Crypto I: Symmetric-Key Cryptography

Chengyu Song

Slides modified from Dawn Song, Dan Boneh, David Wagner, Doug Tygar
Administrivia

- Midterm
- Lab2
Overview

• Cryptography: **secure communication over insecure communication channels**

• Three goals
  • Confidentiality
  • Integrity
  • Authenticity
Brief history

- 2,000 years ago
  - Caesar Cypher: shift each letter forward by a fixed amount
  - Encode and decode by hand
- During World War I/II
  - Mechanical era: a mechanical device for encrypting messages (Enigma)
- After World War II
  - Modern cryptography: rely on mathematics and electronic computers
Modern cryptography

- Symmetric-key cryptography
  - The same secret key is used by both endpoints of a communication
- Public-key cryptography – Two endpoints use different keys
Perfect secrecy

• Claude Shannon: the father of information theory

• Basic idea: ciphertext C should provide no "information" about plaintext M

• Have several equivalent formulations:
  • The two random variables M and C are independent
  • Knowing what values C/M takes does not change what one believes the distribution M/C is
  • Encrypting two different messages m_0 and m_1 results in exactly the same distribution
One-time pad

- **K**: random n-bit key
- **M**: n-bit message (plaintext)
- **C**: n-bit ciphertext
- Encryption: $C = M \text{ xor } K$
- Decryption: $M = C \text{ xor } K$
- To satisfy perfect secrecy, **a key can only be used once** -> Impractical!
Block cipher

- Encrypt/Decrypt messages in fixed size blocks using the same secret key
  - k-bit secret key
  - n-bit plaintext/ciphertext
Feistel cipher

**Encryption**
Start with \((L_0, R_0)\)

\[ L_{i+1} = R_i \]

\[ R_{i+1} = L_i \oplus F(R_i, K_i) \]

**Decryption**
Start with \((R_{n+1}, L_{n+1})\)

\[ R_i = L_{i+1} \]

\[ L_i = R_{i+1} \oplus F(L_{i+1}, K_i) \]
DES - Data Encryption Standard (1977)

- Feistel cipher
- Works on 64 bit block with 56 bit keys
- Developed by IBM (Lucifer) improved by NSA
- Brute force attack feasible in 1997

- Rijndael cipher
  - Joan Daemen & Vincent Rijmen
- Block size 128 bits
- Key can be 128, 192, or 256 bits
Abstract block ciphers: PRPs and PRFs

• Pseudo Random Function (PRF): $F: K \times X \rightarrow Y$ such that:
  • Exists "efficient" algorithm to evaluate $F(k,x)$
• Pseudo Random Permutation (PRP): $E: K \times X \rightarrow X$ such that:
  1. Exists "efficient" algorithm to evaluate $E(k,x)$
  2. The func $E(k, \cdot)$ is one-to-one
  3. Exists "efficient" algorithm for inverse $D(k,x)$
• A block cipher is a PRP
Secure PRF and secure PRP

- A **PRF** $F: K \times X \to Y$ is secure if
  - $F(k, \cdot)$ is indistinguishable from a random function $f: X \to Y$
- A **PRP** $E: K \times X \to X$ is secure if
  - $E(k, \cdot)$ is indistinguishable from a random permutation $\pi: X \to X$
Take-away

- Block cipher approximates one-time pad by using a short key
  - Short secret -> long randomness
- Designing secure block cipher is not easy so
  - **DO NOT EVER TRY TO DESIGN YOUR OWN BLOCK CIPHER**
  - Just use AES, it's secure and fast, even has hardware support
Modes of Operation

- Block ciphers encrypt fixed size blocks
- How to en/decrypt arbitrary amounts of data?
- NIST SP 800-38A defines 5 modes
  - Block and stream modes
  - Cover a wide variety of applications
  - Can be used with any block cipher
Electronic Code Book (ECB)

- Message is broken into independent blocks which are encrypted
- Each block is a value which is substituted, like a codebook
- Each block is encoded independently of the other blocks
ECB

- Encryption

Electronic Codebook (ECB) mode encryption
ECB

• Decryption

Electronic Codebook (ECB) mode decryption
Problems of ECB

- Message repetitions may show in ciphertext
  - If aligned with message block
  - Particularly with data such graphics
  - Or with messages that change very little
- Breaks the requirement of one-time
- Not recommended
Example of ECB failure
Example of ECB failure

Encrypted with ECB
Cipher Block Chaining (CBC)

- Encryption

Cipher Block Chaining (CBC) mode encryption
ECB

• Decryption
Advantages and Limitations of CBC

- Ciphertext block depends on all blocks before it
- Change to a block affects all following blocks
- Need Initialization Vector (IV)
  - Random numbers
  - Must be known to sender & receiver
Example of CBC
Example of CBC

Encrypted with CBC
Stream modes

- Block modes encrypt entire block
- May need to operate on smaller units
  - Real time data
- Convert block cipher into stream cipher
  - **Counter (CTR) mode**
- Use block cipher as PRNG (Pseudo Random Number Generator)
Counter (CTR)

- Encrypts counter value
- Need a different key & counter value for every plaintext block
  - $O_i = EK(IV+i)$
  - $C_i = P_i \text{ xor } O_i$
- Uses: high-speed network encryption
Advantages and Limitations of CTR

- Efficiency
  - Can do parallel encryptions in h/w or s/w
  - Can preprocess in advance of need
  - Good for bursty high speed links
- Random access to encrypted data blocks
- Must ensure never reuse key/counter values, otherwise could break
For next class ...

• Crypto II: Asymmetric Key Cryptography