Ephemeral Diffe-Hellman (EDH / DHE)
  - key generated used only once (popular for session keys)
  - provides perfect forward secrecy
- Elliptic Curve DH (ECDH)
  - Works with ECC
  - Ephemeral variant ECDHE

Key Stretching

Algorithm	Traits
BCRYPT	Uses Blowfish
PBKDF2	HMAC, thousands of times

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
- Padding Oracle On Downgraded Legacy Encryption (POODLE)
  - CBC attack
  - change in one bit of ciphertext block causes next block to be whacked, with bit inverted, and rest of the blocks good-to-go

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