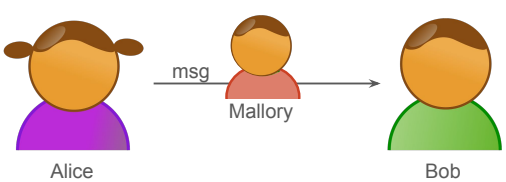
Symmetric Encryption

COMP 435
Fall 2017
Prof. Cynthia Sturton

Cryptosystems

Threat Model



Dolev-Yao Threat Model

The attacker carries the message

Kerckhoffs' Principle

The security of a cryptosystem should depend only on the secrecy of its keys

Symmetric Encryption

Alice

Bob

$C = \mathrm{Enc}_k(msg)$

C

$msg = \mathrm{Dec}_k(C)$

Symmetric Encryption

- $msg = \mathrm{Dec}_k(\mathrm{Enc}_k(msg))$
- Strong confidentiality
- Secure key distribution

Breaking the Encryption Algorithm

- Cryptanalysis
- Brute Force

Threat Models

- Ciphertext attack
- Known plaintext attack
- Chosen plaintext attack
- Chosen ciphertext attack
- Chosen text attack

Computationally Secure

- Cost to break encryption >> value of asset
- Time to break encryption >> lifetime of asset

Theoretically Secure

Attacker can not recover information about the original message without knowing the secret key

Quick Review
(Think, Pair, Share)

Security Principles

- Economy of mechanism
- Fail-safe defaults
- Complete mediation
- Open design
- Separation of privilege

Security Principles

- Least privilege
- Least common mechanism
- Psychological acceptability
- Defense in depth

Back to Symmetric Encryption

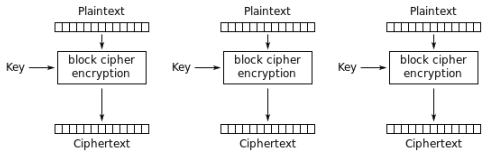
Symmetric Encryption

- Block ciphers
  - DES, 3DES, AES
- Stream ciphers
  - RC4

Block Ciphers: Mode of Operation

- Electronic code book
- Cipher block chaining
- Cipher feedback
- Output feedback
- Counter

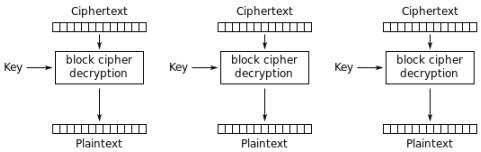
Electronic Code Book (ECB)



Electronic Codebook (ECB) mode encryption

https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

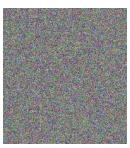
Electronic Code Book (ECB)



Electronic Codebook (ECB) mode decryption

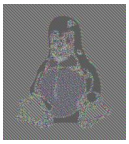
https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Encryption



https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

Encryption Using Electronic Code Book



https://en.wikipedia.org/wiki/Block_cipher_mode_of_operation

One Time Pad

Key material is combined with message by modular arithmetic

One Time Pad

Example:

Msg: “secret”

Key: hektis

Cipher text:

One Time Pad

Immune to brute force attack

One Time Pad

- Key material is as long as message
- Key material is never reused
- Key material is kept secret
- Key material is truly random

Attack Trees
(Think, Pair, Share)

Attacker's Goal

Get officially enrolled in the class