Using SmartCards for Public Key Cryptography

Andy Sayler
Matthew Monaco

Using SmartCards for Public Key Cryptography

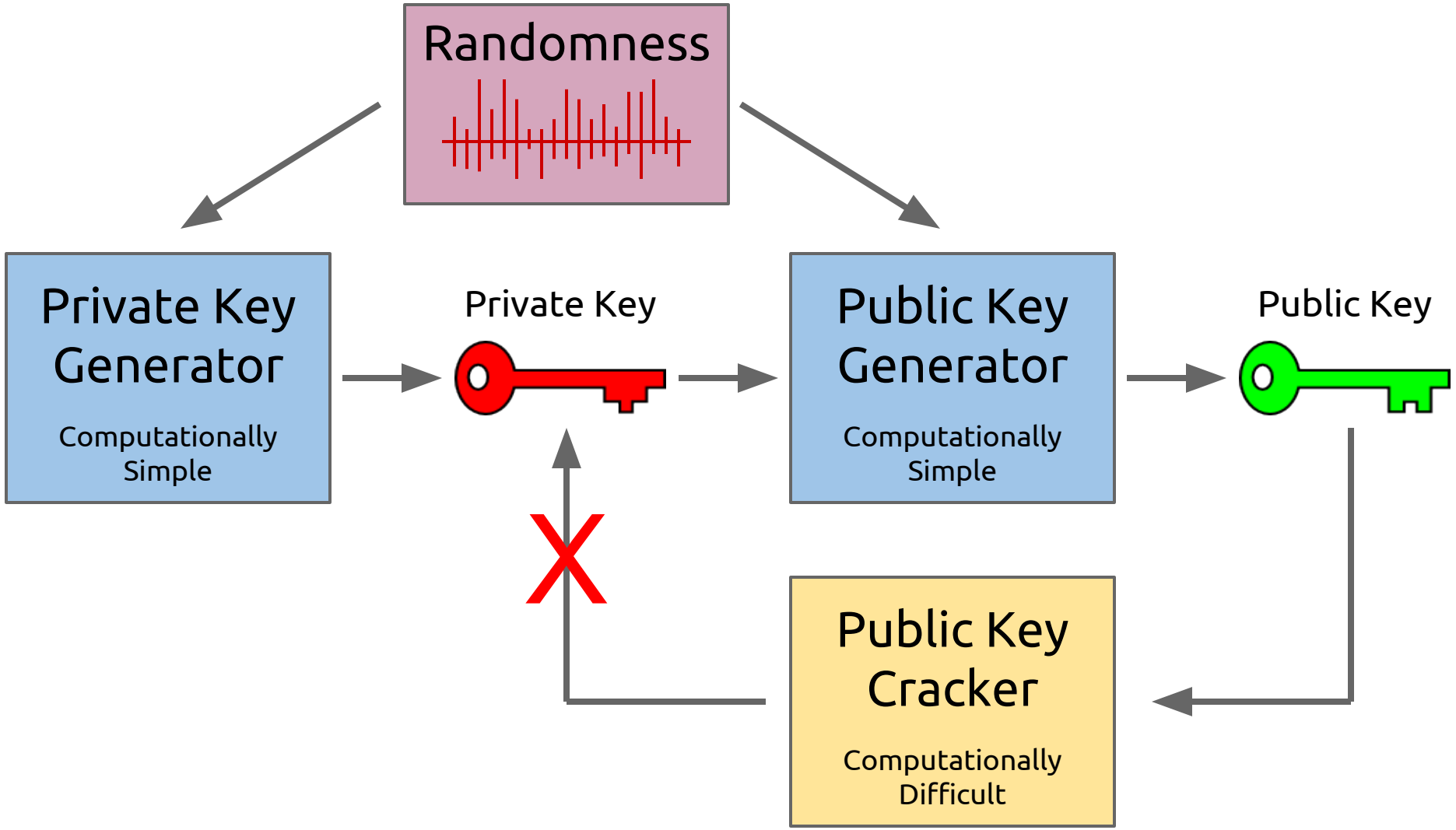
ALICE

Andy Sayler
Matthew Monaco

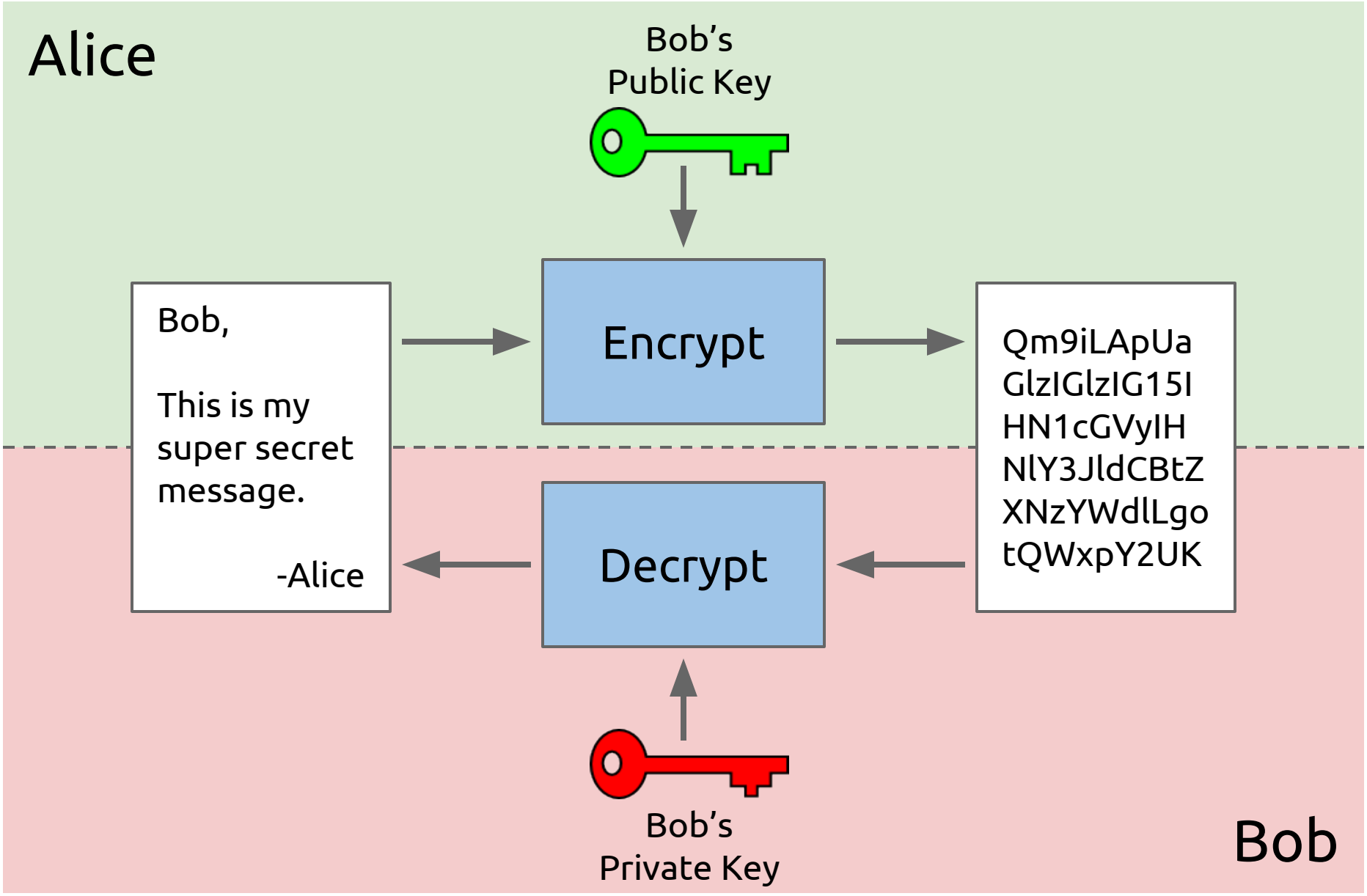
BOB

Public Key Cryptography

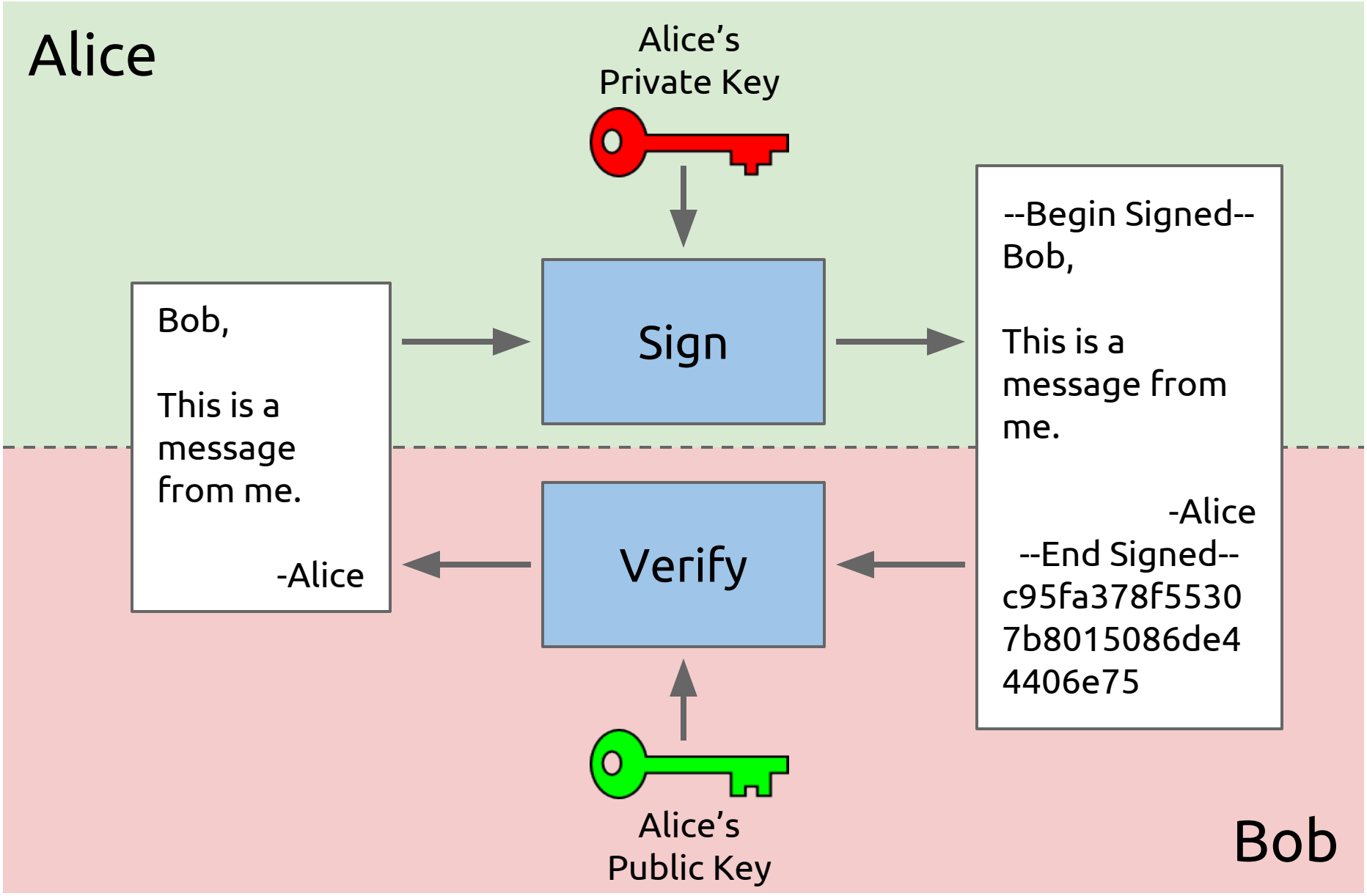
Generate Key



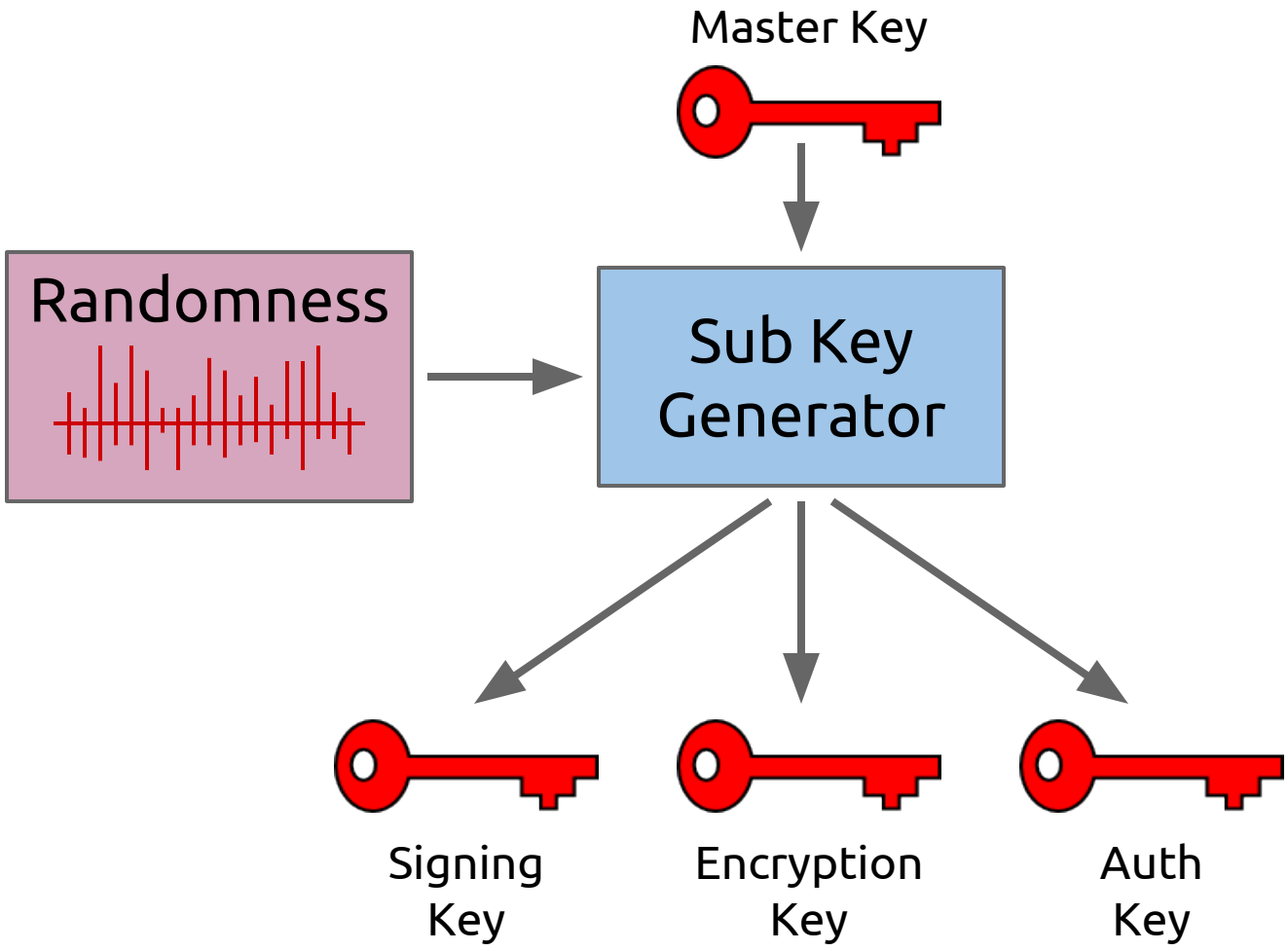
Encrypt Message



Sign Message



Generate Sub-Keys



OpenPGP/GnuPG

RFC 4880: OpenPGP

Network Working Group
Request for Comments: 4880
Obsoletes: 1991, 2440
Category: Standards Track

J. Callas
PGP Corporation
L. Donnerhacke
IKS GmbH
H. Finney
PGP Corporation
D. Shaw
R. Thayer

November 2007

OpenPGP Message Format

Status of This Memo

Abstract

This document is maintained in order to publish all necessary information needed to develop interoperable applications based on the OpenPGP format. It is not a step-by-step cookbook for writing an application. It describes only the format and methods needed to read, check, generate, and write conforming packets crossing any network. It does not deal with storage and implementation questions. It does, however, discuss implementation issues necessary to avoid security flaws.

OpenPGP software uses a combination of strong public-key and symmetric cryptography to provide security services for electronic communications and data storage. These services include confidentiality, key management, authentication, and digital signatures. This document specifies the message formats used in OpenPGP.

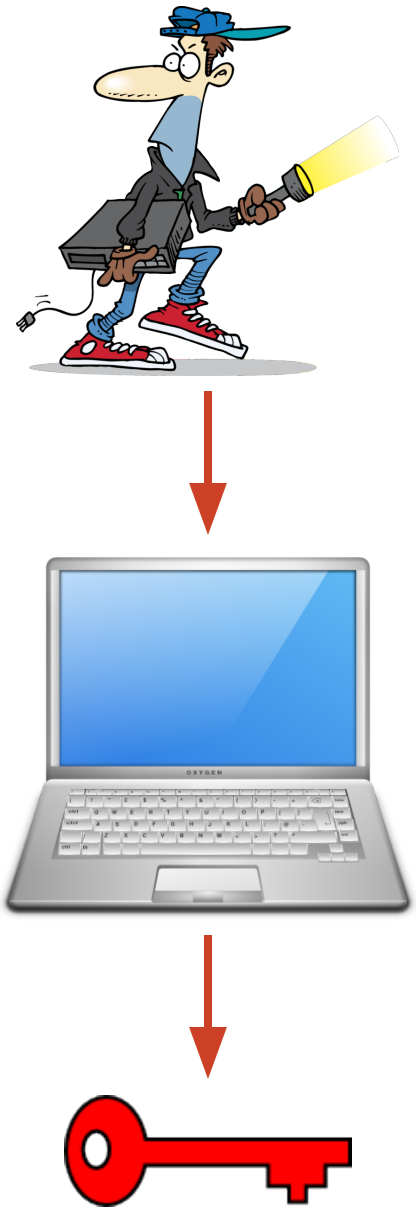

```
asayler@raptor:~$ gpg -K
/home/asayler/.gnupg/secring.gpg
--------------------------------
sec#  4096R/32C59C00 2013-10-08 [expires: 2014-10-08]
uid                  Andrew Sayler <andrew.sayler@colorado.edu>
uid                  Andy Sayler <andy@wmfo.org>
uid                  Andy Sayler (andysayler.com)
uid                  Andrew Jackson Sayler (Born September 6th, 1988)
uid                  Andy Sayler (asayler) <andy.sayler@gmail.com>
uid                  Andrew Sayler (Graduated May 2011, BSEE) <andrew.sayler@alumni.tufts.edu>
uid                  Andy Sayler <neueWelt@gmail.com>
ssb   4096R/89CA44D2 2013-10-08
ssb   4096R/9FF0E192 2013-10-08
```

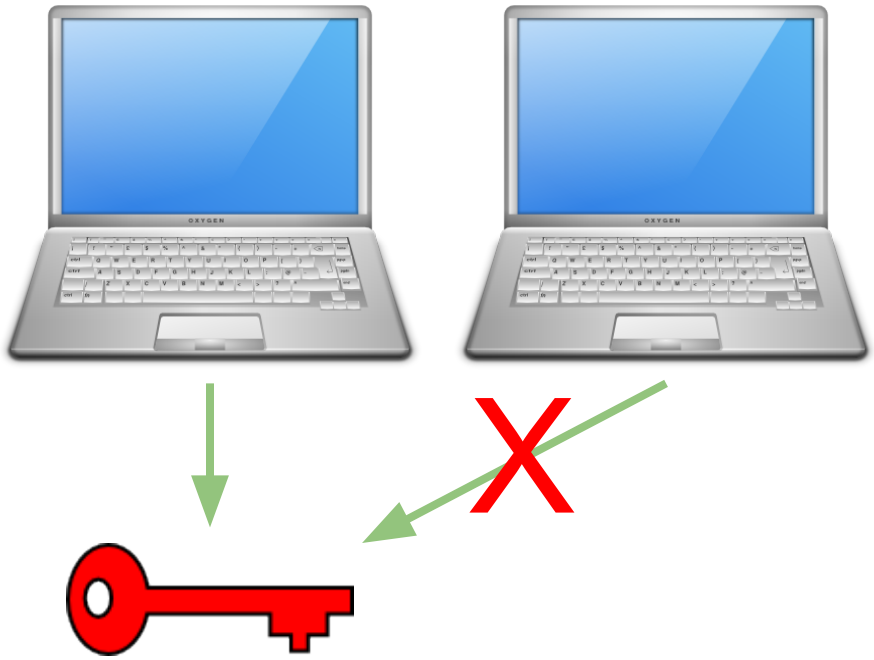
csel.cs.colorado.edu/openpgp.html

Why SmartCards?

How do you securely store private keys?

On your laptop?





SmartCards Provide...

SmartCards Provide...

On-Person Storage

SmartCards Provide...

On-Person Storage

Physical Security

SmartCards Provide...

On-Person Storage

Physical Security

Multi-Device Access

SmartCards Provide...

On-Person Storage

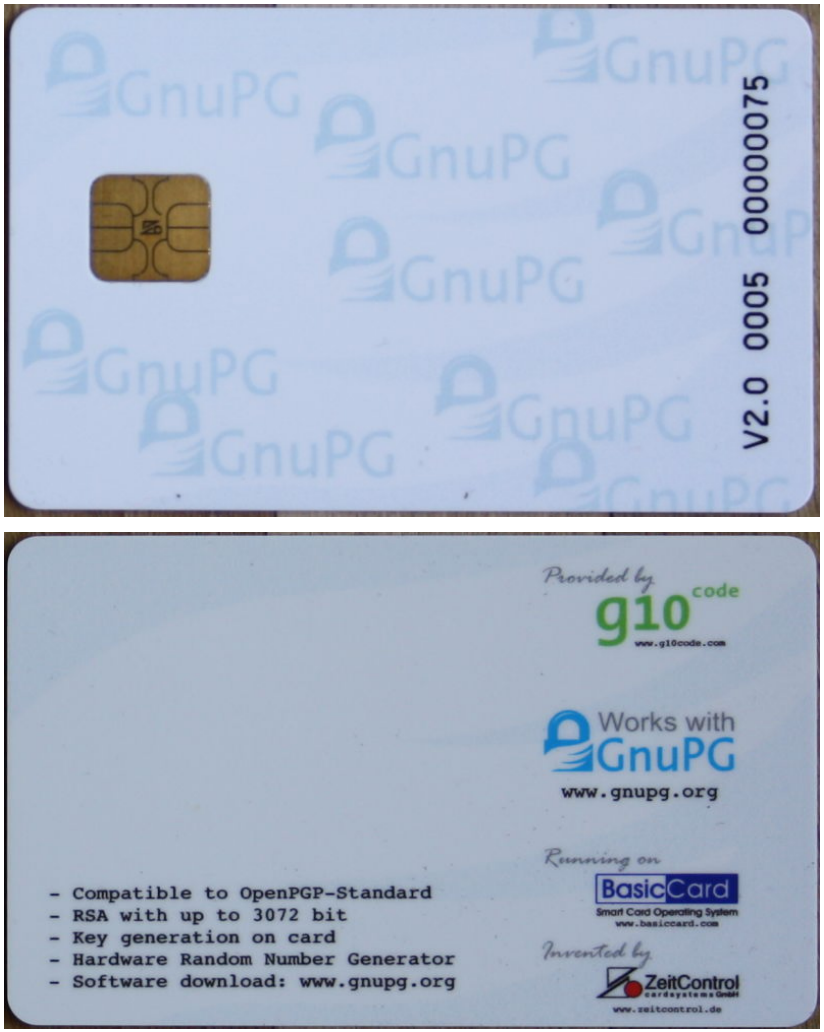
Physical Security

Multi-Device Access

On-Key Crypto

Existing Systems

OpenPGP Card v2.0 (g10 Code)



Type: ISO 7816-4/8 Card

Storage: 3 2048-bit RSA Keys

Security: NIST Hardened

Software PIN

On-Card Key Gen: Optional

Internals: Propriety

Reader: External

Price: ~$30.00

Crypto Stick v1.4 (CryptoStick)

Type: USB Card

Storage: 3 4096-bit RSA Keys

On-Card Key Gen: Optional

Security: Software PIN

Internals: Gnuk

Reader: USB

Price: Discontinued

YubiKey Neo (Yubico)

Type: USB Card

Storage: 3 2048-bit RSA Keys

Security: NIST Hardened

Software PIN

On-Card Key Gen: Required

Internals: JavaCard (GPL)

Reader: USB + NFC

Price: $50

Our Ideal Card

Type: USB Card

Storage: 3+ 4096-bit RSA Keys

3+ EC Keys

Security: NIST Hardened

Physical Button/PIN

On-Card Key Gen: Optional

Internals: Open Source

Reader: USB + NFC + RFID

Price: Under $50

Future Applications

Excellence Award

Presented to

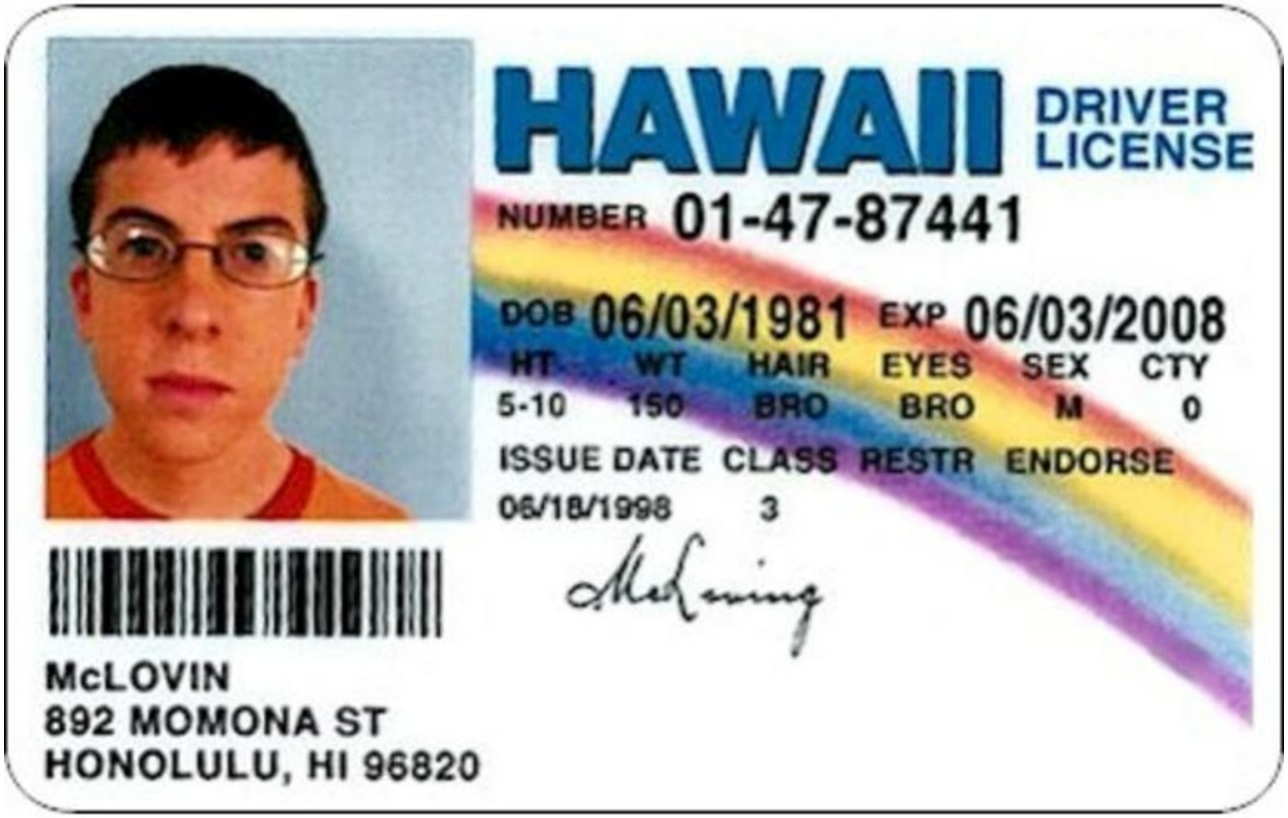
<Type Person's Name Here>

for

<Type brief description here>

<date>

<Type your name>
<Your Title>


HAWAII DRIVER LICENSE
NUMBER 01-47-87441
DOB 06/03/1981 EXP 06/03/2008
HT WT HAIR EYES SEX CTY
5-10 150 BRO BRO M 0
ISSUE DATE CLASS RESTR ENDORSE
06/18/1998 3
McLOVIN
892 MOMONA ST
HONOLULU, HI 96820


35 CLAYTON
FRONT DOOR
GUESTBOOK


August
www.dexigner.com


LOCK
UN LOCK


LOCK
UNLOCK

FROM: AMERICAN EXPRESS


That's all Folks!