Preview

- Cryptography Fundamentals
  - Goals
  - Techniques

Intro to Cryptography

Outline

- Definitions/Terminology
- History
- Paradigms
- The Essence of Ciphers

Reference

- Ciphers by Ritter
  - http://ciphersbyritter.com/
  - Intro to Cryptography
  - Glossary
- Good Stuff

Definitions/Terminology

Cryptography

- Greek for "hidden writing."
- "The art of secret writing"
  - Kaufman, Perlman, Speciner
- "The art and science of keeping messages secure"
  - Bruce Schneier

- The art and science of transforming information into an intermediate form which secures that information while in storage or in transit. As opposed to steganography, which seeks to hide the existence of any message, cryptography seeks to render a message unintelligible even when the message is completely exposed.
  - http://www.io.com/~ritter/GLOSSARY.HTM#Cryptography
- The study of encryption.
  - Yasinsac
Cryptology

The field of study which generally includes:

- steganography
- cryptography
- cryptanalysis

Encryption

- Disguising information so that it is only useful to those intended by the creator.
- Disguising information so that it can only be returned to its original form if you know the "back door".
- Use of mathematics to scramble data so that it is very difficult for anyone other than intended recipients to recover the original plaintext.

Very difficult

- Mathematically complex
- NP Complete/Hard
- Beyond computational capabilities
- Fundamental tenant of Cryptography
- Even perfect encryption only provides temporary protection

Decryption

- Deriving the intended message or other useful information from the cipher text
- Reversing encryption
- Producing the original plaintext from cipher text

Back door / trap door

- A cipher design fault, planned or accidental, which allows the apparent strength of the design to be easily avoided by those who know the trick.
- When the design background of a cipher is kept secret, a back door is often suspected.
- Backdoor: Similar to trap door.
- More generally, a trick that allows one to do something easily that was supposed to be hard to do.

More Definitions

- Cipher: An encryption algorithm
- Encipher: Encrypt
- Decipher: Decrypt
- Cipher (according to Ritter)
  - In general, a key-selected secret transformation between plaintext and ciphertext.
  - Specifically, a secrecy mechanism or process which operates on individual characters or bits independent of semantic content.
More Crypto-Related Definitions

- Plaintext: The unencrypted version of data that has been encrypted.
- Cipher text: The encrypted version of data.

One plaintext may have many cipher texts*
A cipher text has exactly one plaintext

Encryption Processes

Plaintext

Encryption←Key→Ciphertext

Decryption

Plaintext

The Goal of an Encryption Algorithm

- Make cipher text look like random bits, giving no hint of the plaintext
- Perfect encryption
- Example: One time pad

One Time Pad

- Plaintext is xor'ed with a string of random bits
- The result is a random bit string
- Problems
  - Key must be same size as plaintext
  - Generating random bits

Example of a One-Time Key

- Plaintext: T E D
- ASCII of plaintext: 0101 0100 0100 0101 0100 0100
- Key (random): 0111 1011 0110 1001 0000 0000
- Ciphertext: 0010 1111 0010 1100 0100 0100
- ASCII of Cipher text: O L D

Actual Example of a One-Time Key

- Plaintext: T E D
- ASCII of plaintext: 0101 0100 0100 0101 0100 0100
- Key (random): 0110 0110 0111 0011 0001 0010
- Ciphertext: 0011 0010 0011 0110 0101 0110
- ASCII of Ciphertext: 2 6 V
Other Encryption Issues?
- Cryptography paradigm
- Algorithm selection
- Protocol selection
- Key management

Keys Uses
- Authentication
- Session key
- Key distribution key
- Non-repudiation key
- Etc.

Key Lifetime
- Keys degrade over:
  - Time
  - Volume of ciphertext generated
- Keys must be changed

Key Management
- Generation
- Distribution
- Replacement/change

What I've Learned
1. I've learned that regardless of how hot and steamy a relationship is at first, the passion fades, and there had better be a lot of money to take its place.
2. I've learned that we are responsible for what we do, unless we are celebrities (or presidents).
3. I've learned that the people you care most about in life are taken from you too soon and all the less important ones just never go away.
4. I've learned that you can keep vomiting long after you think you're finished.

Simple Encryption
Scramble the plaintext so that the ciphertext is only useable to someone with the appropriate key.
Which layer to encrypt?

- Device-to-device
- Network-to-network
- End[user]-to-End[user]

VPN: Network Encryption

Application Encryption

OSI Model

Which layer to encrypt?

- Link
  - Tactical networks
- Network
  - VPN
- Transport
  - SSL, TLS
- Application
  - PGP, PEM, Clipper, etc.
Encryption at the _______ layer:

- **Application**
  - All headers are in the clear
  - Only the message body is encrypted
- **Network**
  - Layer two and three headers are in the clear
  - Layer 4, 7 headers and the message body is encrypted
- **Link**
  - Layer two headers are in the clear
  - Layer 3, 4, 7 headers and the message body are encrypted
- **Physical:** Every bit on the path is encrypted

Choice of Layers

- Higher layers are more application dependent, but more technology independent
- End-to-end security is provided easier at higher layers; link (point to point) at lower layers
- Higher layers are more likely implemented in software, lower layers in hardware
- Higher layer encryption cannot protect lower layer headers; lower layer encryption may have to trust intermediate nodes
- Middle layer implementations are lagging

Review

- **Security Models**
  - Orange book
- **Cryptography Fundamentals**
  - Goals
  - Techniques
Preview

- Cryptanalysis
- Cipher strength
- Attacks
- Language Redundancy