GPG Key Signing Party

Fedora 21 Release Party & Hardware Freedom Day 2015

PRESENTED BY:
Tong Hui 佟辉
4096R/A6D42018

https://tonghuix.fedorapeople.org/F21-HFD2015.pdf

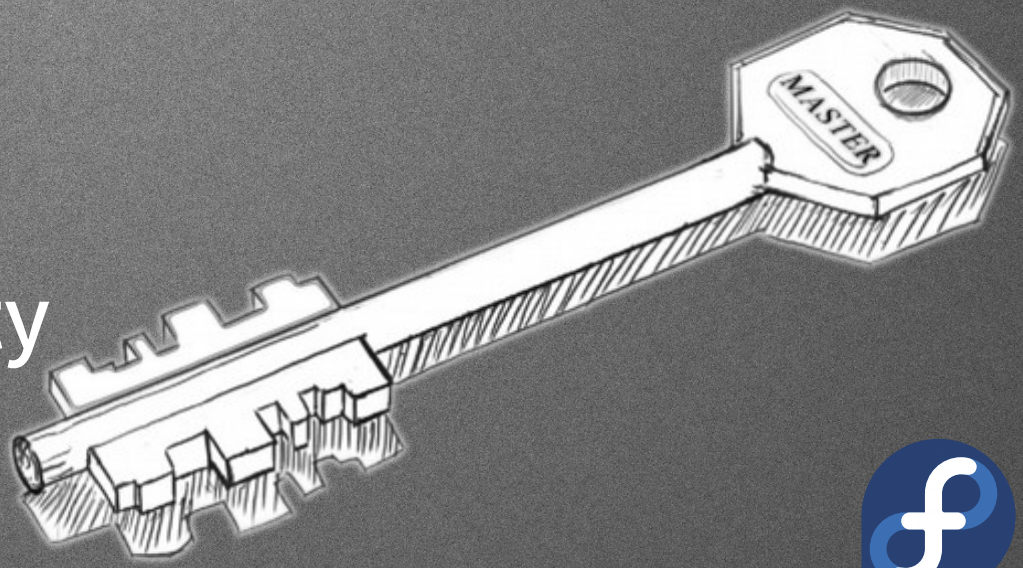
开始之前……

安装 Seahorse 、 Kgpg

```
sudo yum install seahorse kgpg
sudo yum install seahorse-nautilus
```

Agenda

- Password / Passphrase / 口令 / 密码
- 随机与散列
- 密钥与对称加密
- 非对称加密
- 我可以信任你吗?
- WoT 与 Signing Party



若已有 GPG 密钥对

- 请执行

  `gpg --fingerprint KEYID`

- 并将输出结果原封不动的贴到：

  https://blug.hackpad.com/F21-GPG-Key-Signing-Party

- 并执行

  `gpg --send-keys`


口令
Password

口令的那些事……

- Password / Passphrase 口令
- 芝麻芝麻快开门。。
- 天王盖地虎，……

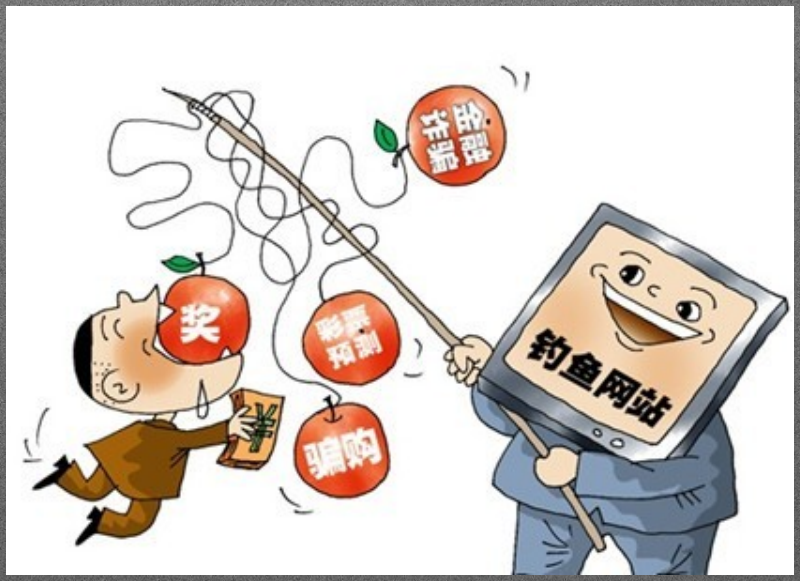
口令的注意事项

- 保密
- 密码空间（长度），抵抗暴力穷举破解
- 抵抗社会工程学（Social Engineering）攻击
- 随机
- 易记忆
- 密钥与密文分离

社会工程学
Social Engineering

- 假托（pretexting）
- 调虎离山（diversion theft）
- 钓鱼
- 等价交换
- 尾随

……



简单的办法……

- Passwordcard.org

随机与散列

生活处处有随机

- 掷硬币
- 掷骰子
- 转笔
- ……

随机的特性

- 随机性
- 不可预测性
- 不可重现性

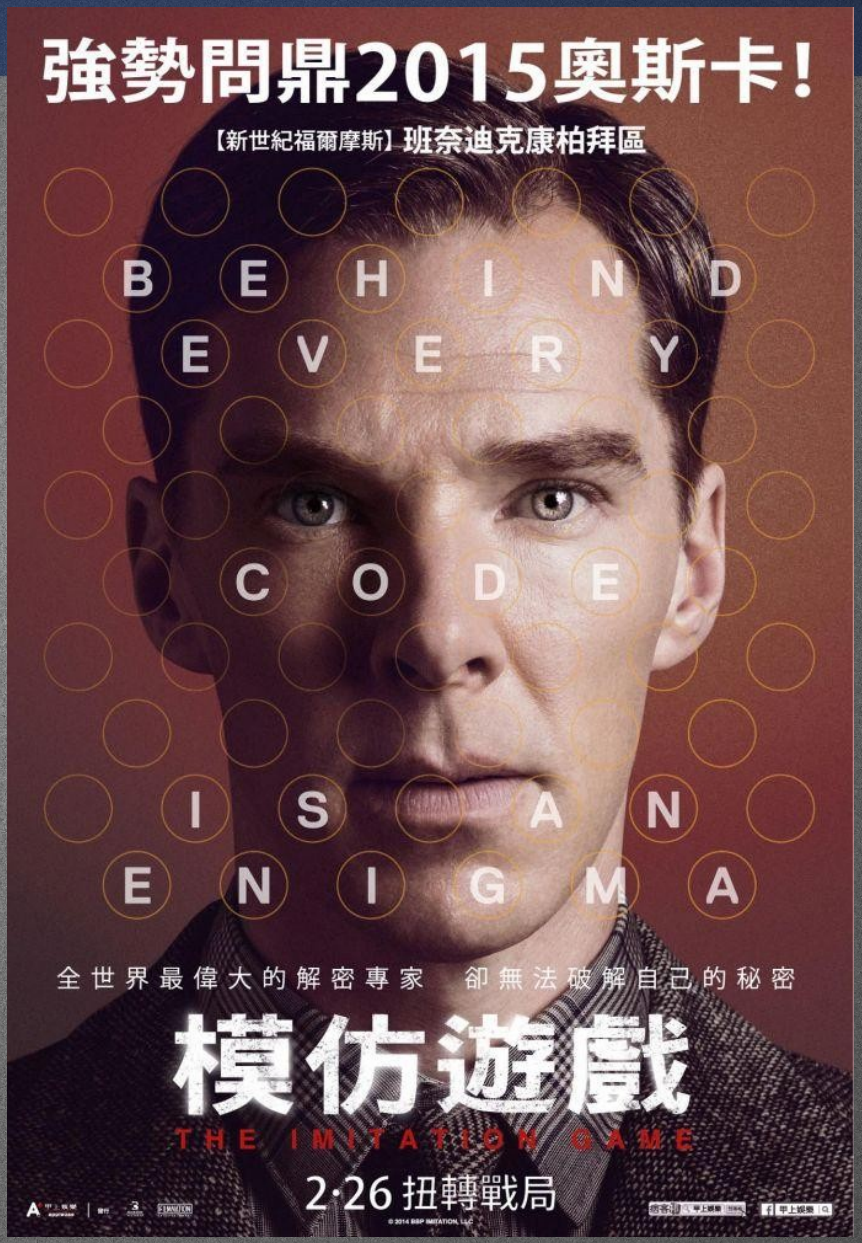
散列 Hash

- hash (杂碎的肉、剁碎、俚语表示传闻)
- 取文件的摘要，文件完整性验证，防止篡改
- 单向性，不可逆
- 唯一的散列值，即指纹 Fingerprint
- 常见散列算法 MD4/MD5 、 SHA-1 、 SHA-256/224 、 SHA-512/384 等
- 口令验证，例如 /etc/shadow
- 验证校验和，文件完整性
  - md5sum
  - sha256sum
  - sha512sum

密钥与对称加密

从一部电影说开去……

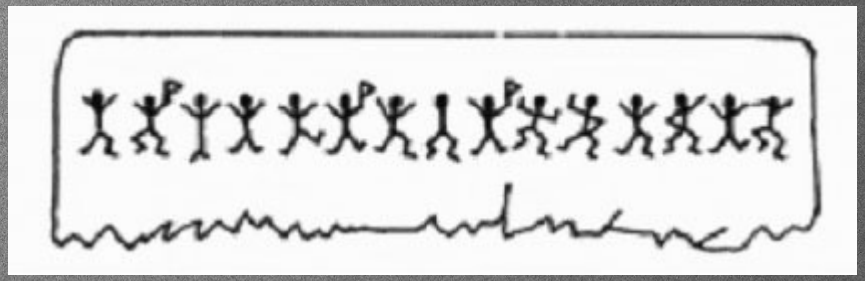
- 导演：莫滕·泰杜姆
- 编剧：格拉汉姆·摩尔
- 主演：本尼迪克特·康伯巴奇 /
- 凯拉·奈特莉 / 马修·古迪
- 类型：剧情 / 传记 / 战争
- 制片国家 / 地区：英国 / 美国
- 语言：英语
- 上映日期：2014-11-14(英国)
- 2014-12-25(美国)
- 片长：114 分钟
- 又名：模拟游戏



生活处处有对称加密

替换加密：

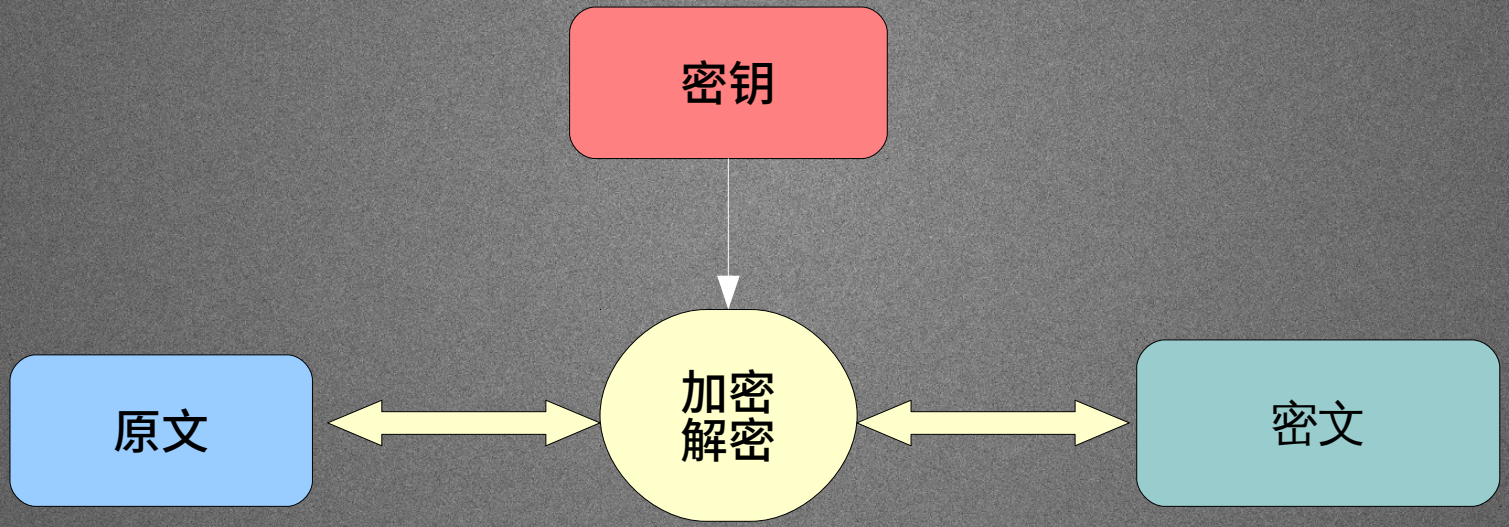
MD！ 我的 VPN 又 TM 被 GFW 了！
What the F**k！



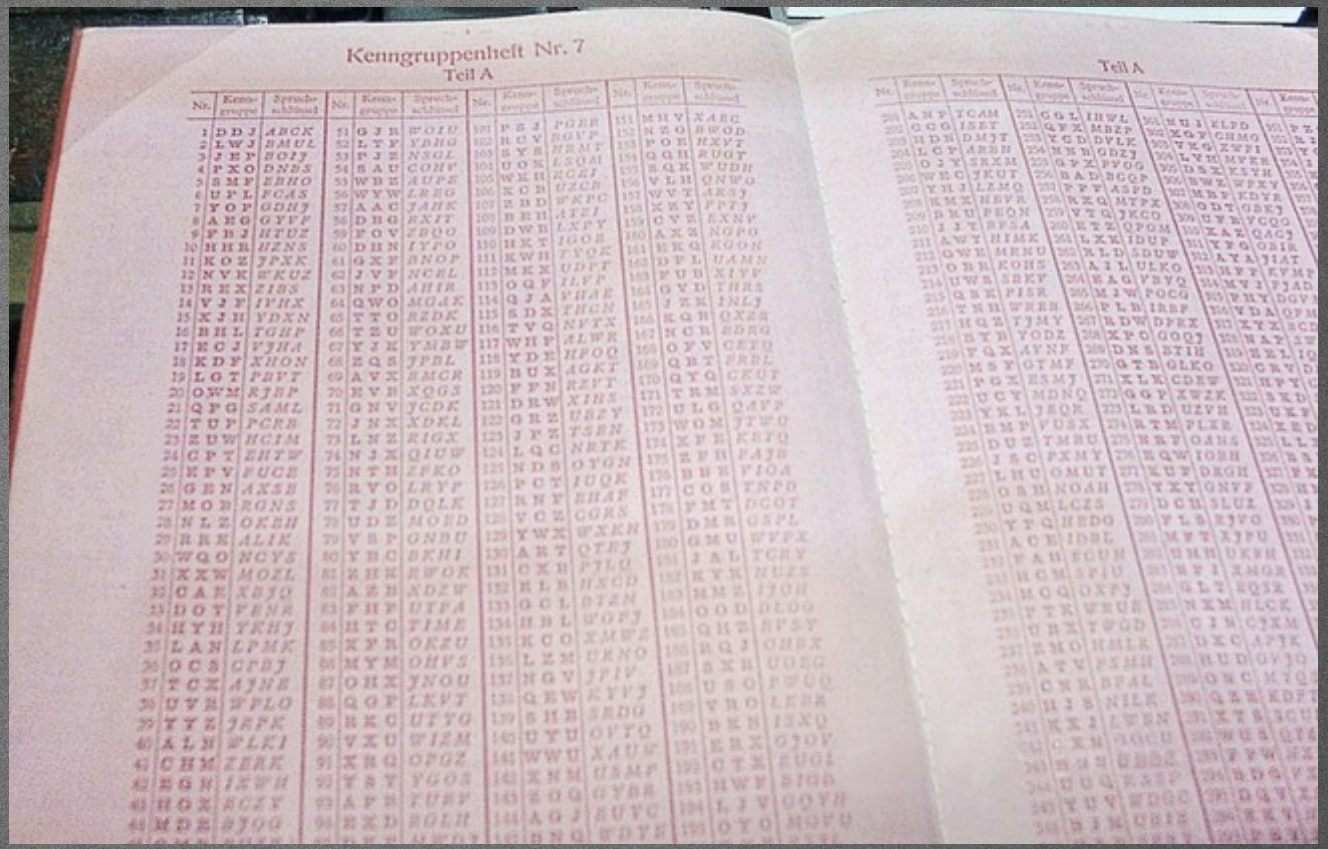
密码棒

对称加密

- 同法同钥莫同传



德国纳粹的 Enigma



现代计算机的对称加密

常见对称加密算法： DES、 DES3、 AES、 IDEA、 Blowfish 等

```
openssl des3 -a -salt -in <plaintxt> -out <encrytofile> # 加密
```

```
openssl des3 -d -a -in <encrytofile> -out <decrytofile> # 解密
```

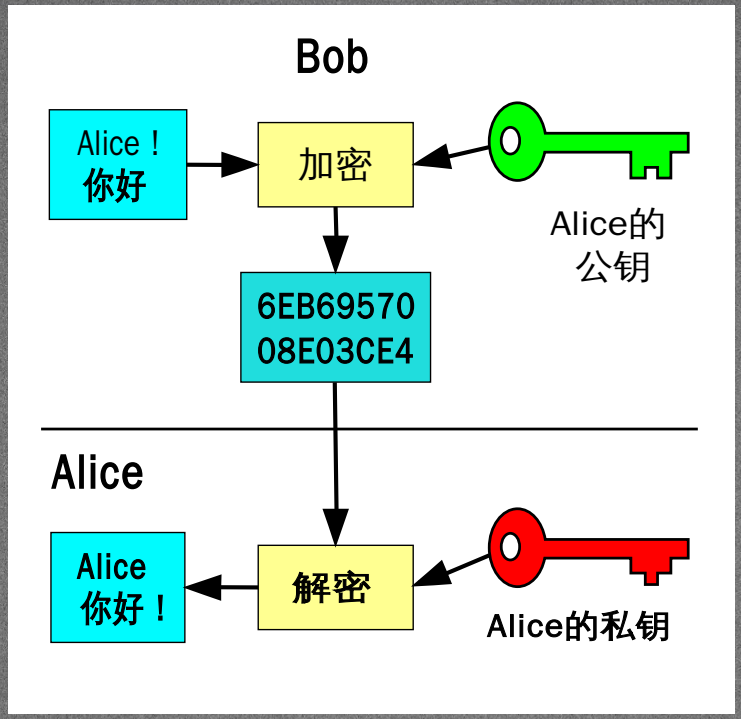
http://www.tutorialspoint.com/unix_commands/enc.htm

对称加密面临的问题

- 密钥的存储
- 密钥的变更
- 密钥的传送（Diffie–Hellman 密钥交换）
- 密钥的保密性
- 基于密钥的加密（PBE）

非对称加密

基于公钥的加密



- 公钥加密私钥解，私钥签名公钥验
- 公钥扩散如孢子，私钥秘藏不示人
- 常见公钥加密算法： RSA、 Elgamal、 Robin
- 基于 Diffie-Hellman 密钥交换算法产生的公钥

PGP、OpenPGP、GnuPG

- 公钥加密速度慢！特别慢！
- PGP (Pretty Good Privacy) 是一种混合加密的商业软件
- OpenPGP (RFC4880) 基于 PGP 的混合加密标准
- GnuPG (GPG) 是基于 OpenPGP 标准的自由软件实现

GnuPG

GnuPG 的图形客户端

- GNOME / MATE 桌面环境 Seahorse
- KDE 桌面环境 Kgpg
- 通用客户端 Kleopatra / GPA
- Mac OS X 工具包 gpgtool
- Windows 工具包 Gpg4win
- 邮件客户端：
  Evolution、 Kmail、 Thunderbird+Enigmail
- 命令行邮件客户端： mutt、 Emacs + mew 等

实际操作：生成 GPG 密钥对

- 安装 Seahorse、 Kgpg

```
sudo yum install seahorse kgpg \
                 seahorse-nautilus
```

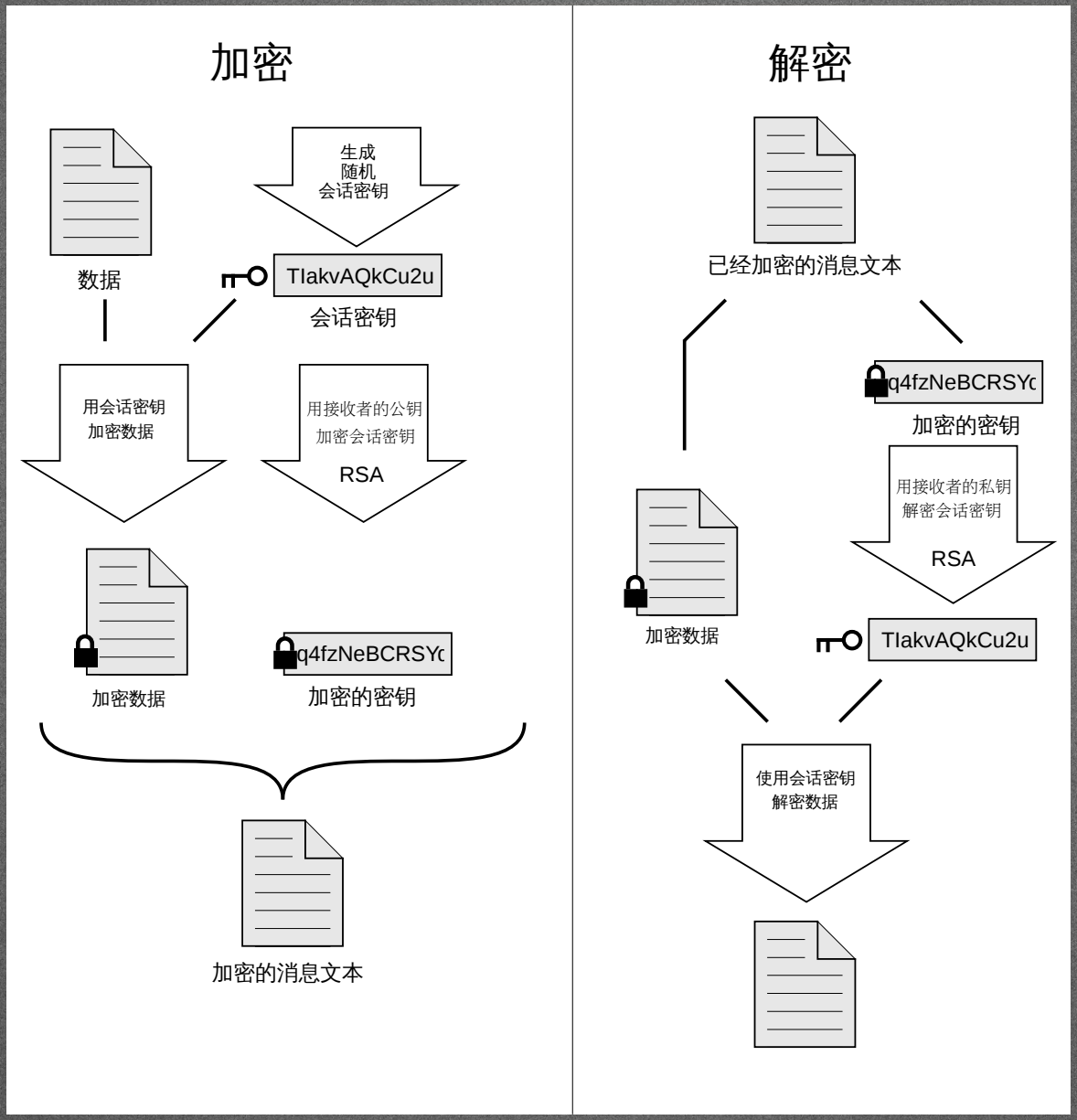
- 生成一个 GPG 密钥对 (Keyring)

- 查看刚刚生成的密钥对

混合加密

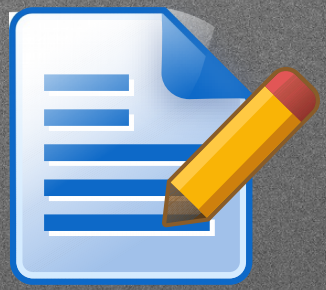
- 用随机数（盐）和散列产生一次性会话密钥（Session Key）
- 用此会话密钥对称加密明文
- 用公钥非对称加密会话密钥
- 将加密的会话密钥和密文组合打包

混合加密

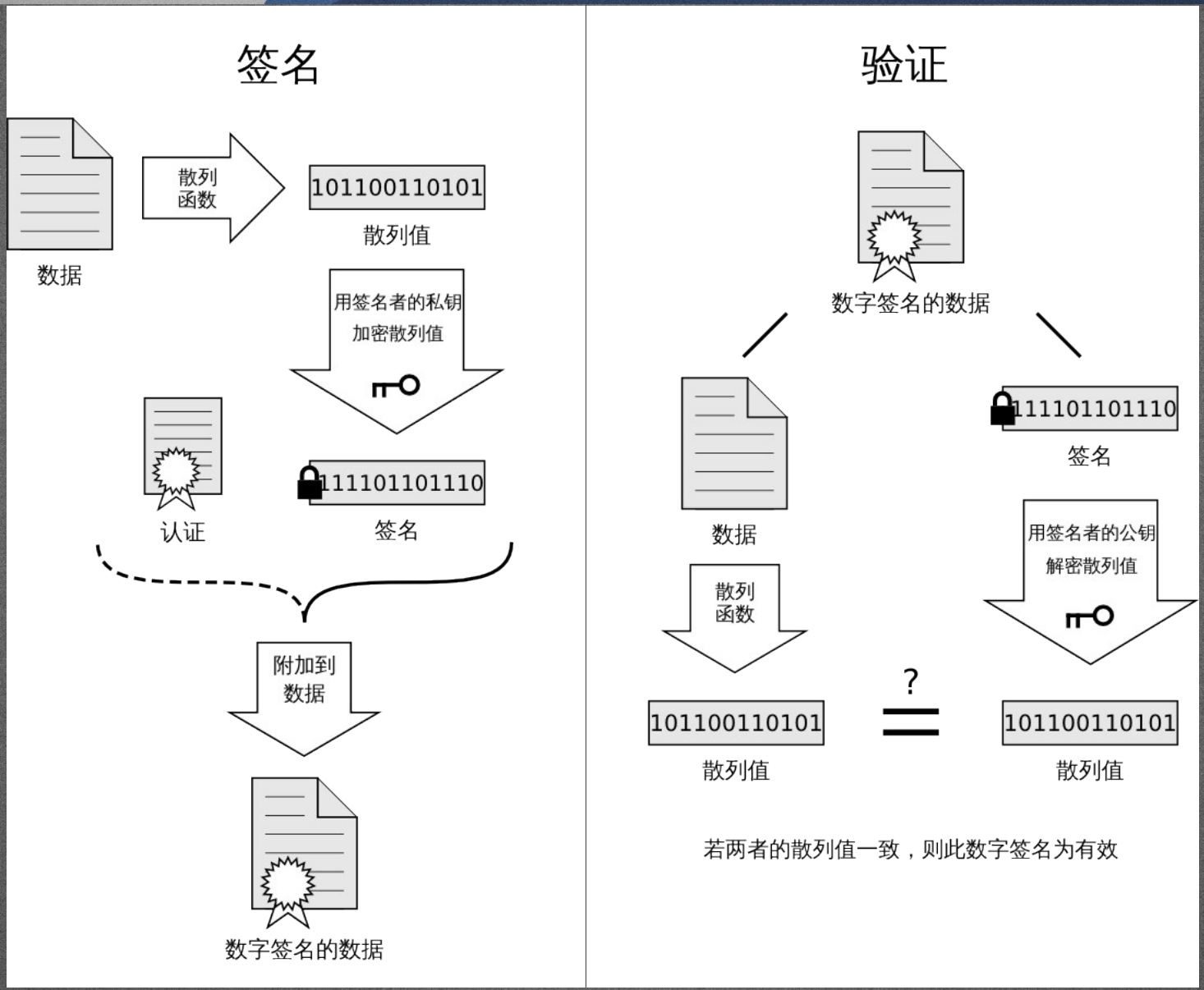

加密
数据
生成
随机
会话密钥
TIakvAQkCu2u
会话密钥
用会话密钥
加密数据
用接收者的公钥
加密会话密钥
RSA
加密数据
q4fzNeBCRSYc
加密的密钥
加密的消息文本
解密
已经加密的消息文本
q4fzNeBCRSYc
加密的密钥
用接收者的私钥
解密会话密钥
RSA
加密数据
TIakvAQkCu2u
使用会话密钥
解密数据

数字签名 (Digital Signature)

- 私钥签名公钥验
- 证明身份
- 验证传输，防止篡改
- 防止反悔 / 否认
- 签合同和协议
- 具有法律效力《中华人民共和国电子签名法》



数字签名

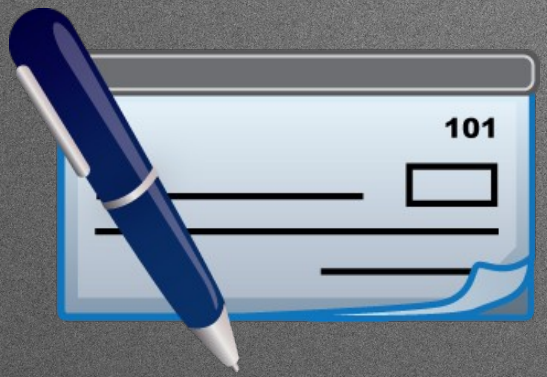

签名
数据
散列
函数
101100110101
散列值
用签名者的私钥
加密散列值
认证
111101101110
签名
附加到
数据
数字签名的数据
验证
数字签名的数据
111101101110
签名
数据
用签名者的公钥
解密散列值
散列
函数
?
101100110101
散列值
101100110101
散列值
若两者的散列值一致，则此数字签名为有效

实操环节

- 生成一个 GPG 密钥对
- 用自己的公钥加密一个文件
- 解密刚刚加密的文件
- 签名一个文件
- 验证此文件和签名
- 以文本形式导出 GPG 公钥
- 与 LDAP 服务器同步公钥（此步小心，无法删除服务器上已同步的公钥）
- https://keys.fedoraproject.org/

我可以信任你（的公钥）吗？

- 公钥的可信度 和 PKI (Public Key Infrastructure ，公钥基础架构)
- 能否防止反悔 / 否定
- 能否防止篡改
- 能否验证“此人持此钥”

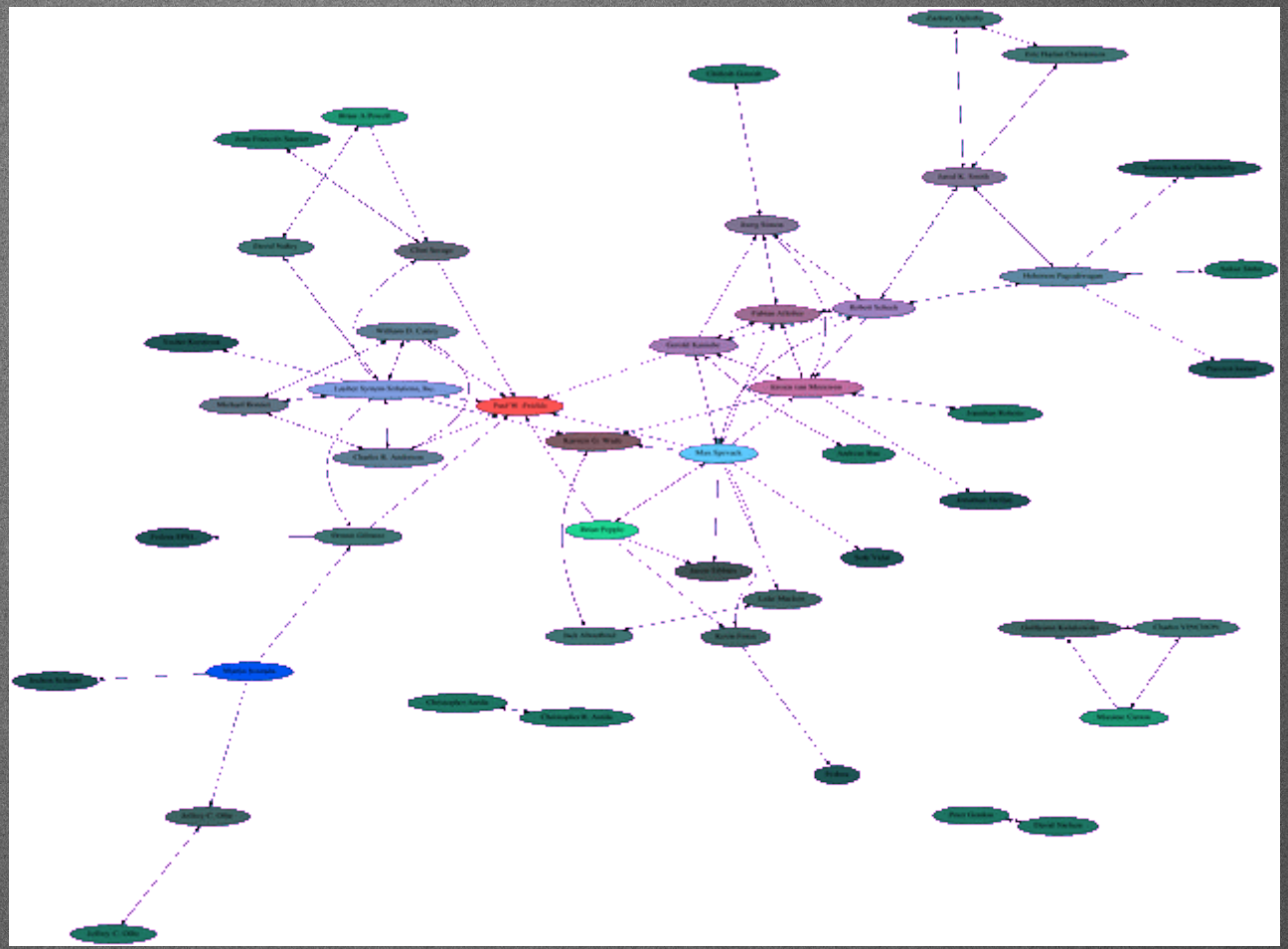


PKI 之 CA

- CA (Certificate Authority) 一个充分可信的第三方机构“有关部门”（政府机构或公司）
- 签发认证证书、签名用户证书、管理证书等
- 无法避免流氓和伪造根证书，无法防止中间人攻击（MITM）

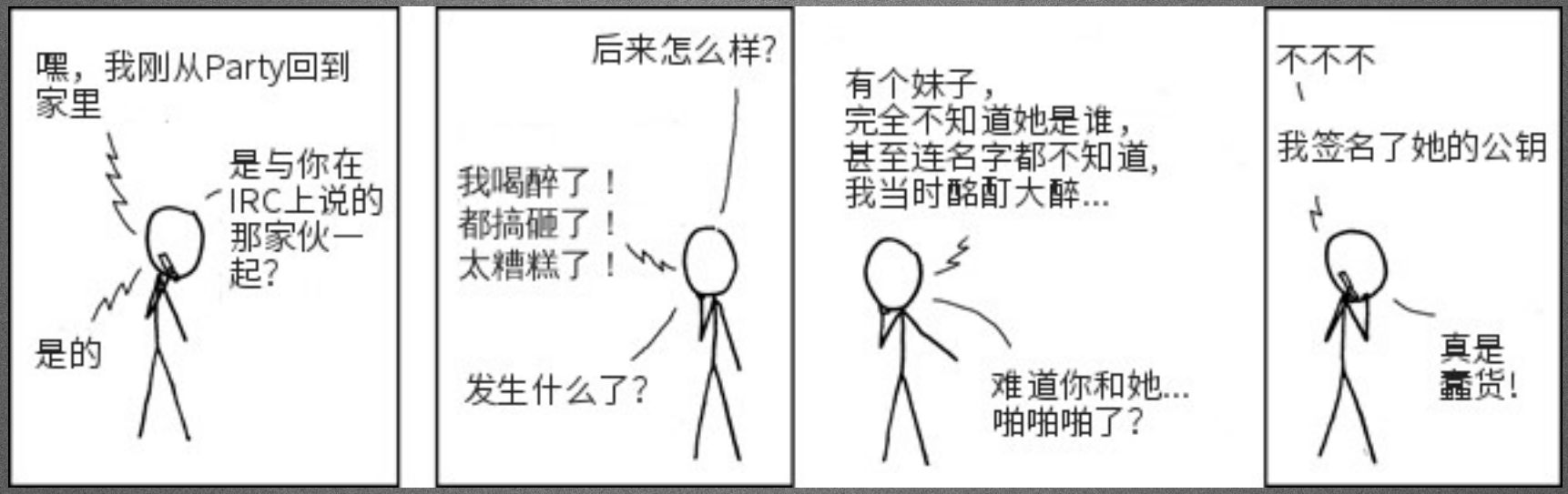
PKI 之 WoT

- WoT (Web of Truse) 信任网
- 通过平面的互相签名认证，构筑网状信任体系
- 去中心化
- 仍不完美……



Key Signing Party

- 信人品不信公钥，指纹身份核对好



翻译自 XKCD

Key Signing Party

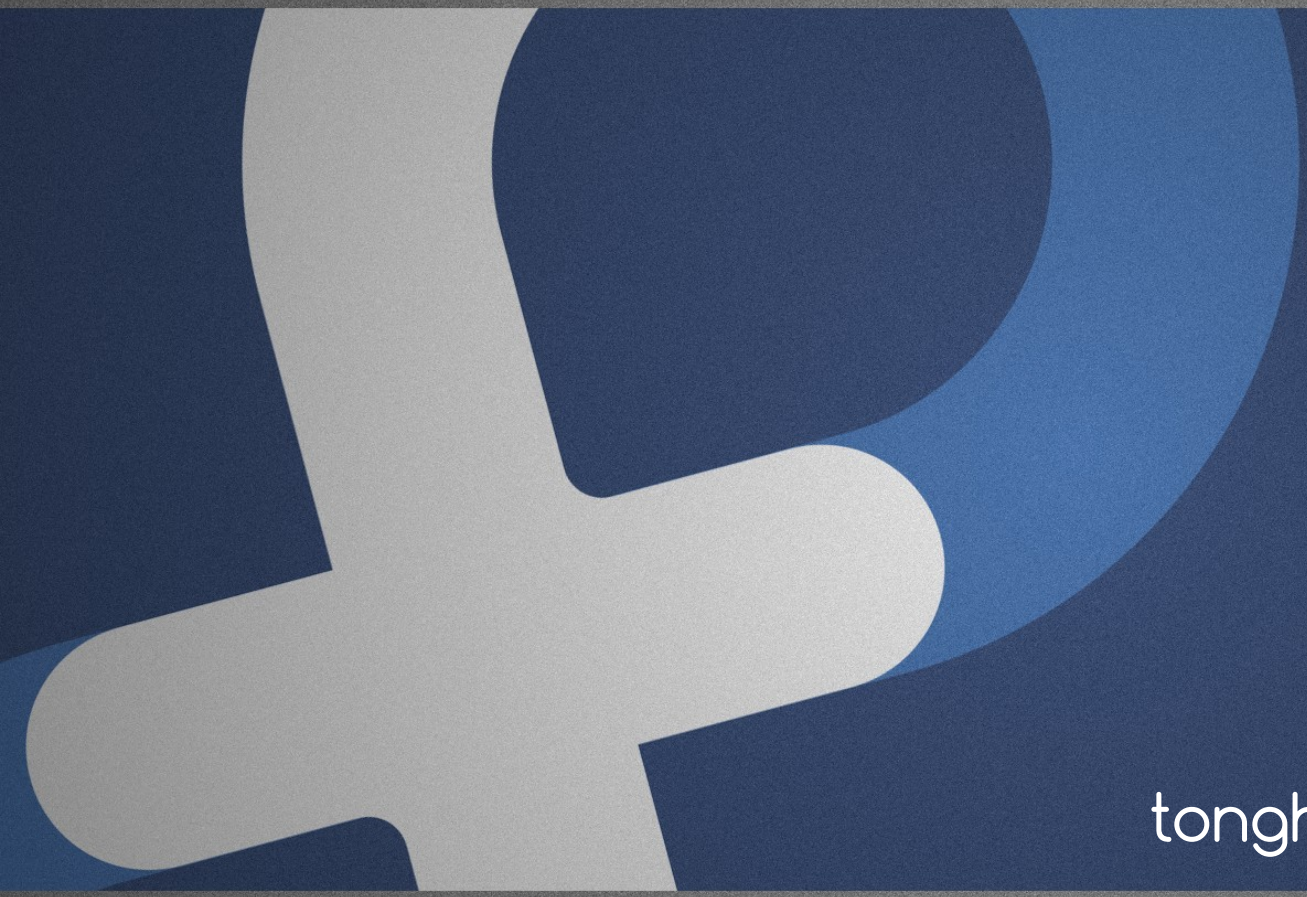
- 工具： gpg ， seahorse ， kgpg ， kleopatra, caff ， Keylookup
- 1. 检查公钥指纹
- 2. 检查 UID 与其身份证件匹配
  - 身份证、户口本、驾驶证、护照、港澳通行证、往来大陆通行证、居住证、暂住证
  - 军人证、老年优待证、残疾人优待证、军烈属证明
  - 学生证 (卡)、工作证 (卡)、职业认证、结婚证
  - 工牌、名片、其他身份证件
- 3. 导入其公钥，并签名 *（顺便留下美女的联系方式）*

实操环节

- 向 LDAP 服务器同步自己的公钥
- 请执行 `gpg --fingerprint KEYID`

  将输出结果原封不动的贴到：

  https://blug.hackpad.com/F21-GPG-Key-Signing-Party
- 从 LDAP 服务器下载别人的公钥
- 为别人的公钥签名
- 将签名以后的公钥同步到 LDAP 服务器



Questions?

Tong Hui - A6D42018:
tonghuix@fedoraproject.org