Computer Science 1000: Part #9

Computer Security

- Authorization and Authentication
- Network-based System Attacks
- The Hacker Mystique
- Cryptography: A Privacy Survival Tool

Computer Security: An Overview

- Three basic tasks of computer security:
  1. Ensuring you are who you say you are (**Authentication**)
  2. Ensuring you can only access and do what you are allowed to access and do (**Authorization**)
  3. If (1) or (2) fails, ensuring that accessed material cannot be misused (**Encryption**)
- All of this is complicated enough when dealing with the multiple users of a single computer system; becomes much more difficult when dealing with networks of computers and sophisticated applications operating on such networks, e.g., E-commerce.

Authentication

Implement authentication by issuing each valid user a unique username-password pair, e.g., `ToddW / Daa45&K4%`. All such pairs are stored in a password file, e.g.,

ToddW	Daa45&4%
Tijara	Popsicle
Murphy	badboy2
Jaylynn	mom
Edward	123456
BillyBob	MyPassword
...	

and checked when system access is attempted.

Authentication (Cont'd)

To prevent misuse of stolen password files, stored passwords are typically transformed using some method M such as a hashing function, e.g.,

ToddW	M(Daa45&4%) $\Rightarrow$ aAV3JHS
Tijara	M(Popsicle) $\Rightarrow$ ok2llhyd
Murphy	M(badboy2) $\Rightarrow$ ebdsjgh
Jaylynn	M(mom) $\Rightarrow$ ddd2d0bZvn
Edward	M(123456) $\Rightarrow$ Invfryup
BillyBob	M(MyPassword) $\Rightarrow$ bkjk56ss
...	

which is also applied to any password entered in a system access attempt.

Authentication (Cont'd)

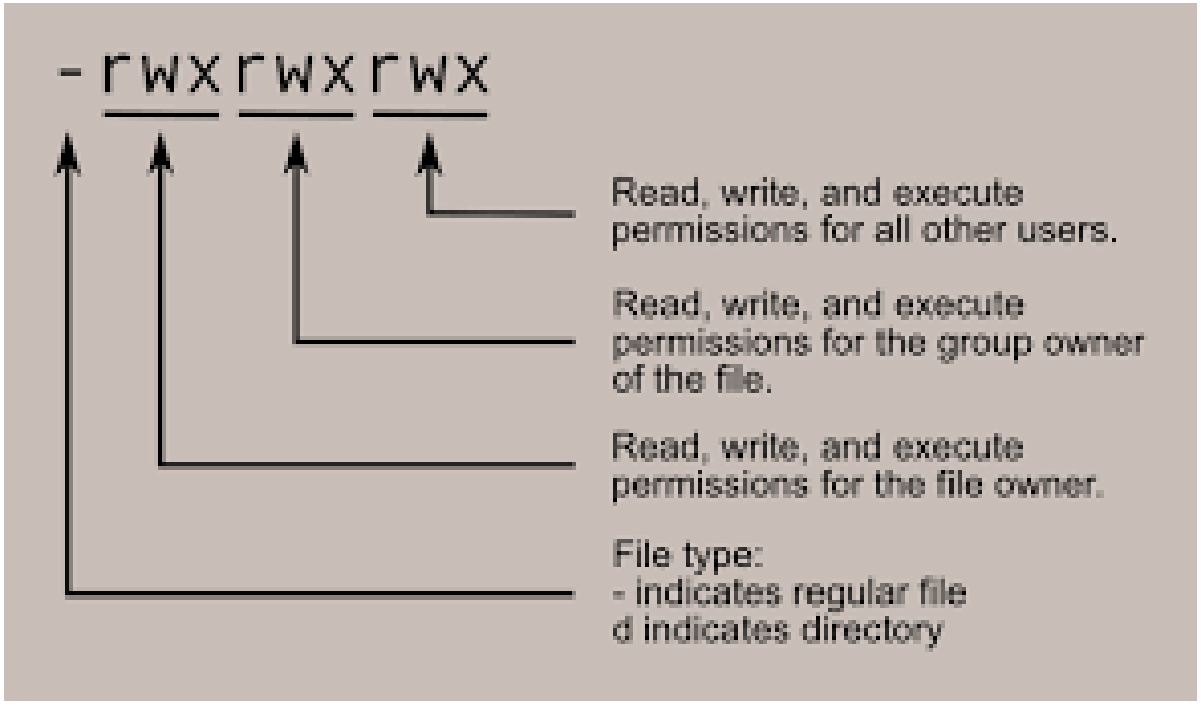
- If M is known, authentication can be compromised by password-cracking software,
- Given a valid username, such software generates possible passwords by various techniques, e.g.,

  1. Apply M to common-word dictionary, e.g., `123456`.
  2. Apply M to common-phrase dictionary, e.g., `MyPassword`.
  3. Apply M to all possible password-strings.

  Each generated password is then transformed by M and tried with the username until the system is accessed.
- Social engineering is actually the easiest (and most disconcertingly effective) way to obtain passwords, e.g., postit snooping, shoulder surfing, imposter pleading.

Authorization

Implement authorization by splitting system users into groups and associating **access bits** with each resource to specify which groups can use that resource, e.g., UNIX access bits:



Access bit rules (hopefully) enforced by operating system

Network-based System Attacks

- There are a variety of types of malware, e.g., popups, keystroke loggers, ransomware.
- There are a variety of network-based ways to infect a system with malware, e.g.,
  - **Virus**: Spread by infected file that embeds malware in another program; activated by running that program.
  - **Worm**: Spread by self-replicating program that automatically infects other machines.
  - **Trojan Horse**: Spread by downloading an infected program or website.
- Regular network communications can also be subverted to overload targeted systems (**Denial of Service**).
- Malware and attack methods developed by hackers.

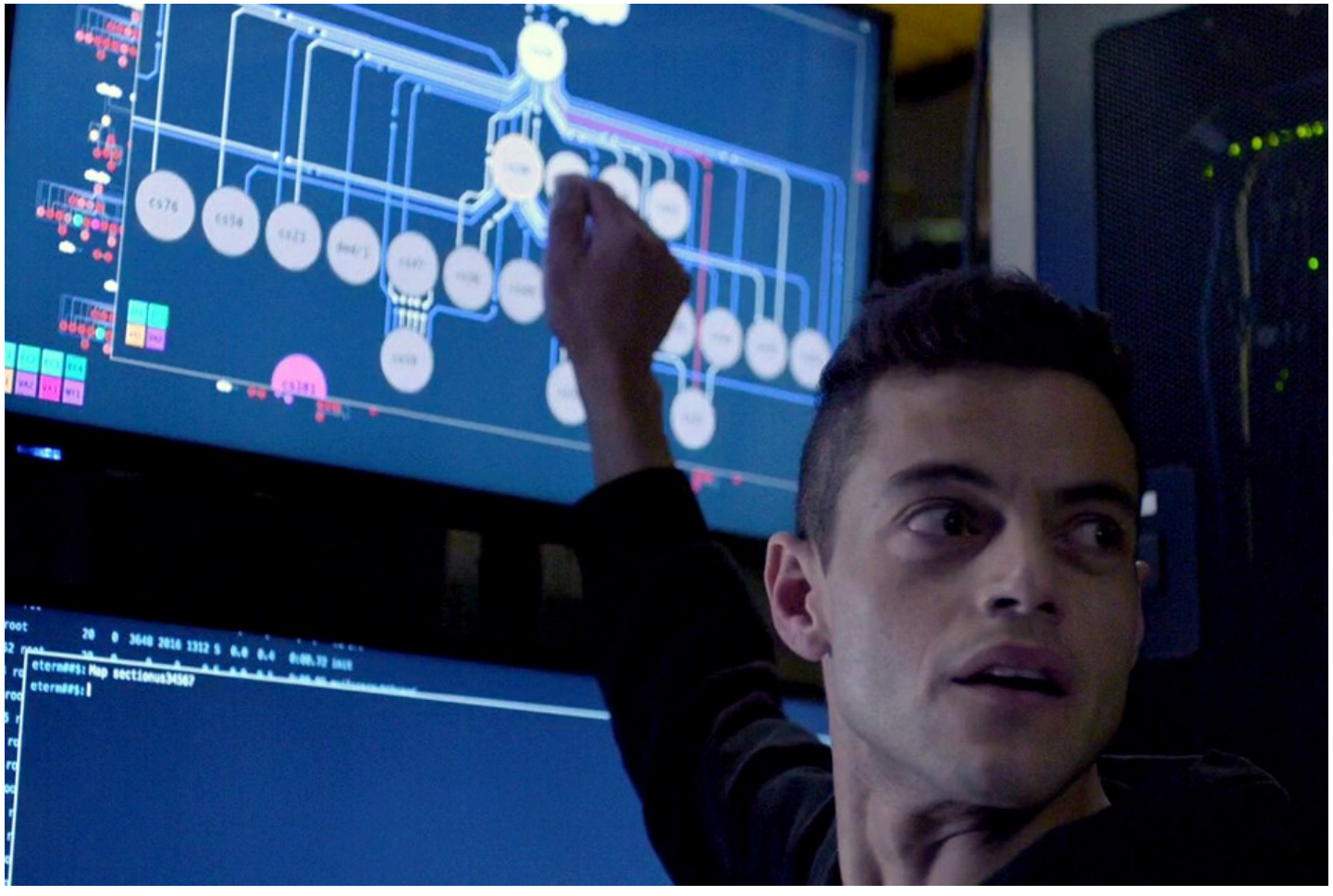
The Hacker Mystique: The Image

WarGames (1983)

The Hacker Mystique: The Image (Cont'd)

Sneakers (1992)

The Hacker Mystique: The Image (Cont'd)



Mr. Robot (TV) (2015–2019)

The Hacker Mystique: The Reality

MIT Tech Model Railroad Club (TMRC) (mid-1950s)

The Hacker Mystique: The Reality (Cont'd)

PDP-1 with Teletype

MIT AI Laboratory (early 1960s)

The Hacker Mystique: The Reality (Cont'd)

- With arrival of TX-0 and PDP-1 computers at the MIT AI lab in 1959 and 1960 as well as first undergraduate courses in computer programming, first hackers emerge from TMRC Signals & Power Subcommittee.
- Early hackers share austere set of core values, i.e.,
  - Dedication to solving problems ("Code 'till you drop");
  - Intensity and focus while solving problems;
  - Curiosity about technical system details;
  - Beauty (Commitment to technical complexity and elegance of solutions); and
  - Purity (All solutions available to anyone for free).
- Rigors of hacker ethic resemble those of religious orders; also induce side effects in some hackers, e.g., lack of sleep, bad diet, poor personal hygiene, arrogance.

The Hacker Mystique: The Reality (Cont'd)

- With increasing availability of minicomputers in academia in mid to late 1960s, hacker cultures emerge outside MIT, e.g., Stanford AI Laboratory (SAIL).
- Core aspects of hacker ethic are retained but often moderated, e.g., SAIL focus on gentle fantasy rather than rough adversarial gaming (Adventure vs. SpaceWar).
- As hackers leave academia, hacker ethic percolates into citizen projects, e.g., Community Memory, and industry, e.g., late 1970s West Coast computer games companies.
- Hackers emerge in general population courtesy of PC and Internet use explosion starting in the early 1980s.

The Hacker Mystique: The Reality (Cont'd)

Community Memory Public Terminal
(San Francisco, 1973–1975)
[FINDing: free / ADDing: 25 cents]

CM Terminal
(CRT version)

The Hacker Mystique: The Reality (Cont'd)

Robert Morris (1965–)

Kevin Mitnick (1963–)

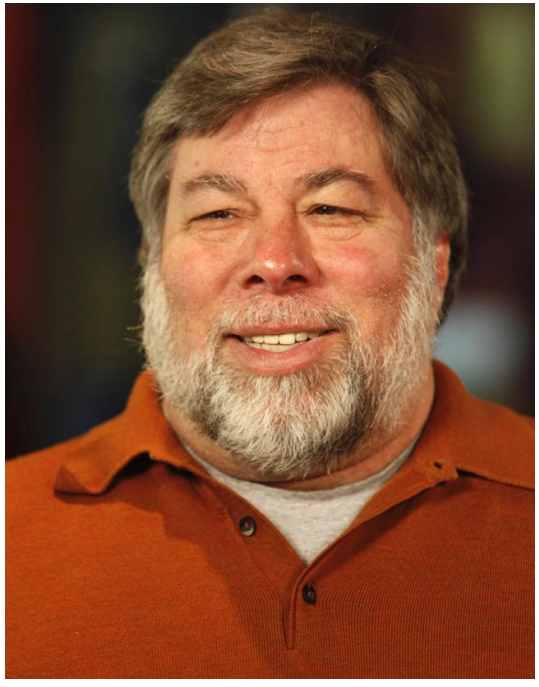
- Hacking goes public starting in late 1980s with high-profile prosecutions for accidental (Morris Worm (1990)) and planned (Mitnick (1988, 1995)) computer disruptions.

The Hacker Mystique: The Reality (Cont'd)

- With ever-increasing computer and network usage, criminal and government hacker subcultures have emerged; are now unfortunately focus of hacker coverage in media.
- Terms for different types of hackers have emerged based on primary activity (**cracker**) and technical maturity (**script kiddie, guru**).
- Arguably most important distinction is guiding purpose:
  - **Black Hats**: Work for criminal or malicious purposes.
  - **Gray Hats**: Perform illegal acts to impress friends and/or gain technical knowledge.
  - **White Hats**: Work to create beneficial systems and/or expose flaws in existing systems so they can be fixed.

The Hacker Mystique: The Reality (Cont'd)

Notable White Hats:



Steve Wozniak (1950–)
Co-founder of Apple

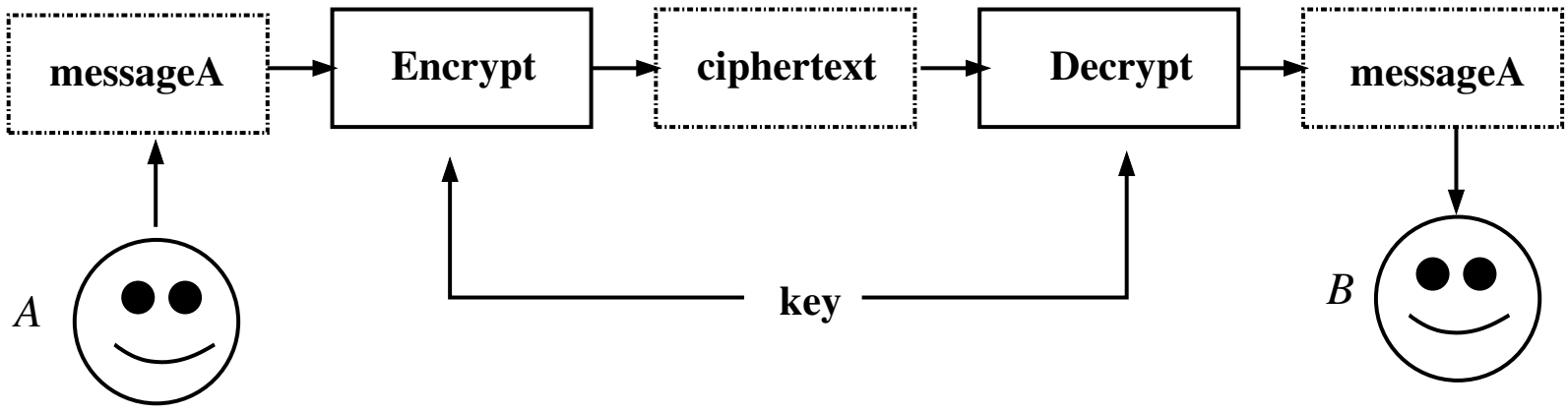
Linus Torvalds (1969–)
Creator of Linux

Cryptography: A Privacy Survival Tool

- Protect personal data and identity using cryptography.
- A cryptographic system allows you to **encrypt** a message to someone else (creating a **ciphertext**) such that the person for whom this message is intended can **decrypt** the ciphertext to obtain the original message.
- If it is either impossible or very difficult for anyone but the intended recipients to successfully decrypt ciphertexts, the cryptosystem is **secure**.
- Two types of cryptosystems: **symmetric (one key)** and **asymmetric (two key)**.

Cryptography: A Privacy Survival Tool (Cont'd)

- Symmetric (one key) cryptography:

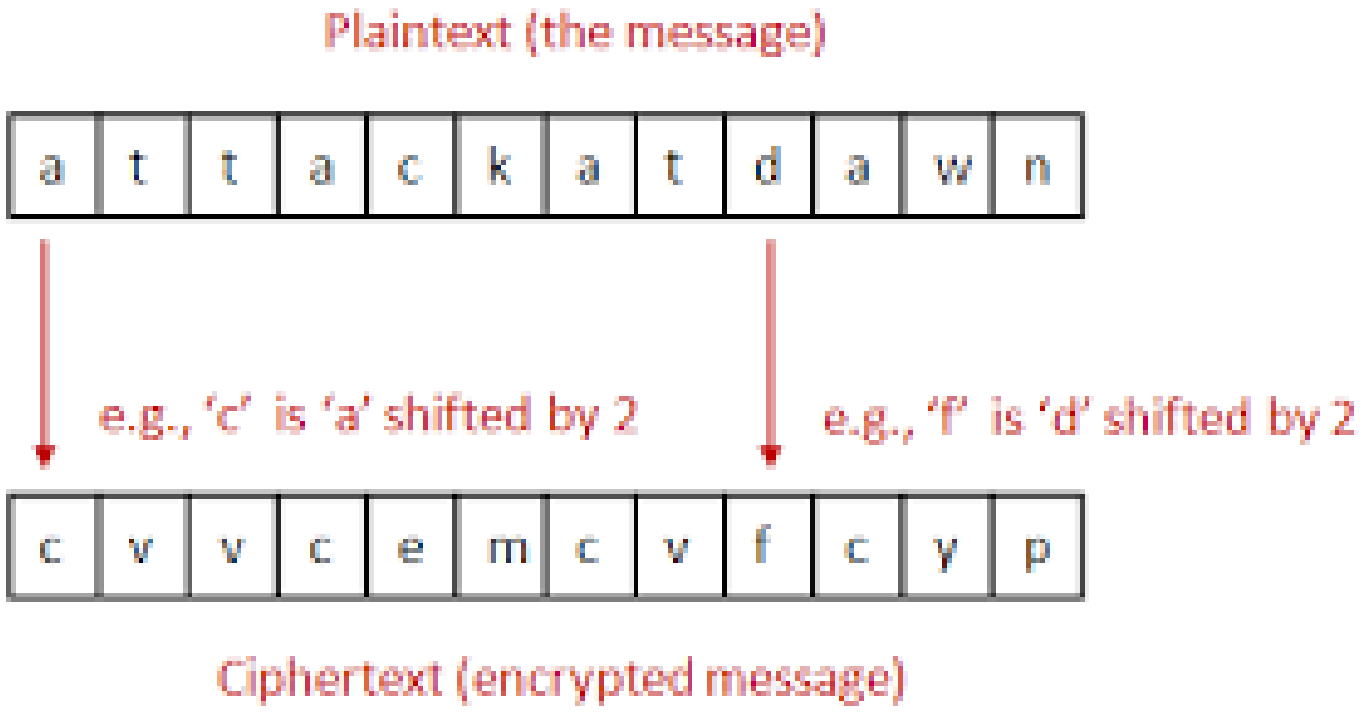


Pros:
- Computationally quick
- Provably uncrackable in certain situations

Cons:
- Key can be stolen / deduced
- Available software may be compromised by national security agencies

Cryptography: A Privacy Survival Tool (Cont'd)

A classic symmetric cryptosystem is the **Caesar (shift) cipher**, in which the key is the number of letters in the alphabet a letter in the message is shifted to create the ciphertext equivalent



Cryptography: A Privacy Survival Tool (Cont'd)

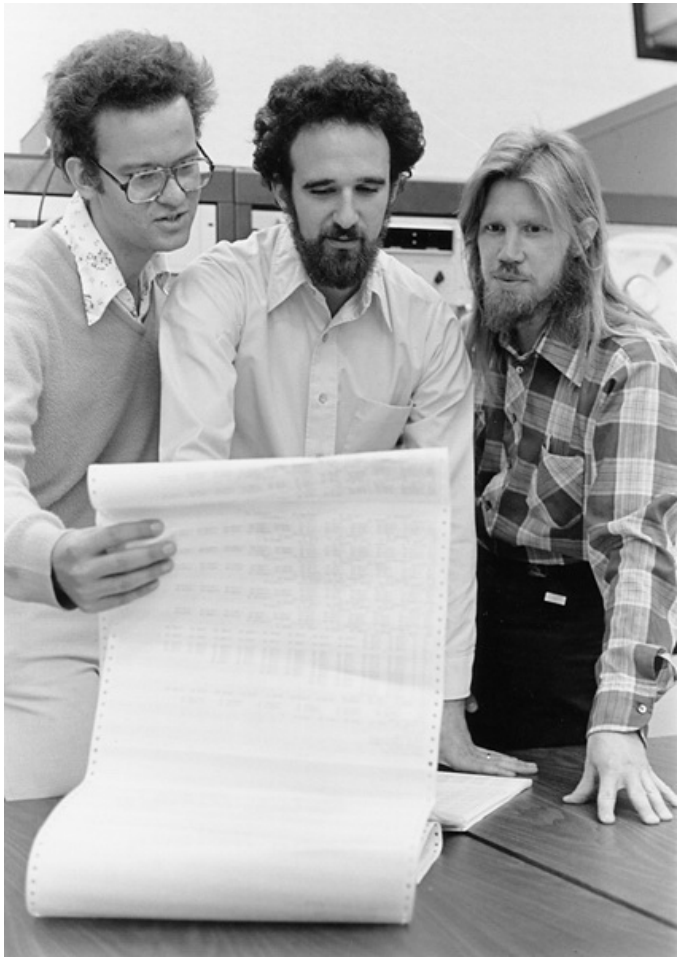
- Cryptosystem research controlled by national agencies.
- Research classified and system export prohibited, *e.g.*, International Traffic in Arms Regulation (ITAR: USA).

National Security Agency
(NSA; est. 1952 (USA))
["No Such Agency"]

Gov. Communications HQ
(GCHQ; est. 1919 (UK))

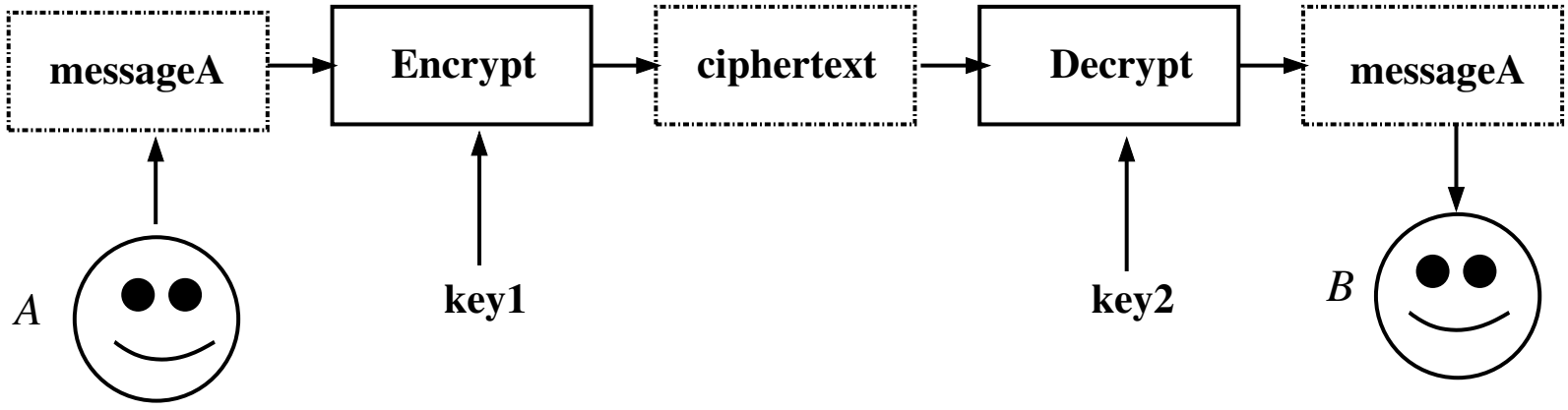
Cryptography: A Privacy Survival Tool (Cont'd)

- Asymmetric cryptography created by Whitfield Diffie (1944–) [R] and Martin Hellman (1945–) [C] in 1975; first implementation made in collaboration with Ralph Merkle (1952–) [L] in 1976.
- Research published in open scientific literature.
- First developed in 1969 by James Ellis (1924–1997) at GCHQ but was classified.



Cryptography: A Privacy Survival Tool (Cont'd)

- Asymmetric (two key) cryptography:

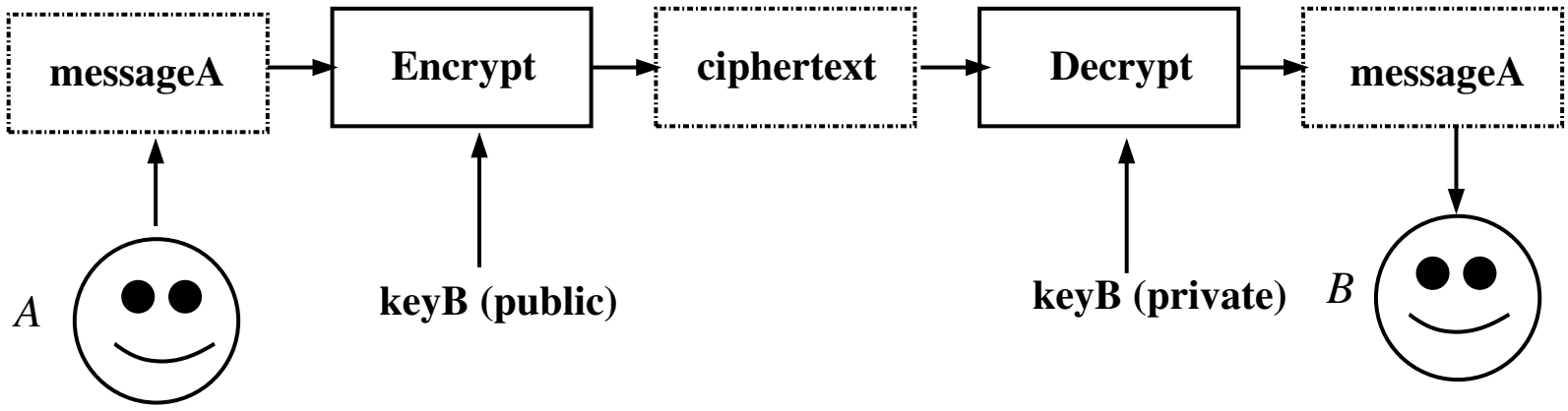


Pros:
- Provides secure messages and signatures
- Not impossible but very hard to crack
- Much software available

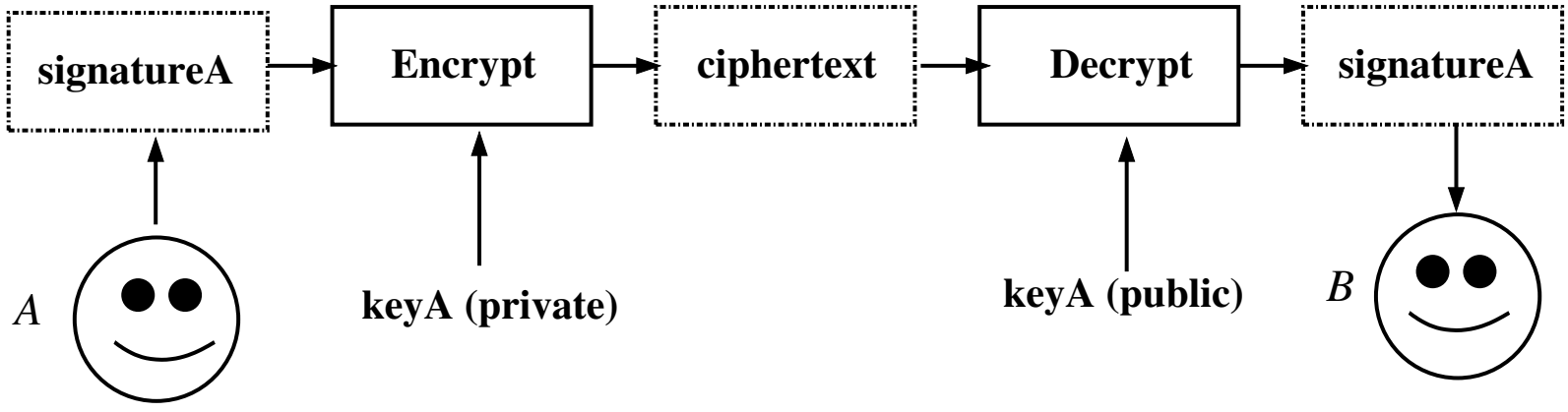
Cons:
- Computationally more expensive
- Keys can be stolen / deduced
- Available software may be illegal or compromised

Cryptography: A Privacy Survival Tool (Cont'd)

- Secure messages (encrypt message with B's public key):

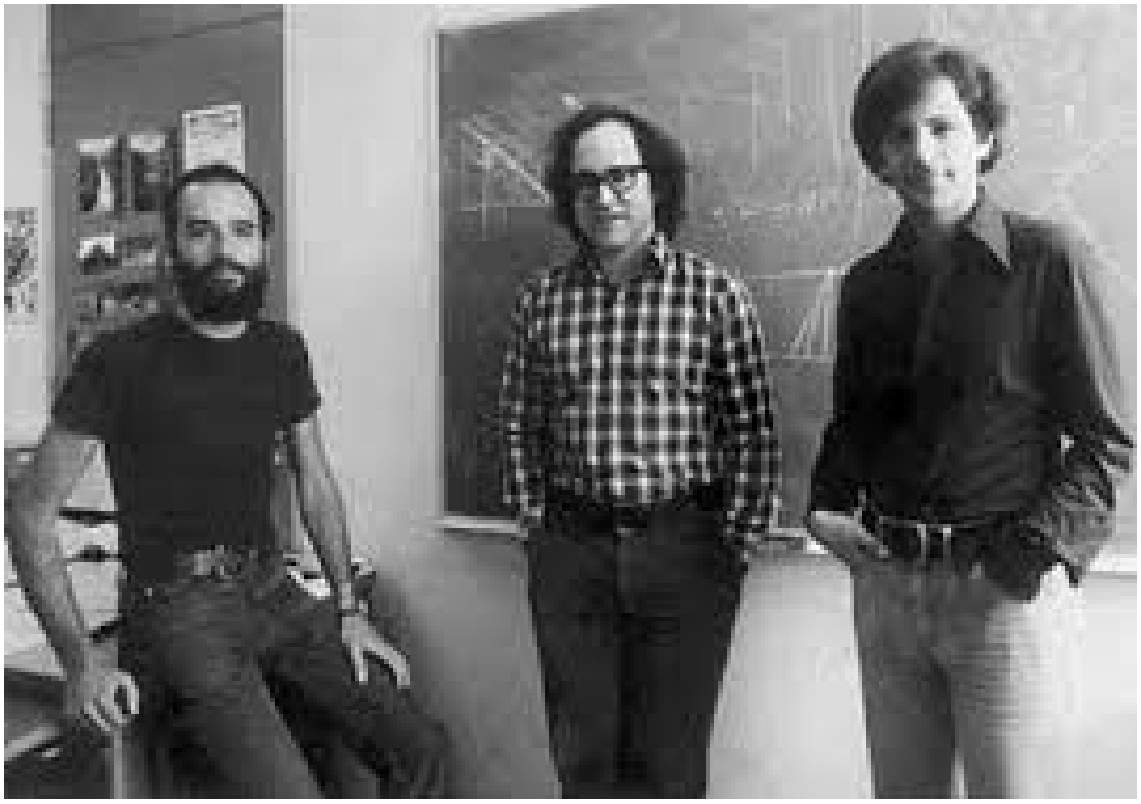


- Secure signature (encrypt signature with A's private key):



Cryptography: A Privacy Survival Tool (Cont'd)

First practical implementation of asymmetric cryptography created by Ron Rivest (1947–) [C], Adi Shamir (1952–) [L], and Len Adelman (1945–) [R] in 1977 (RSA Algorithm); based on integer factorization.



Cryptography: A Privacy Survival Tool (Cont'd)

Asymmetric cryptography propagates (illegally) worldwide via Pretty Good Privacy (PGP) in 1991.

Phil Zimmerman (1954–)

Cryptography: A Privacy Survival Tool (Cont'd)

- NSA attempted to prevent spread of asymmetric cryptography by invoking export regulations and proposing its own (NSA-crackable) cryptographic mechanisms, *e.g.*, Digital Encryption Standard (DES), Clipper Chip. Under industry pressure, such legal and technical challenges ended in December 1999.
- Following the 9/11 attacks, the threat of terrorism has been invoked by governments to pressure companies to decrypt data on request and by security agencies to dramatically increase the extent and abilities of covert electronic surveillance, *e.g.*, PRISM (NSA), TEMPORA (GCHQ).
- To say nothing of advances in quantum computing . . .

. . . The Crypto-Wars are far from over . . .

. . . And If You Liked This . . .

- MUN Computer Science courses on this area:
  - COMP 2007: Introduction to Information Management
  - COMP 2008: Social Issues and Professional Practice
  - COMP 4820: Modern Cybersecurirty & Applied Cyber Defence
- MUN Computer Science professors teaching courses / doing research in in this area:
  - Ed Brown
  - Mark Hatcher
  - Dean Parsons