Cryptography and You

Corey Ford, Liam Kirsh

The White Hat

2015-01-14

Why Encrypt?

Public-Key Encryption

PGP

Tutorial!

What data is out there?

- The web searches you make
- The links you click
- The emails you send
- The chats you have

Who has access?

Third-party advertisers

- Advertisers build an online profile of you
- They have more data on people than any other source (even 9/11 attackers)
- Data collection companies store a list of data points about 1,500 items long
- Addresses, credit, pets, health

Selling data

Your profile can be sold and show up in...

- hotel and airline pricing

On Orbitz, Mac Users Steered to Pricier Hotels

By DANA MATTIOLI

- insurance costs

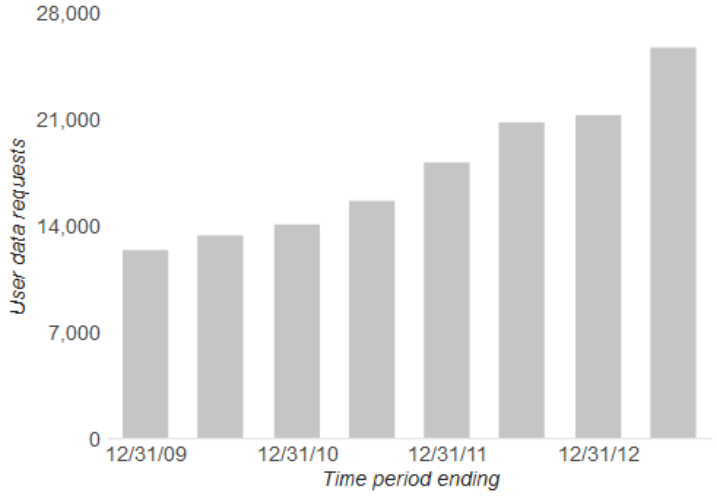
Insurers Test Data Profiles to Identify Risky Clients

By LESLIE SCISM And MARK MAREMONT

Leaking data

Your emails and searches can be...

- subpoenaed and used against you in court



- snooped on by Google employees

  This Is The Second Time A Google Engineer Has Been Fired For Accessing User Data

- leaked to hackers

  Google Hack Attack Was Ultra Sophisticated, New Details Show

Chilling Effects

"You had to live–did live, from habit that became instinct–in the assumption that every sound you made was overheard, and, except in darkness, every movement scrutinized." - 1984 by George Orwell

Who's affected?

- activists
- journalists
- lawyers
- domestic abuse victims

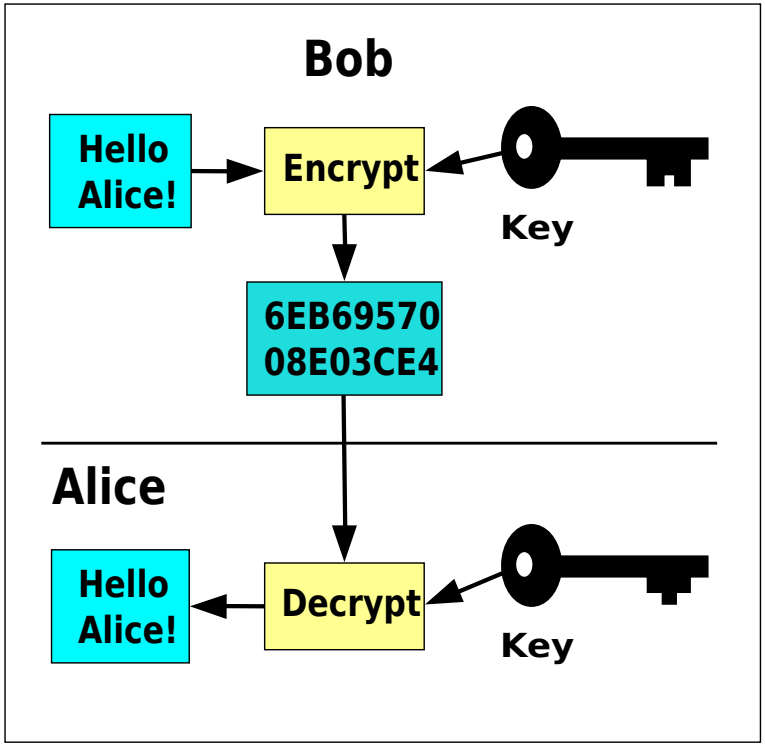
Why Encrypt?

Public-Key Encryption

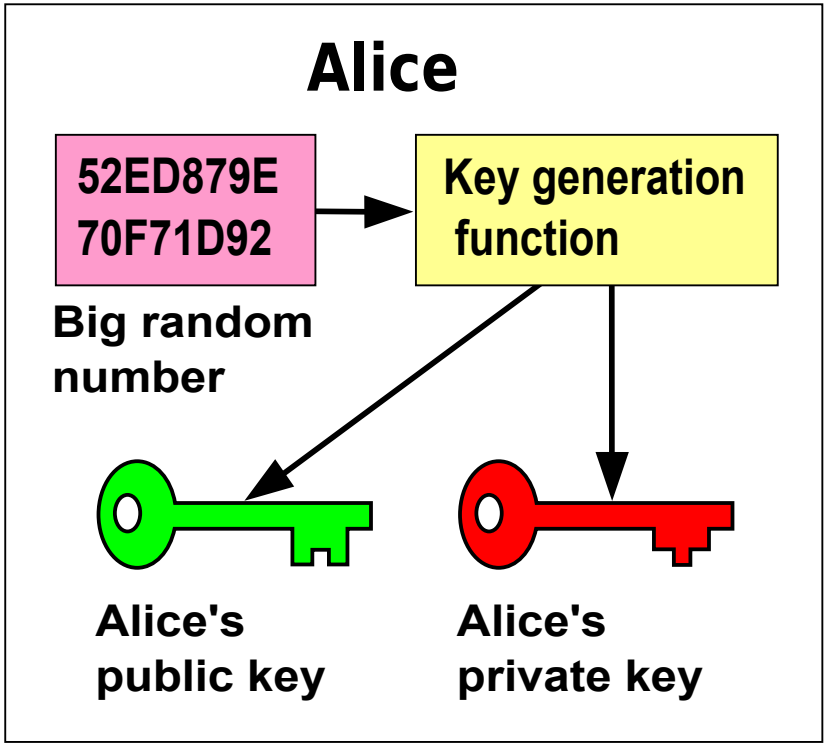
PGP

Tutorial!

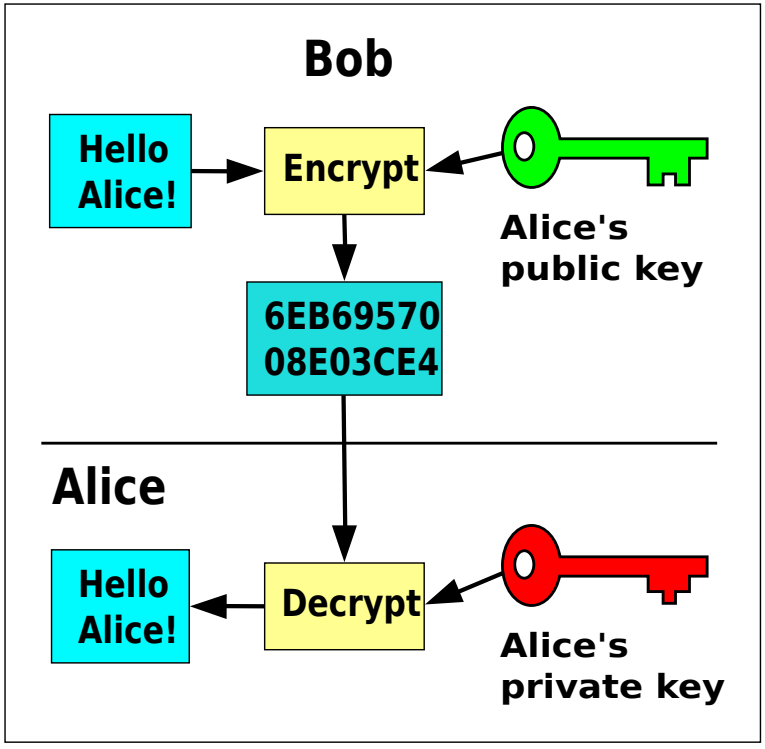
Symmetric (Private-Key) Encryption



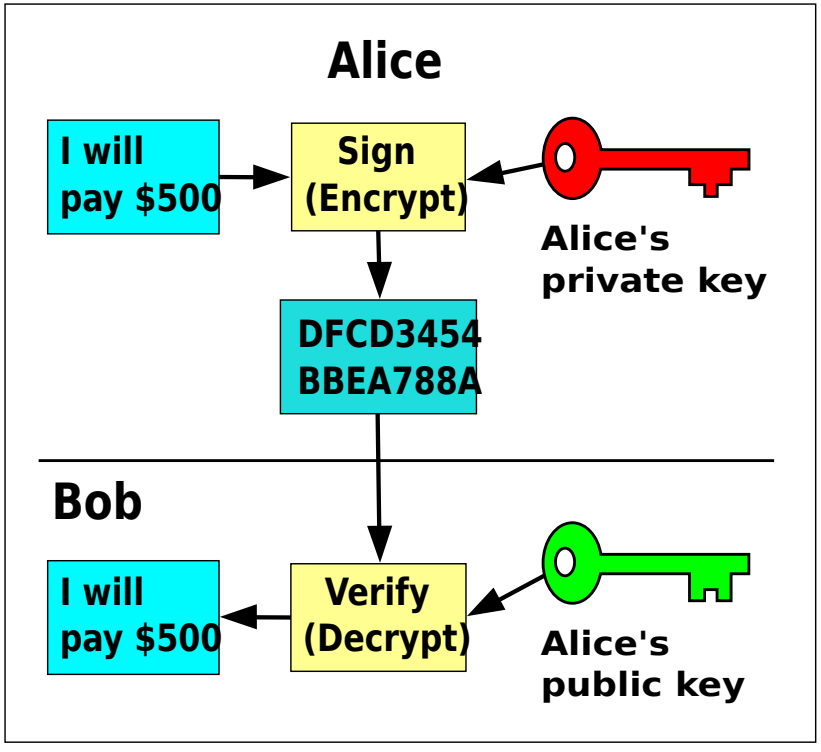
Asymmetric (Public-Key) Cryptography



Asymmetric (Public-Key) Encryption



Asymmetric (Public-Key) Signatures



RSA

- finite group $\mathbb{Z}_N$ (modular arithmetic)
- choose large primes p, q, let $N = p \cdot q$
- $\phi(N) = (p-1)(q-1)$, with the property

$$\forall_{x \in \mathbb{Z}_N^*} : x^{\phi(N)} = 1 \mod N$$

- choose e, d such that $e \cdot d = 1 \mod \phi(N)$
  (hard to find d given just e and N)

$$\begin{aligned} c &:= [m^e \mod N] \\ m &:= [c^d \mod N] \\ &= [(m^e)^d \mod N] \\ &= [m^{k\phi(N)+1} \mod N] = m \end{aligned}$$

Why Encrypt?

Public-Key Encryption

PGP

Tutorial!

Pretty Good Privacy

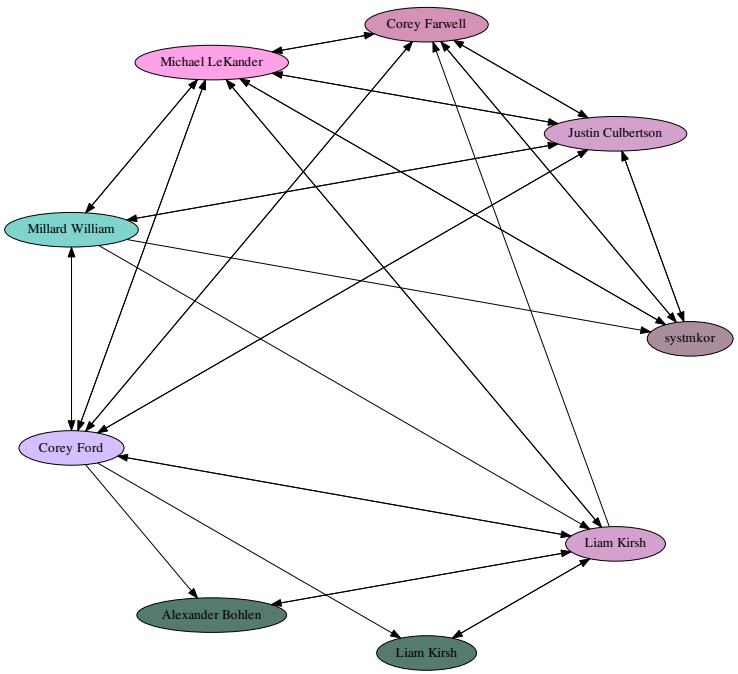
- encryption software for files, emails, . . .
- public-key (RSA) encryption and signing
- "keyring" stores:
  - public keys (lots)
  - private keys (a few)
  - user IDs (name, email)
  - signatures on user IDs
  - . . .

History, Terminology

- created by Phil Zimmerman in 1991
- circumvented export restrictions by publishing source code in a book
- OpenPGP: a standardized protocol
- GNU Privacy Guard (GnuPG): an open-source implementation

Web of Trust

- how to establish trust/identity?
- signatures on user IDs by other keys!
- decentralized (transitive) trust
- keyservers (untrusted) to distribute public keys



Why Encrypt?

Public-Key Encryption

PGP

Tutorial!

Do

1. install stuff
   - GnuPG (`gpgtools.org`, `gpg4win.org`)
   - Thunderbird + Enigmail (or use Apple Mail)
2. generate a key pair, recommendations:
   - 4096-bit RSA
   - correct name + email, no comment
   - expiration in 2–5 years
   - save revocation certificate when prompted
3. share public key (upload to `pgp.mit.edu`)
4. sign keys
   - find someone else who has uploaded their public key
   - download it from a keyserver (by email or fingerprint)
   - verify key fingerprint + identity (photo ID)
   - if satisfied, sign key
   - upload key again