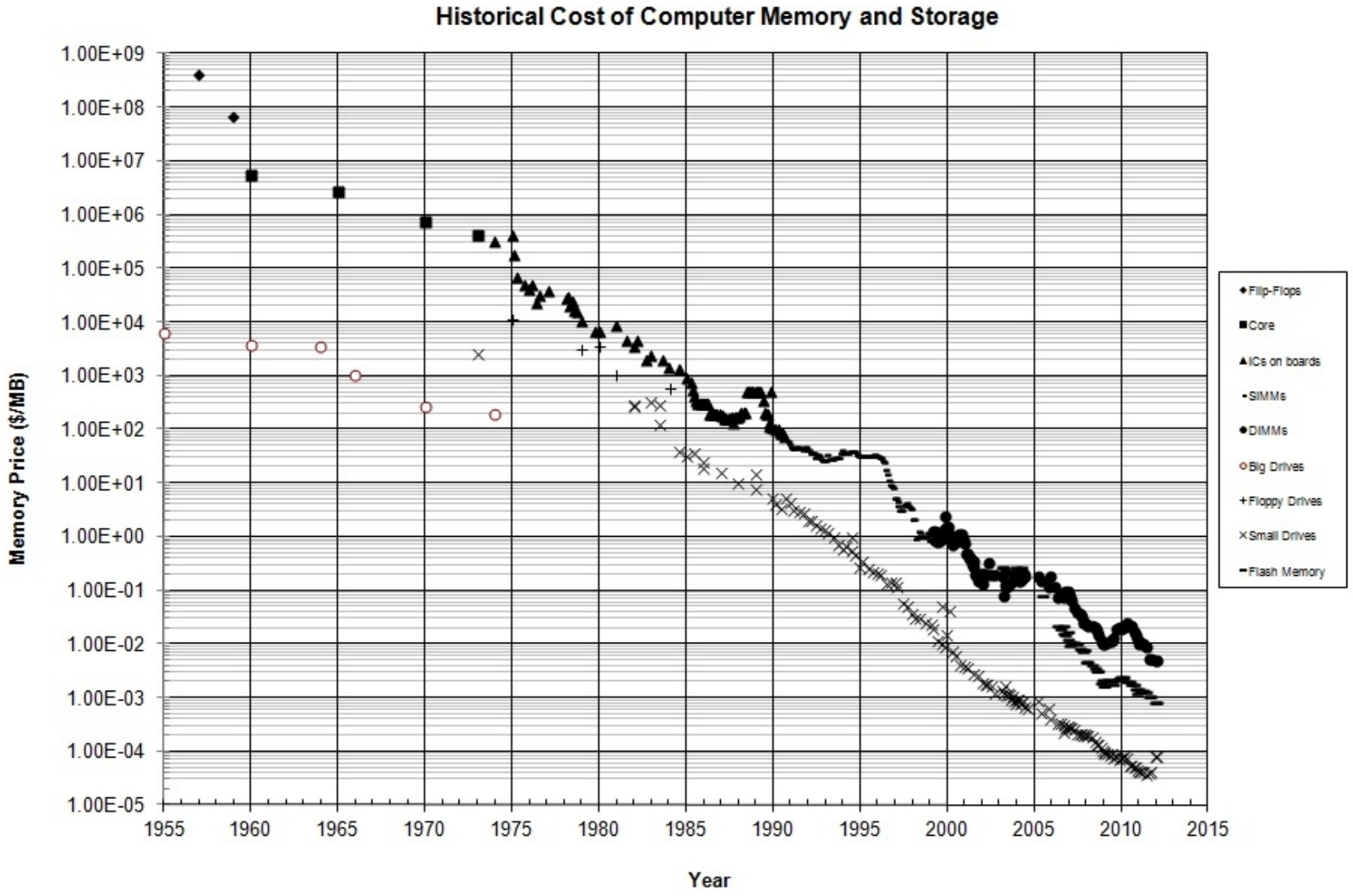
Computer Science 1400: Part #7:

Where We Are:
Big Data and Online Privacy

THE EVOLUTION OF STORED DATA

PROTECTING YOURSELF ONLINE

The Computer Memory Cost Implosion



The Evolution of Stored Data

local	$\Rightarrow$	networked / distributed
use-specific	$\Rightarrow$	detailed / overall
short-term	$\Rightarrow$	(very) long-term
user-accessible	$\Rightarrow$	anyone-accessible
bulky	$\Rightarrow$	(very) portable
one copy	$\Rightarrow$	(very) many copies
hard to copy	$\Rightarrow$	(very) easy to copy
authority-verified	$\Rightarrow$	anyone-verified

Stored Data: Joys and Perils

Joys	Characteristics	Perils
		Store false / misleading easily
Store anything easily	Storage easy	Find false / misleading easily
Find anything easily	Storage easy	Integrate / reconstruct easy
Spread anything easily	Store anything	Steal anything easily
Everything remembered	Store anytime	Spread impossible to stop
Personal customization	Store forever	Nothing forgotten
		Personal commercialization

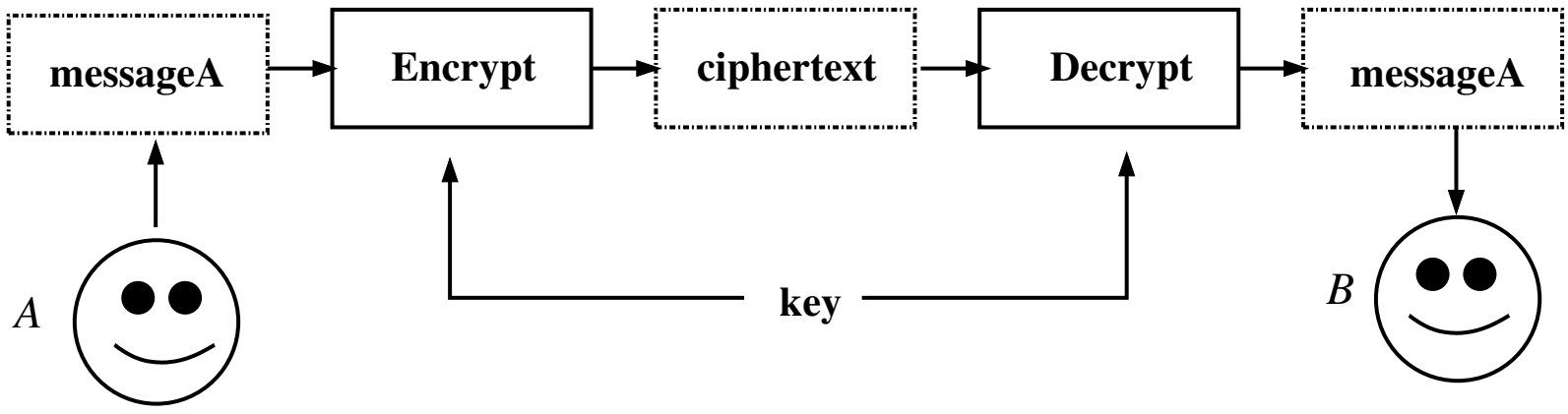
- Appropriate governance and laws are critical in mitigating the perils above; so is responsible behaviour by people.

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)

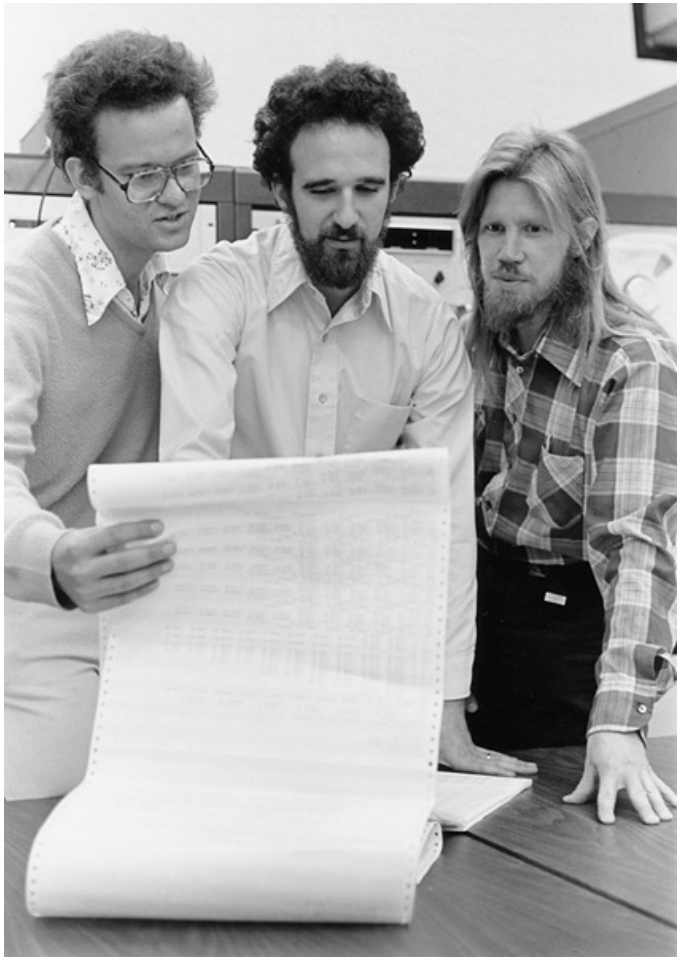
- Cryptosystem research controlled by national agencies.
- Research classified and system export prohibited, *e.g.*, International Traffic in Arms Regulation (ITAR: USA).

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

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

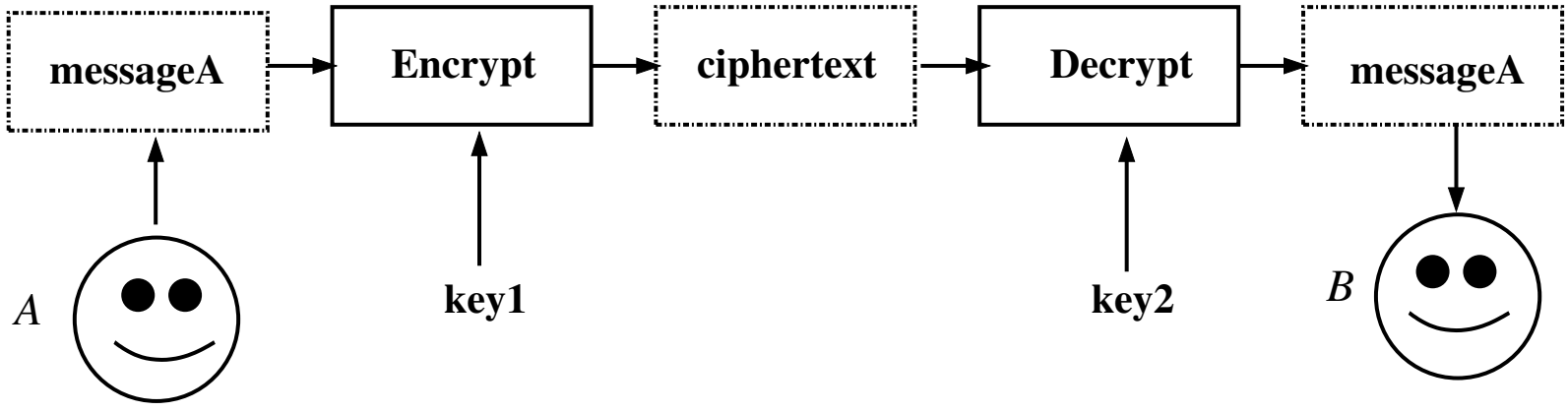
Cryptography: A Privacy Survival Tool (Cont'd)

- 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:

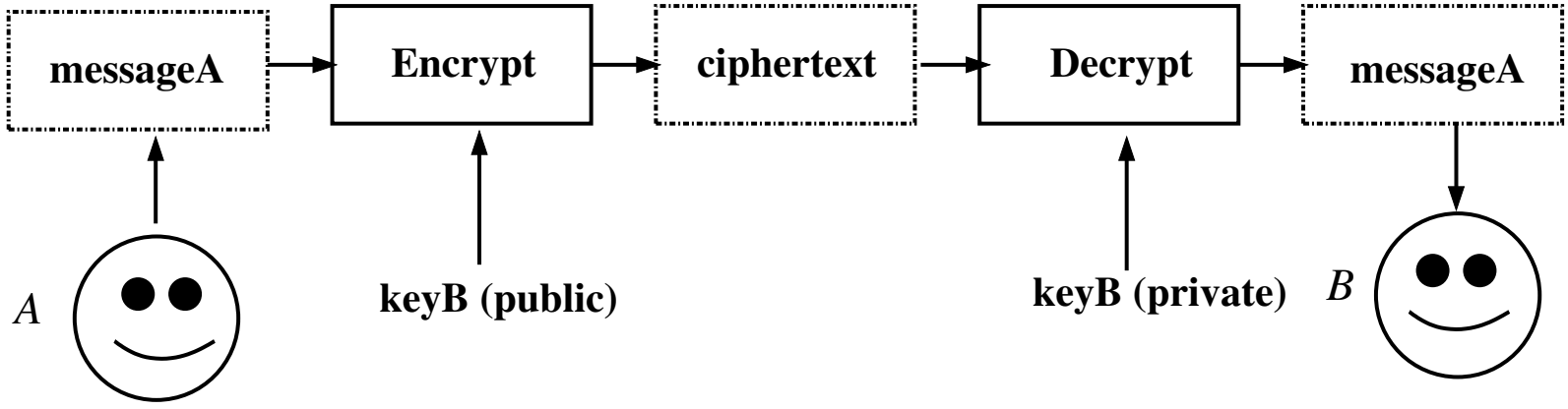


Pros:
- Provides secure messages and signatures
- Not impossible but very hard to crack
- Much software available

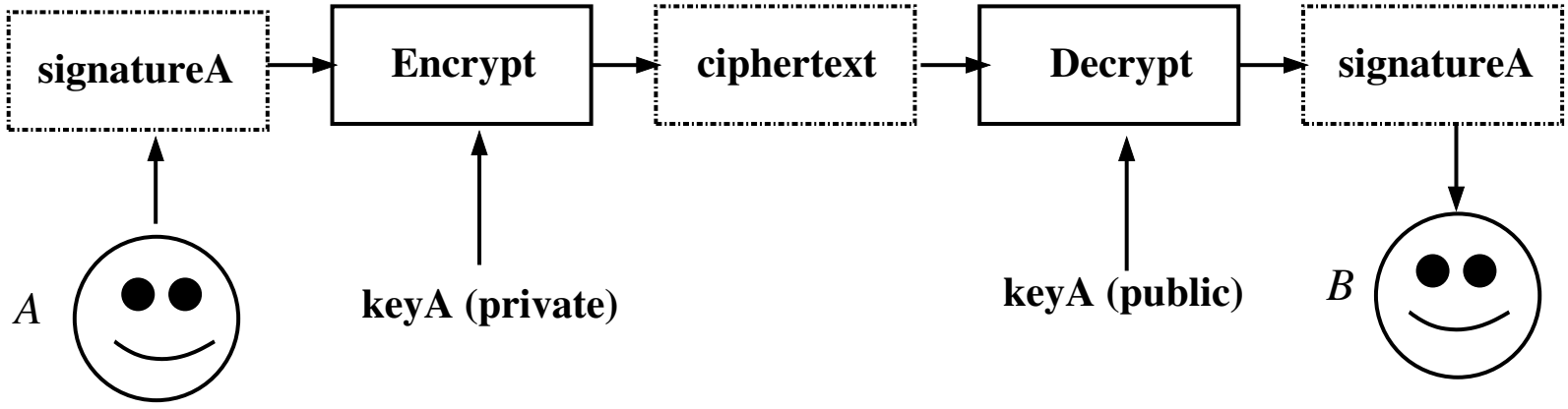
Cons:
- Computationally more expensive
- Keys can be stolen / deduced
- Available software may be illegal or compromised

Cryptography: A Privacy Survival Tool (Cont'd)

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

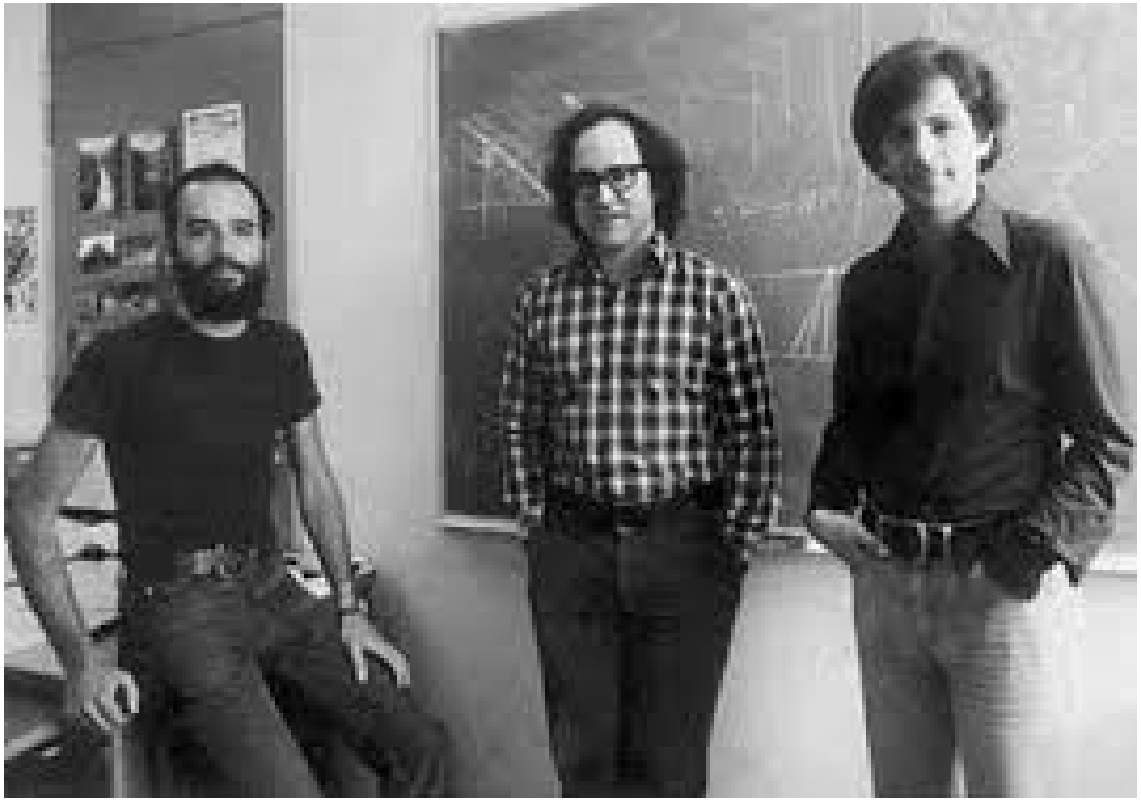


- Secure signature (encrypt signature with A's private key):



Cryptography: A Privacy Survival Tool (Cont'd)

- First practical implementation of asymmetric cryptography created by Ron Rivest (1947–), Adi Shamir (1952–), and Len Adelman (1945–) in 1977 (RSA Algorithm).



Shamir, Rivest, and Adelman (1977)

Cryptography: A Privacy Survival Tool (Cont'd)

- Asymmetric cryptography propagates (illegally) worldwide via the Pretty Good Privacy (PGP) system created by Phil Zimmerman 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).

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

Surviving and Thriving with Big Data

- Learn crap detection and online research skills (Rheingold)
- Limit degree of personal (esp. commercial) exposure online
  - Know privacy settings and use appropriately
- Limit types of personal exposure online
- Use encryption where possible (and legal)
- Update your computing devices with security fixes regularly
- Be aware of what's going on privacy-wise both technologically and commercially

"Don't Panic" – *The Hitchhiker's Guide to the Galaxy*
"Let's be careful out there" – *Hill Street Blues*