Cryptography in Practice

- Crypto History
- Crypto Technology
- Living with Crypto

Crypto History

- Government use (diplomatic, military)
- Manual, simple transposition
- Mechanical (WWII)
- Mathematical

Genies and Bottles

- Early Crypto Marketplace
- IBM: Lucipher
- NBS, two rounds
- DES

Who Let the Genie Out?

- 1997, Fall of DES
- FBI, NSA opposition
- Today, S/MIME, PGP, AES. . .

How Cryptography Works

Let's look at a trivial example. . .

$$Key = 2^{16}\left[E_{v_1 \oplus pad}\left(E_{v_1 \oplus pad}\left[\frac{v_2}{2^{16}} \bmod 2^{64}\right]\right)\right]$$
$$\oplus\left[\left(\frac{E_{v_1 \oplus pad}\left[\frac{v_2}{2^{16}} \bmod 2^{64}\right]}{2^{48}}\right) \oplus \left(v_2 \bmod 2^{16}\right)\right]$$

. . . just kidding.

What Crypto Can Do

- Privacy
- Authenticity

Crypto Technology

- Symmetric
  - ⋆ One key for all uses
- Asymmetric
  - ⋆ One key for each use
  - ⋆ One-way functions

Defending With Crypto

- Hiding contents
- Signing contents

Attacking Crypto

- Metadata
- Traffic analysis
- Backup files
- Swap
- Cryptanalysis

An Example

John Adams, of the English Colony of Massachusetts is suspected of HIGH TREASON by agents of His Royal Majesty George III, King of England. If guilty, he shall hang.

Watching John's Online Activity

- King's Men Install Carnivore at John's ISP
- Reading his mail
- If John uses PGP. . .

What We Have

- Who is mailing whom
- How much
- When

More Sophisticated Analysis

- Can attack the system itself
- Weak keys
- Cribs
- Implementation flaws

Grabbing John's Machine

- Now we have access to his PGP keyrings
- Looking for backup files
- Temporary files
- Filenames

Attacking Keyring

- Brute-forcing passphrase
- What the key gets us

Moral of the Story

- No silver bullet
- Crypto necessary for security
  - ⋆ e.g., to protect against terrorists
- Crypto necessarily limits law enforcement
- Welcome to America

Questions?

Matt Curtin
Interhack Corporation
2599 E Main St #512
Columbus OH 43209
cmcurtin@interhack.com
web.interhack.com