

Science 1000: Part #4 (Wareham):

Where We Are: Big Data and Online Privacy

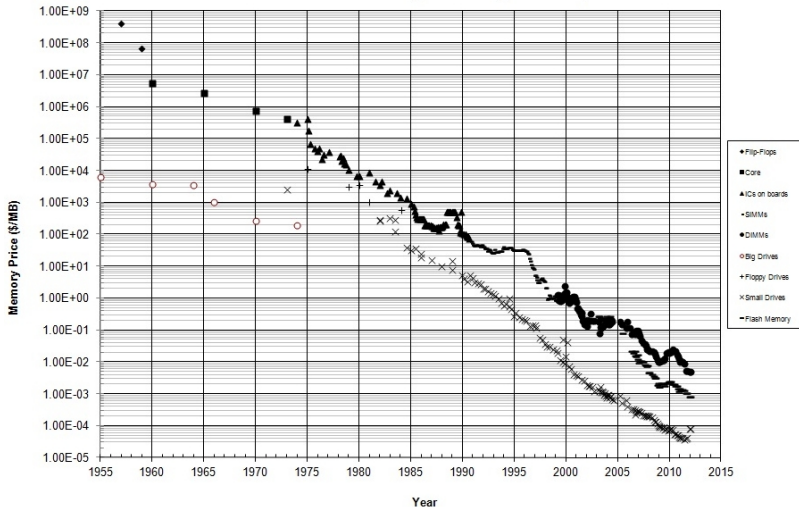
THE EVOLUTION OF STORED DATA

THE EVOLUTION OF PRIVACY

PROTECTING YOURSELF ONLINE

The Computer Memory Cost Implosion

Historical Cost of Computer Memory and Storage



The Evolution of Stored Data

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

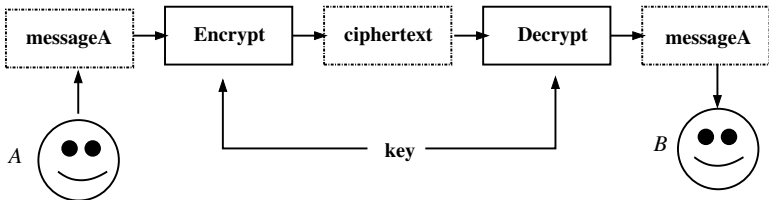
Stored Data: Joys and Perils

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

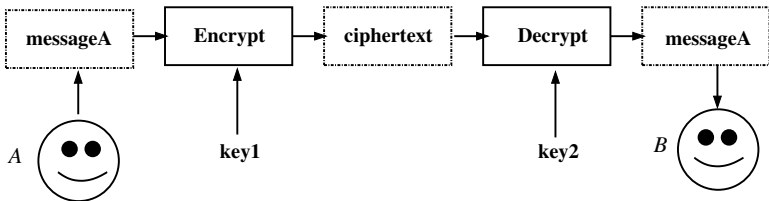
- Protect personal data and identity using cryptography.
- Symmetric (one key) cryptography:



- 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)

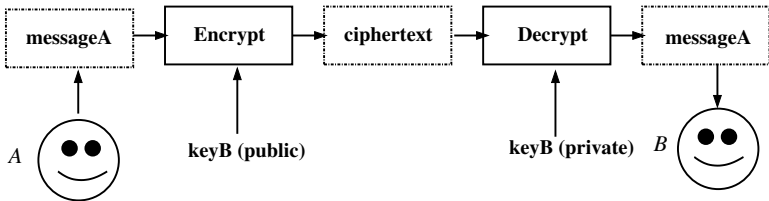
- Asymmetric (two key) cryptography:



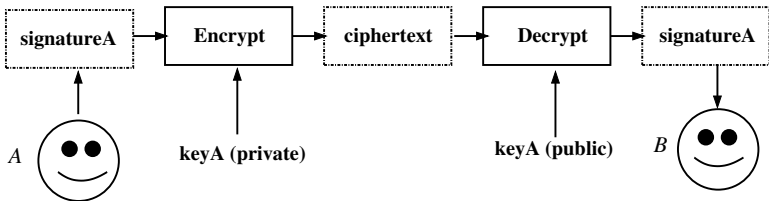
- Pros:**
- Provides secure messages and signatures
 - Not impossible but very hard to crack
 - Much software available
- Cons:**
- Computationally more expensive
 - Keys can be stolen / deduced
 - Available software is often illegal

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):



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 Hitchiker's Guide to the Galaxy*

“Let's be careful out there” – *Hill Street Blues*