Introduction to GPG

Christopher Hopkins

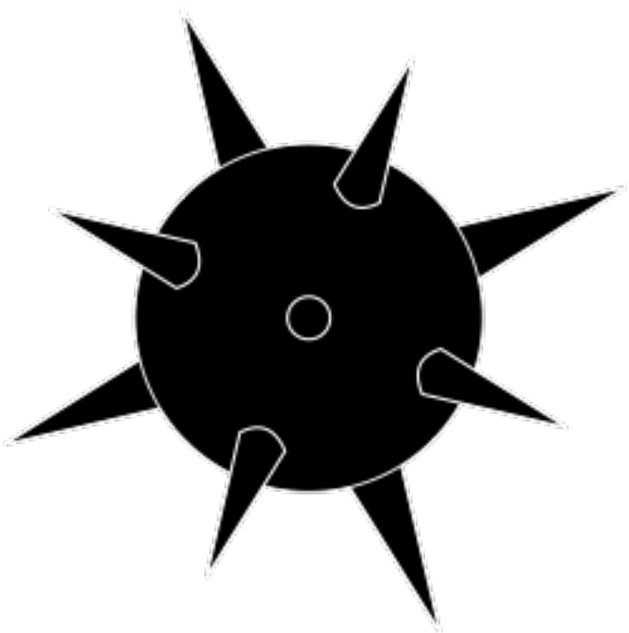
Why use GPG?

Confidentiality

Integrity

Authenticity

Security Limitations



Installation

```cpp
#include <iostream>

using namespace std;

void main()
{
    float var, total = 0;

    for(int i=1;i<=3;i++)
    {
        cout << "Enter number:" << endl;
        cin >> var;
        total = total + var;
    }

    total = total/3.0;
    cout << "Avg: " << total << endl;
    system("pause");
}
```

Source

Package Management

Download

Front End Tools

Generating Keys

Kerckhoffs' Principle

A crypto-system should be secure even if everything about the system, except the key, is public knowledge.

Generating Keys

DSA VS 

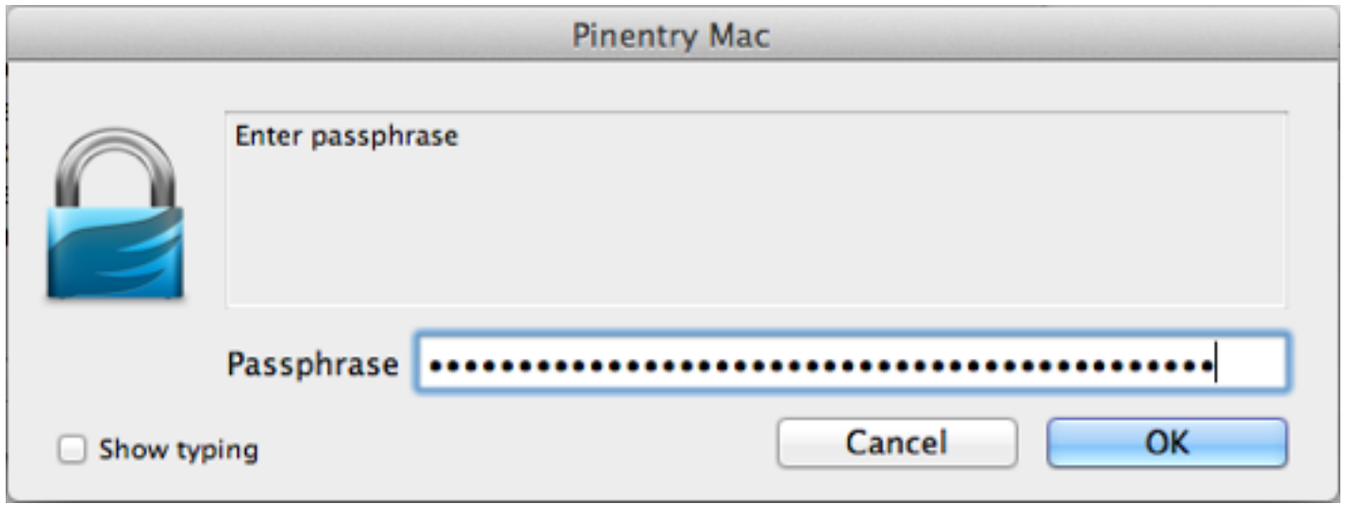
Cipher

Generating Keys

Security (Bits)	Symmetric encryption algorithm	Minimum Size (Bits) of Public Keys		
		DSA/DH	RSA	ECC
80	Skipjack	1024	1024	160
112	3DES	2048	2048	224
128	AES-128	3072	3072	256
192	AES-192	7680	7680	384
256	AES-256	15360	15360	512

Key Size

Generating Keys



Passphrase

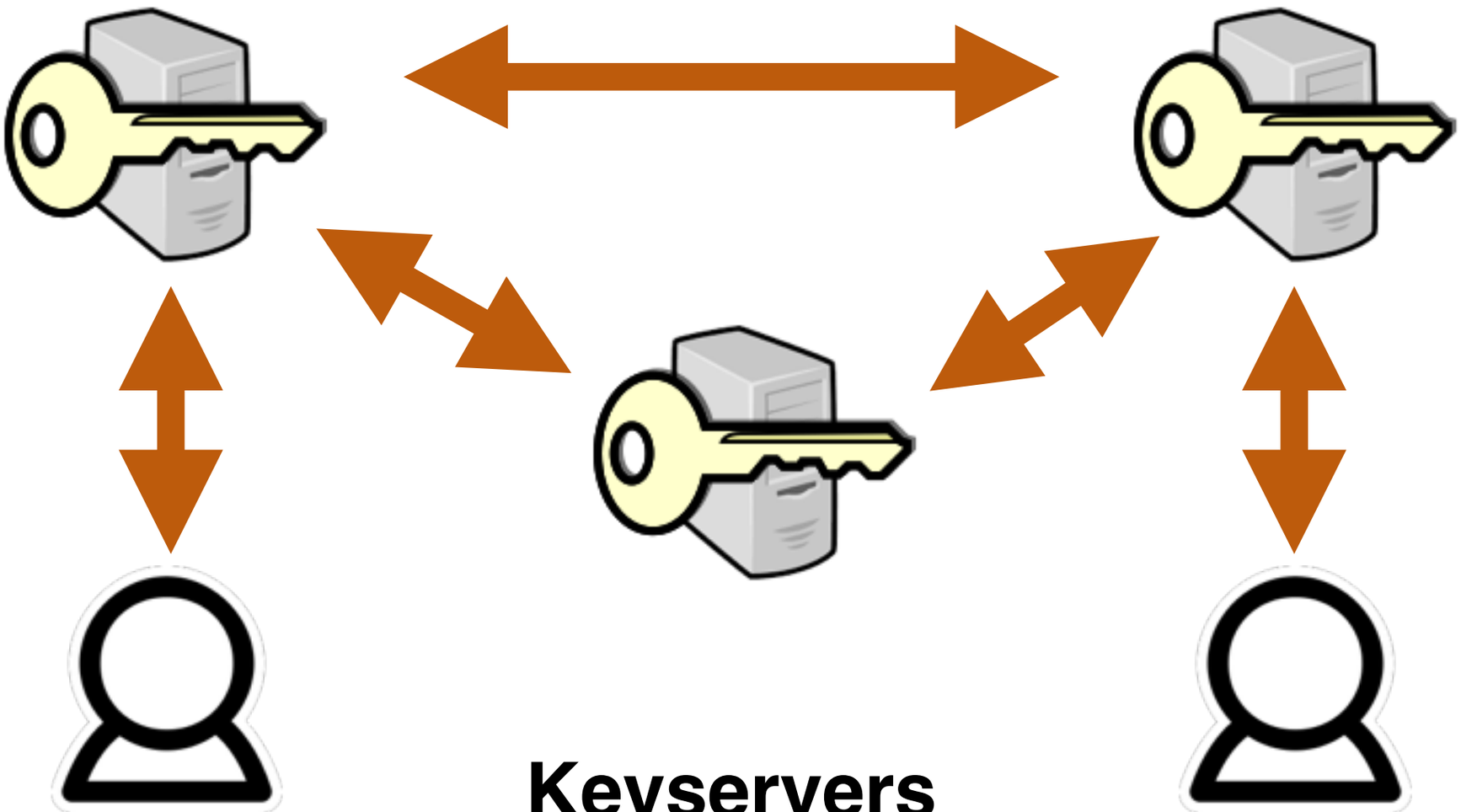
Sharing Keys

Sharing Keys

Export

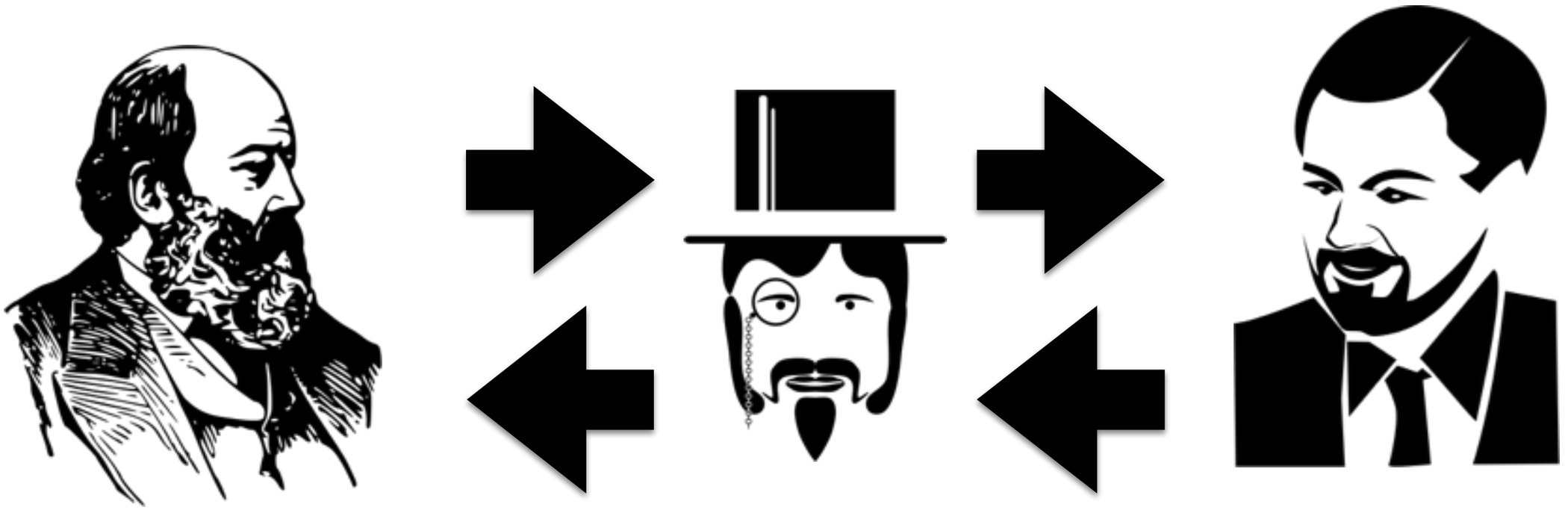
Import

Sharing Keys



Trust & Authenticity

Man in the Middle

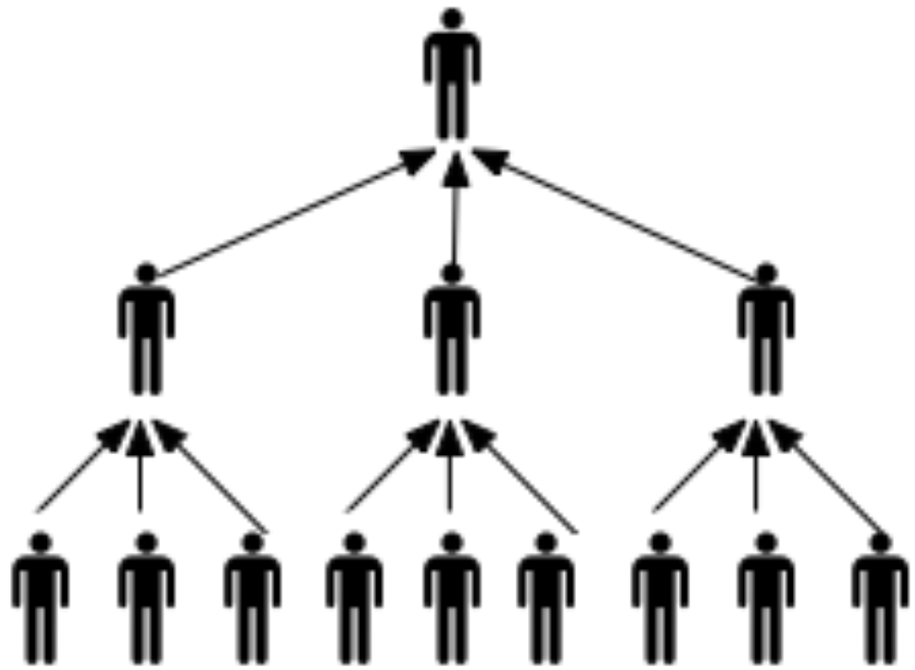


Observe and/or Manipulate Content

Trust Models

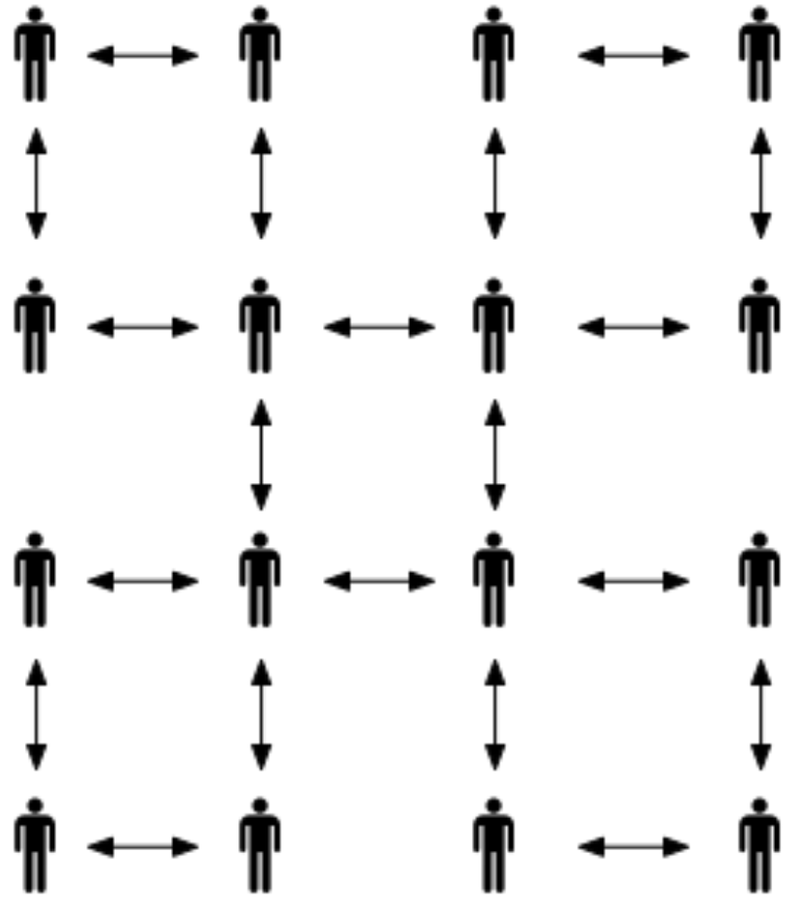
Direct

Trust Models



Hierarchical

Trust Models



Web of Trust

Trusting Keys

Key Signing Parties

Trusting Keys

-----BEGIN PGP PUBLIC KEY BLOCK-----

mQINBFN5atQBEACxFq40n+qU9BawPtztyYq4q5fYhlDhgs4Lm0l4Ezs5Na+rtSz4
eNpHMasAKEOdlwlbyLeLVSryG9ayqe0RUT8VLOMM1oucZjfR3LWZon7jrKo4etBL
3IVlyTzbDYK/8n4YoRMEykMWXKm5KoyNe3UAWbqx1V3W40GAes012grSdXwbXcru
kHRTy8bEZCJHLLeWuDD0kBQG/gJUcp5G/WLkffwW9pvwdgLj6EG/294OVGkv8Vfq
pX3qOiQINUqkhO4JiDkH+j/qPS7EjsFQcqRNsYqwwkYBizq+kA7EWVgxtkdVNoVD
N0FCneGy3oEbe58sWgd3uarJweJOqfIUNaeC7AcLBEGbwEU1vDYpvUJd9xQU+RkF
2a6mLnXEJyHxFN/Izljm6jNsJyyAZcAQSpXvSw2pDr+VjEOBC9Ptyh9rWGJOXDP7
sR7DAUVqLo/riKLnSNJ/CX0PUzs0EINpvc2Q5iJp8qOT0P7mcIO9ItEbrO+rn1u6
ffmXQ1SlRQ/7Tpc9ZxXXHgFYJY35GefP5R0VjzfZRBFOtapHgDUmDOLEn1lD7Av4
jlnf5uFxr+YAX0IVOjJqNYt9apR5vqP0UAmp8Ofu9tbIesu9/iWggTbTZp3LfW+X
T9cKYZxJidIsz24G1T1LsIfn+Dk6BUJnJSEq+eADh5+ZK+Vz51xxtlpgFwARAQAB
tDFDaHJpc3RvcGhlciBIb3BraW5zIDxjZGhvcEBkaXNxdWlldGluZ2NhbmRvci5u
ZXQ+iQI9BBMBCgAnBQJTeWrUAhsDBQkHhh+ABQsJCAcDBRUKCQgLBRYCAwEAAh4B
AheAAAoJELxkuZDIZw2NXIMP/0grqTqsm745rKARBDMo5F98lvgudPhrLvSQpECE
kEuMKyB2dR77tj82Zo9Mde01MCCUFNCUxbLeiF7kDp+WhRarMrB5UQF5UV0mi/Qo
FStlAKCESXWQCpLqPcVaGdVSnGTsyWa867BIBmKqnJSoepzDKroVqJbs6UtNPLLu
Kjrv9QppmvG1K59gOFE9vRogTQwjy16K5WN4A5egA71njkIIhUvdSqqgs0NTPqHG
6RwfddgwXtbl48kz++bR9zW4rWZri2wM2Me0+ftTP5Ji5Olos8mvIe0bOKSQh/gy
7nYAWg+BEN/U9fQL+id/ZcwKpOfiNdduA71U6DB5w7CapQps6QrvvvIbnD+9QDX5
QmO/wapnibBsolSrpH7bkGw/jWkmw4nrxut204pCKw5OrkPc6F0RnMansHod7Be
Ds2T+7N2+F0CvxggQXj8Trt2Q+bc6rOg6lZ3b4K445Fsxa+rwbHf4VCOtmbeEfgF
SI6esUbUVhS5fPX7KOenp28Z8bf4ejTDiUCIgqLcpHSEG0od7QCwhoWupT68g/91
t7kIpEa9f7gctZjs5YScoxuHieuFsg2eznm8CCGw/HkIfuAYsYyLnragI2TUCbSB
2F2TvY6/XZ1gS0RKHy9ENPLeu/Ax0KqCAaL7nJ9ee65ZEO8hvqjB3IHTCmeSsXAA
wi

DD20 0640
7227 1479
17AF 4D8F
BC64 B990
C867 0D8D

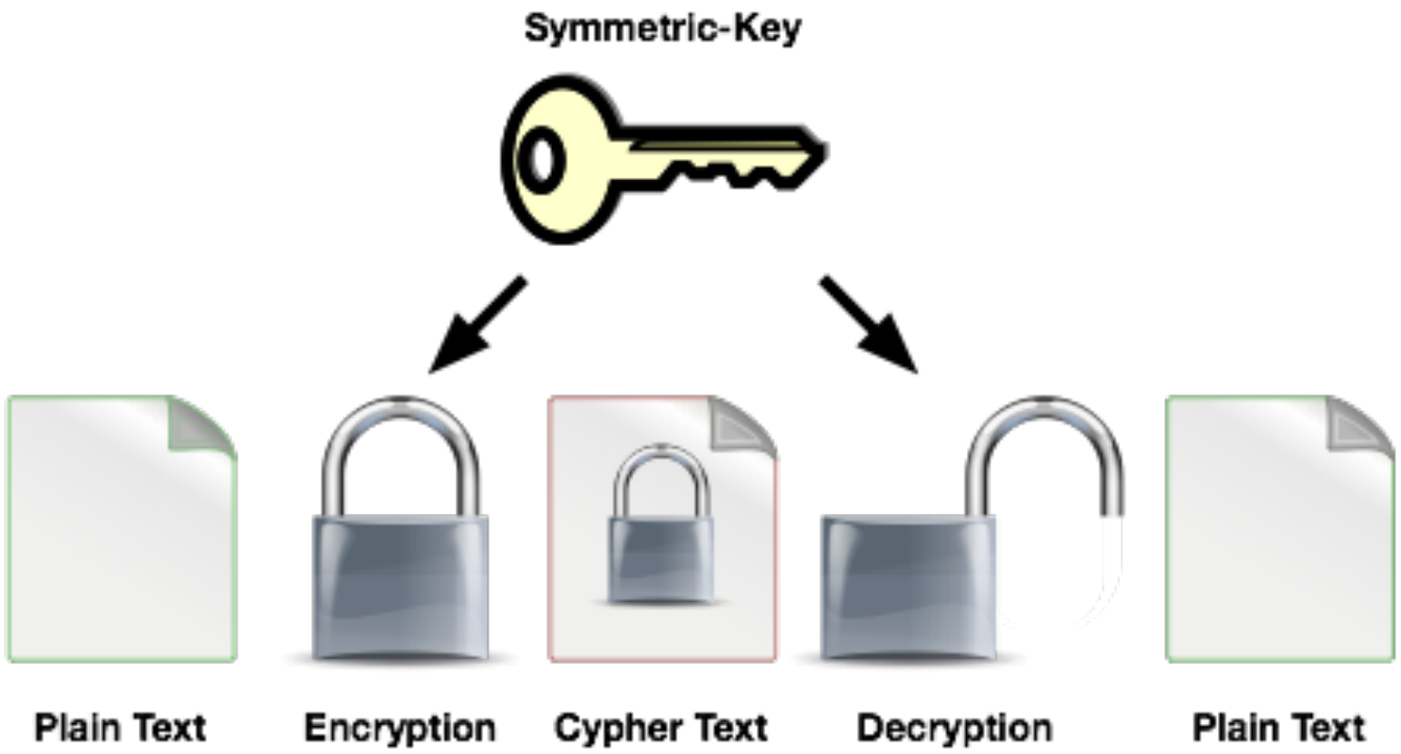
Fingerprints and Key IDs

Trusting Keys

Keybase.io

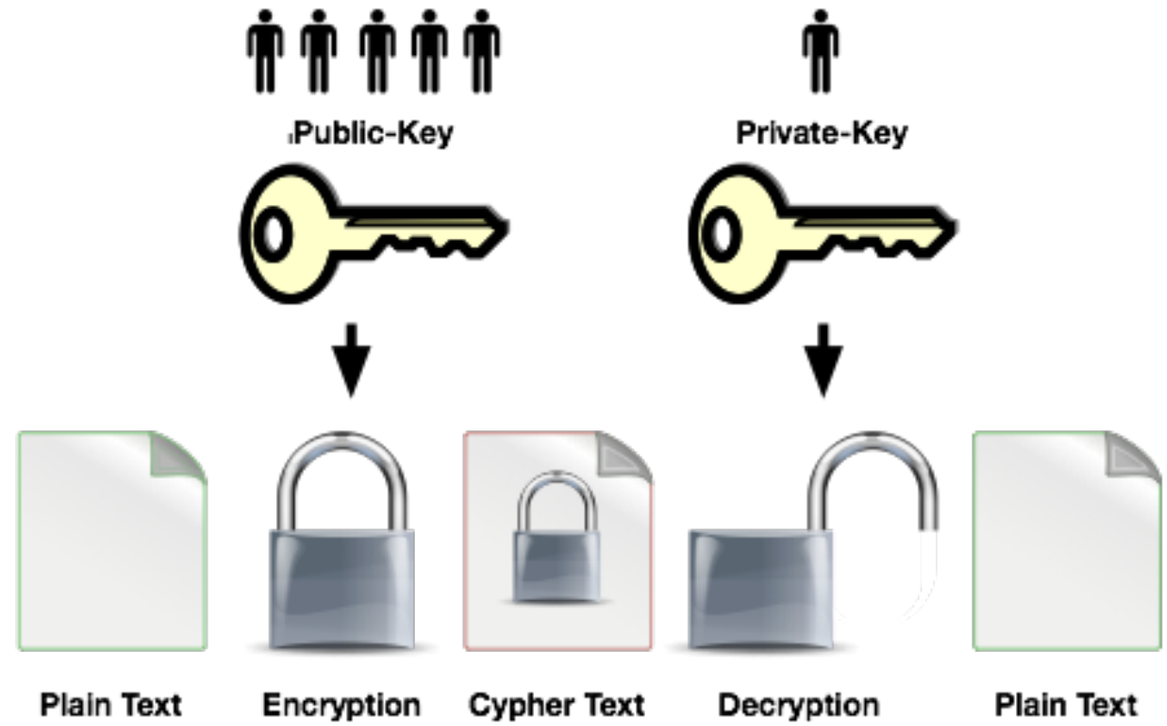
Using Keys

Using Keys



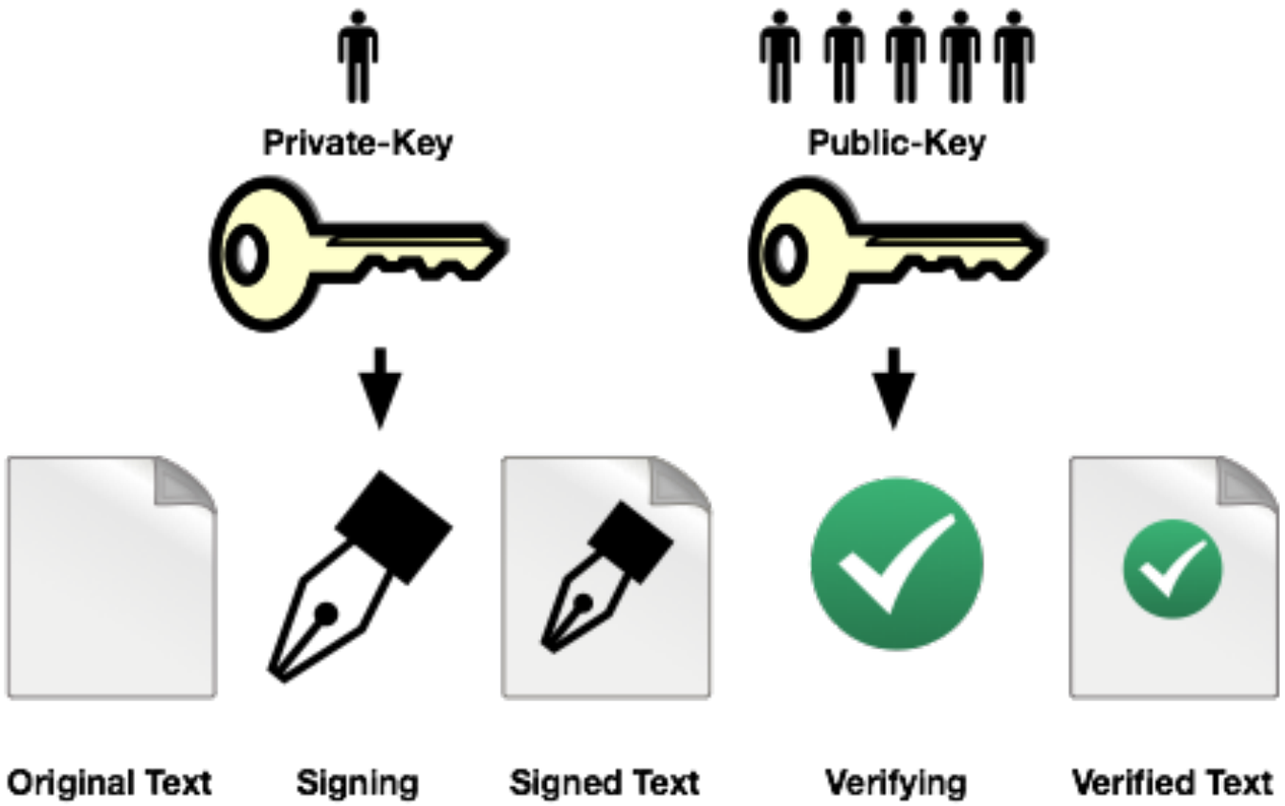
Symmetric Encryption

Using Keys



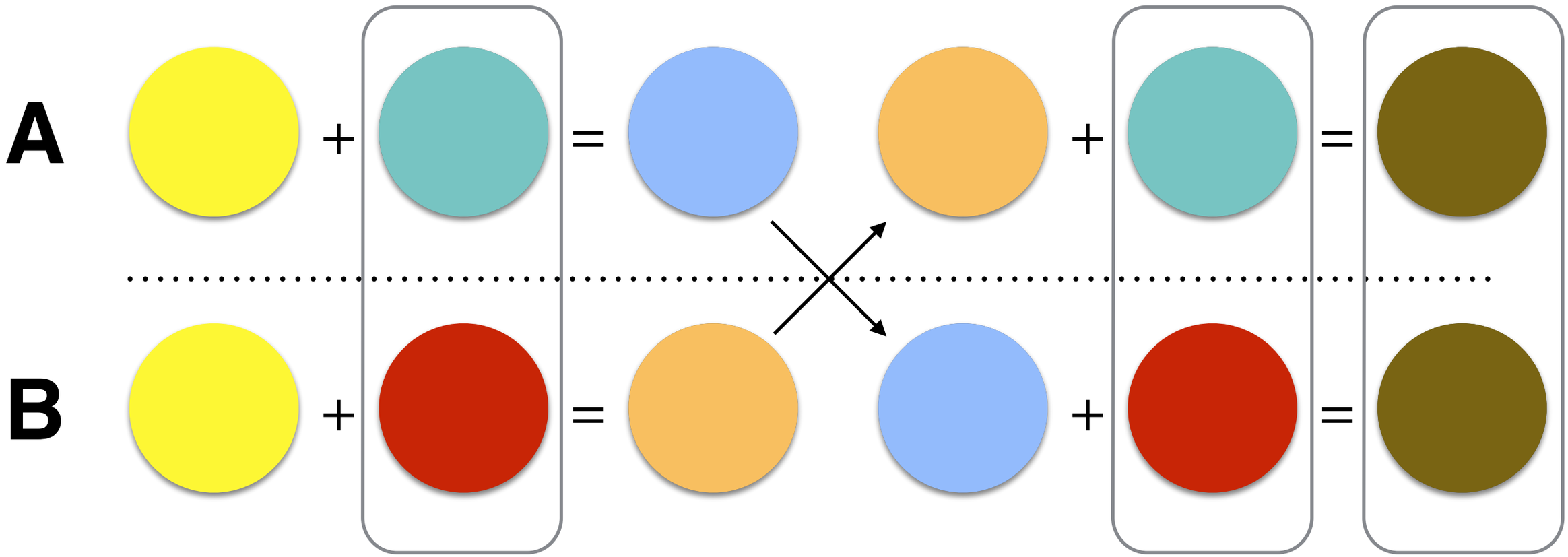
Public Key Encryption

Using Keys



Digital Signatures

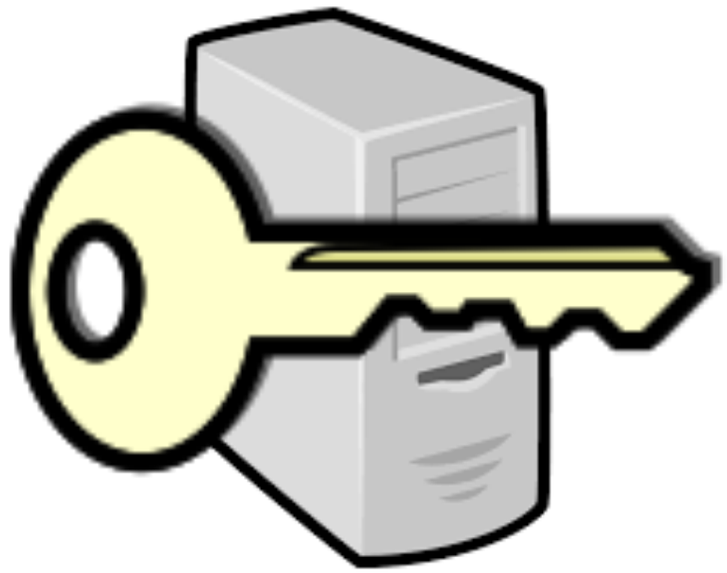
Public Key Encryption



Diffie-Hellman Key Exchange

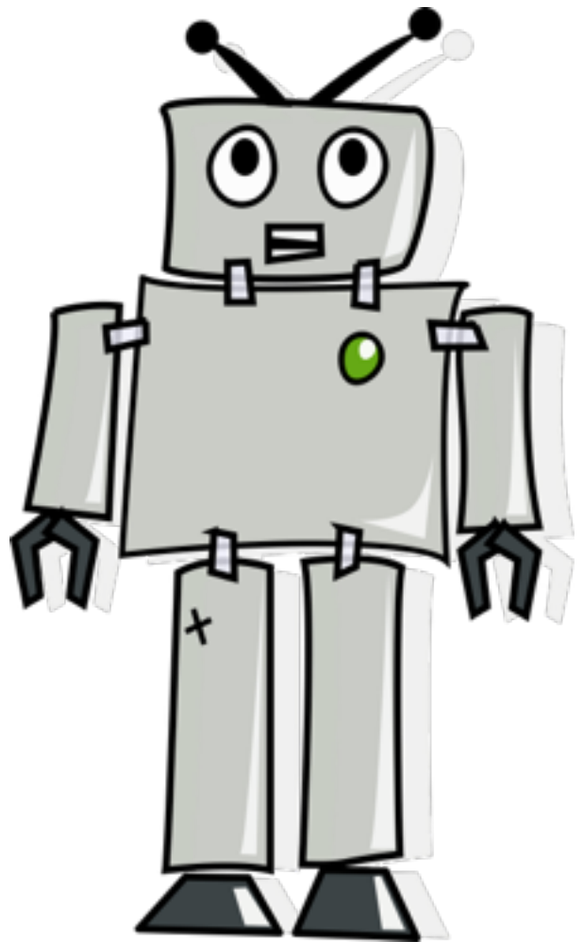
Practical Exercise

Training Keyserver



keyserver.cryptopartyutah.org

The friendly OpenPGP email robot



adele-en@gnupp.de

Challenge

Invitations

Further Study

- **Homepage: https://www.gnupg.org/**
- **Keyservers: http://pgp.mit.edu**
- **PGP & GPG: Email for the Practical Paranoid (ISBN: 978-1593270711)**
- **Applied Cryptography (ISBN: 978-0471117094)**