

# File Encryption

Kati Reiland

Information Security Group

November 1<sup>st</sup>, 2005



# Why Encrypt?

---

## ⌘ Personal Computer

- Phone number
- Home & Work Addresses
- Social Security Numbers
- Tax & Financial Info
- Personal Photos
- Birth Dates
- Calendar / Schedule
- Love Letters
- Personal Email
- Address Books
- Personal Medical Info

## ⌘ Company Computers

- Financial Data
  - Customer Data
  - Employee Data
  - Confidential Work / Projects / Trade Secrets
  - Email Communications
  - Tax Info
  - Calendars / Schedules
  - In-house Policies
  - Legal Info
-

# Does anyone really want any of that information?

---

- # In the US between July 2002 and July 2003, ~ 7 million people became victims of identity theft
    - That is 19,178 per day, 799 per hour, 13.3 per minute.
    - 80% increase from previous year
    - Will continue to rise
  - # Avg amt of time spent to completely recover from identity theft (per individual) = 600 hours
  - # Avg arrest rate of identity theft criminals = <5%
-

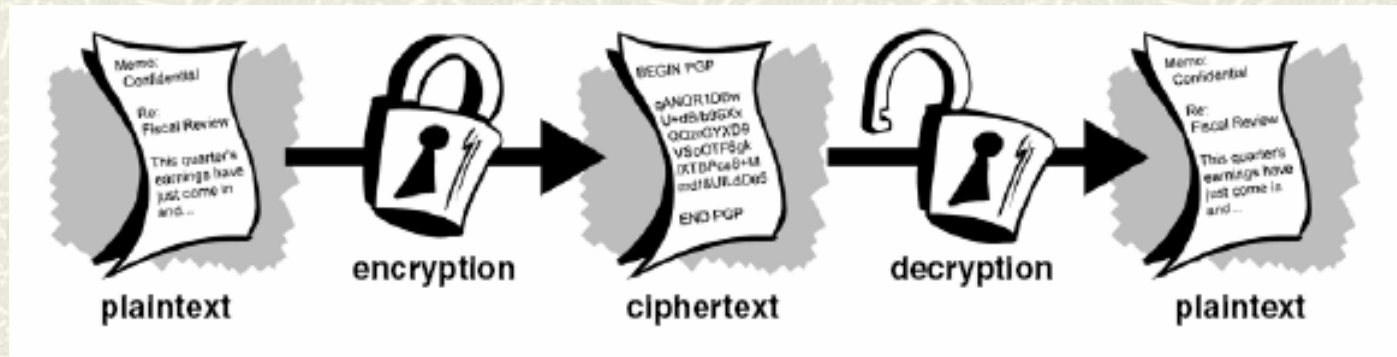
# Another Reason to Encrypt

---

***USA PATRIOT Act***

---

# How it Works



*“There are two kinds of cryptography in this world: cryptography that will stop your kid sister from reading your files, and cryptography that will stop major governments from reading your files.”*

*~ Bruce Schneier, Applied Cryptography*

# Weak Encryption

---

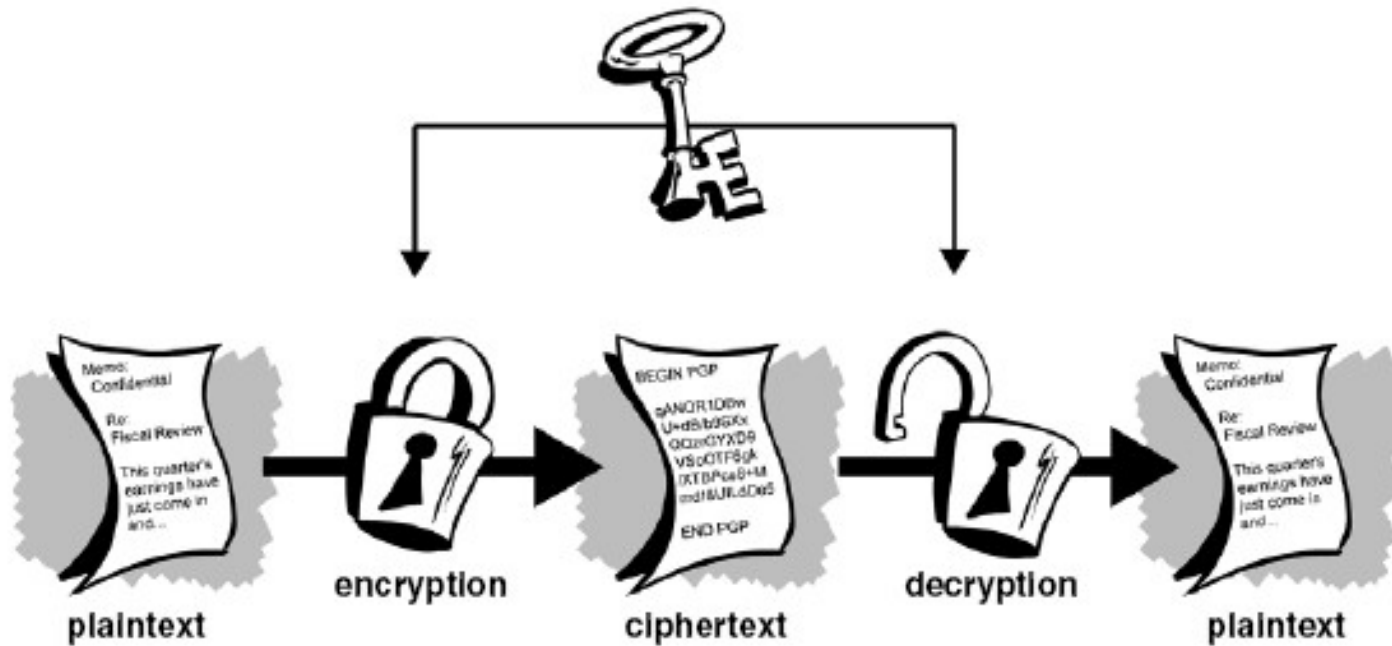
- # Keeps out the kid sister, not the government
- # Any encryption algorithm that contains a detectable pattern in the cipher text
  - Detectable pattern = easily broken
- # Example = Ceasar's Cipher

# Strong Encryption

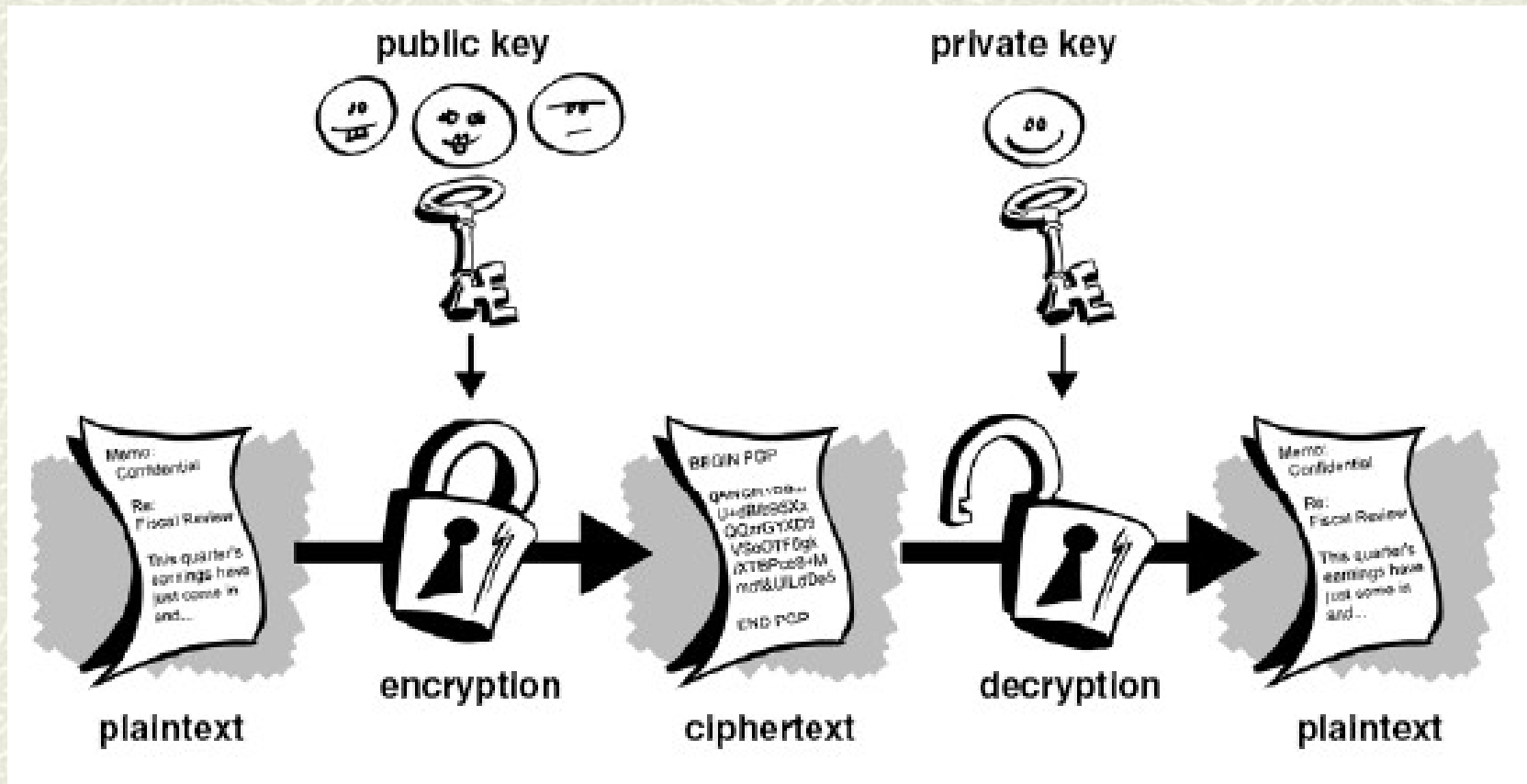
---

- # Keeps the government out (hopefully)
  - # Most commonly used algorithms today use this
    - e.g. RSA, PGP, GPG, Diffie-Hellman, DSA, hashes, etc
-

# Private Key (Symmetric)



# Public Key (Asymmetric)



# File Encryption Tools

---

## # PGP (Pretty Good Privacy)

- Costs money
- Available for Windows or Mac
- Supports most email and IM applications
- Desktop Home version (\$99)
  - File encryption
  - Whole disk encryption
  - IM encryption
  - Email encryption
  - Virtual disk encryption (USB drives, CDs, Zip drives, etc)
  - File Shredder

## # GPG (Gnu Privacy Guard)

- Free
  - Available for Windows, Mac, or Linux
  - Mostly for file encryption
-

# For More Information

---

- # **The Code Book** by Simon Singh
  - # **The Codebreakers** by David Kahn
  - # **Applied Cryptography** by Bruce Schneier
  - # **Crypto: How the Code Rebels Beat the Government – Saving Privacy in the Digital Age** by Steven Levy
  - # **Privacy on the Line: The Politics of Wiretapping and Encryption** by Whitfield Diffie and Susan Landau
  - # [www.pgp.com](http://www.pgp.com)
  - # [www.gnupg.org](http://www.gnupg.org)
  - # [www.privacy.org](http://www.privacy.org)
-

# Lab Exercise - GPG

---

- # Log into Linux machines and follow the handout steps.