Introduction to GPG

Christopher Hopkins

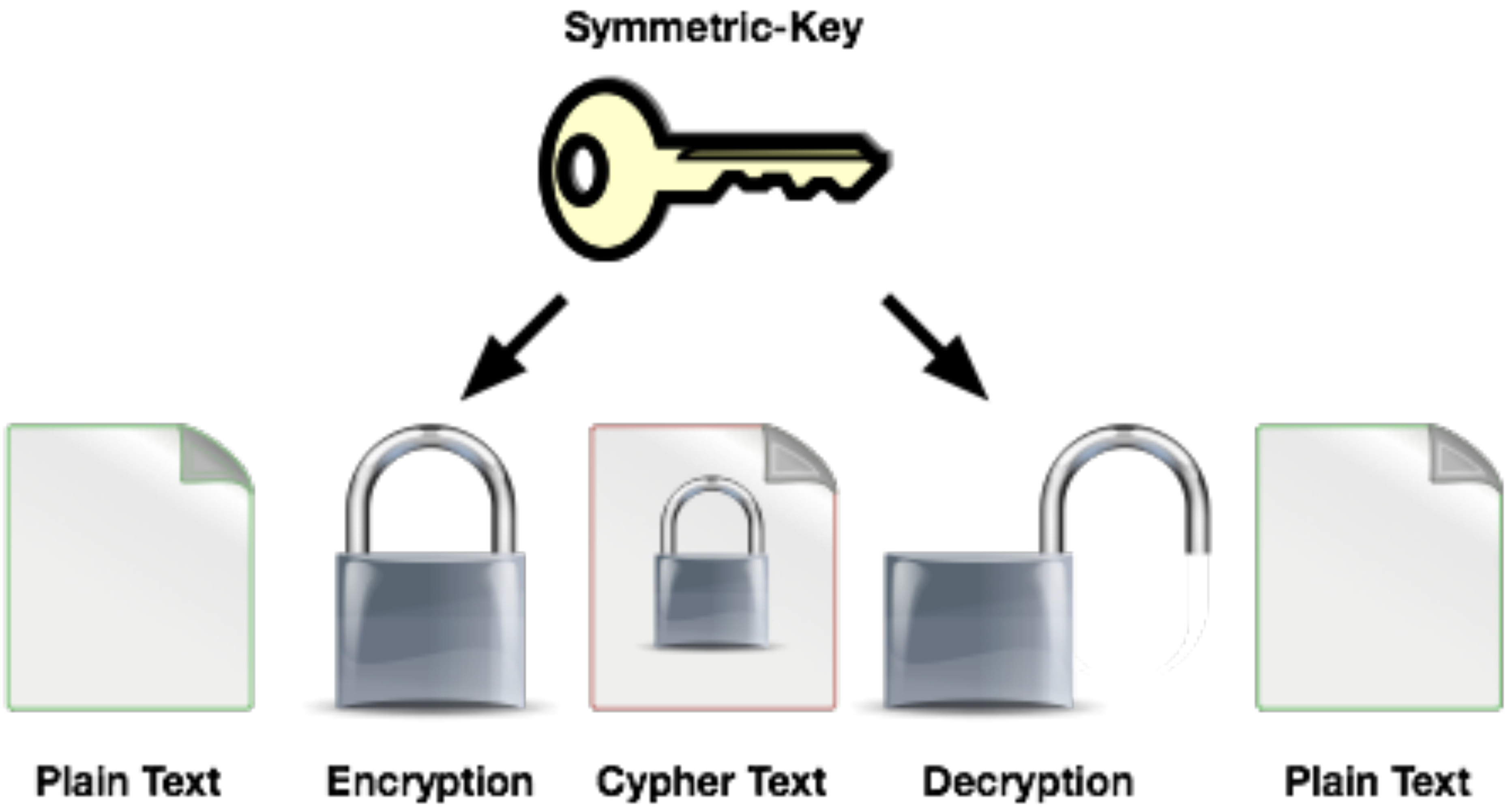
Why use GPG?

Confidentiality

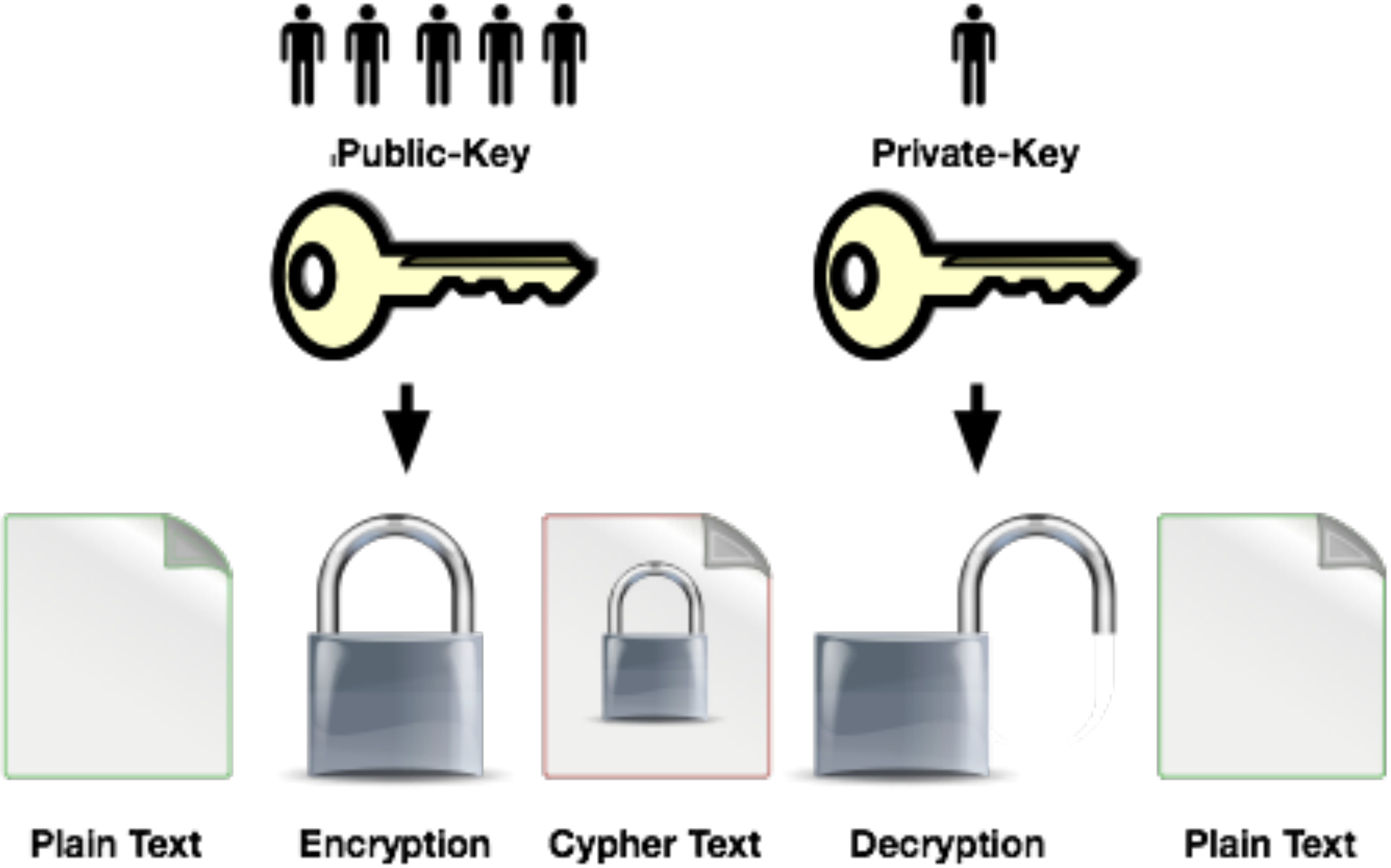
Integrity

Authenticity

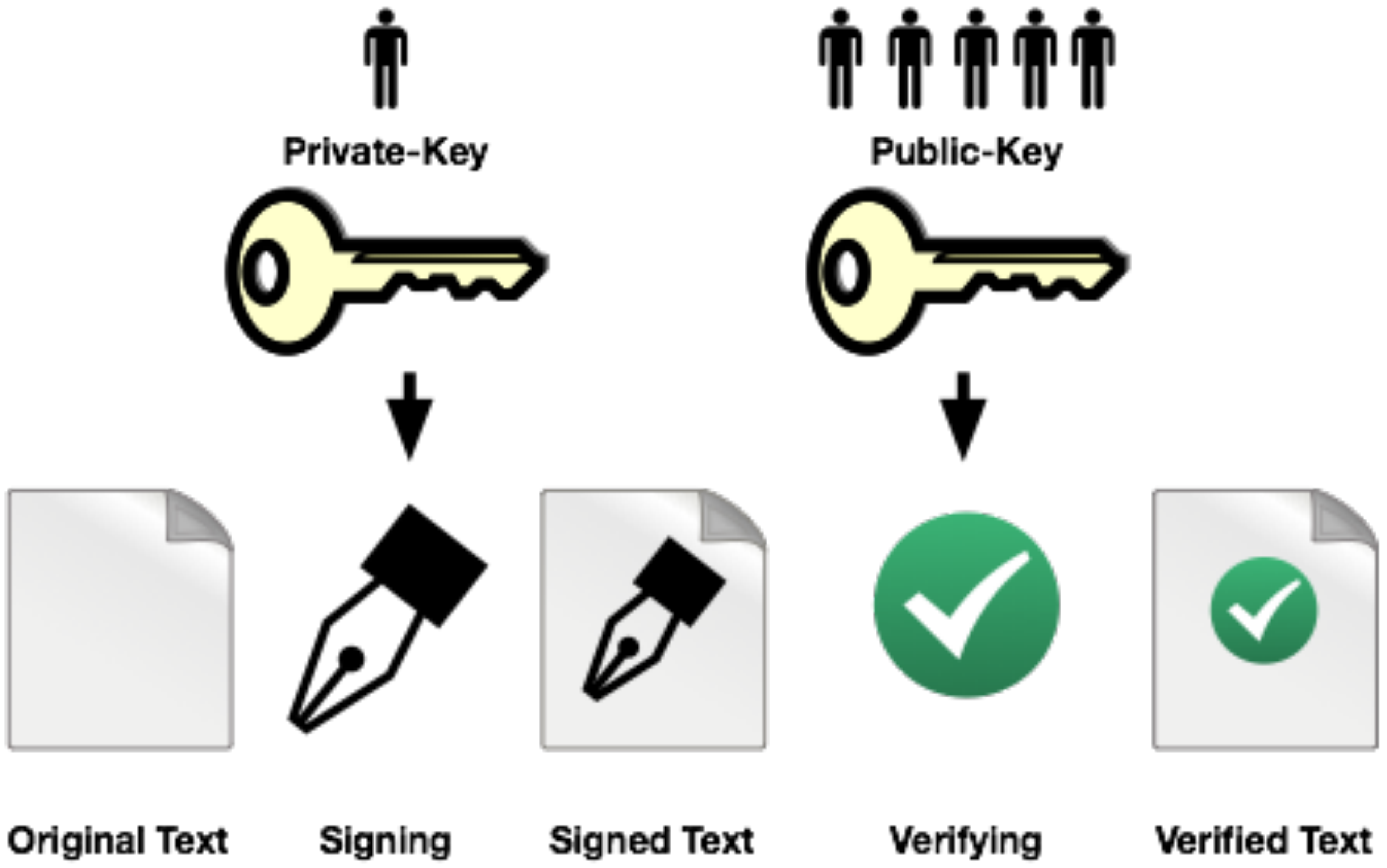
Symmetrical Encryption



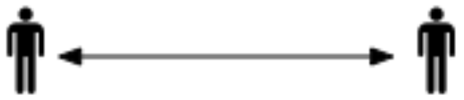
Public Key Encryption



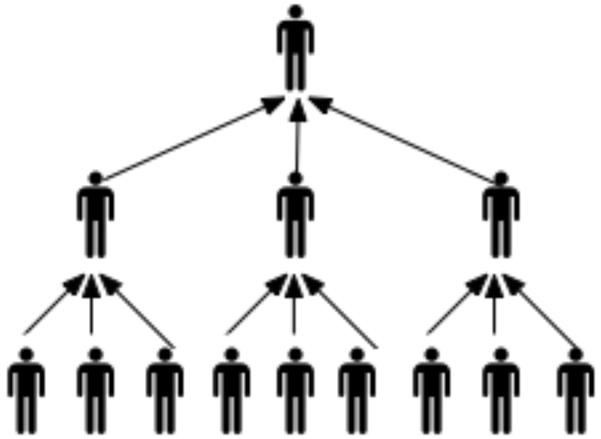
Digital Signatures



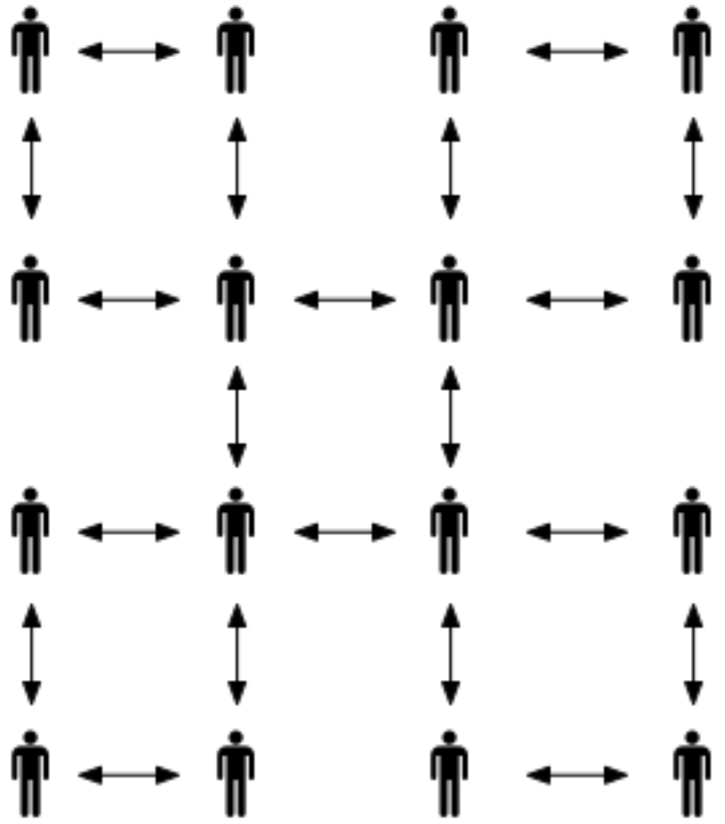
Trust Models



Direct

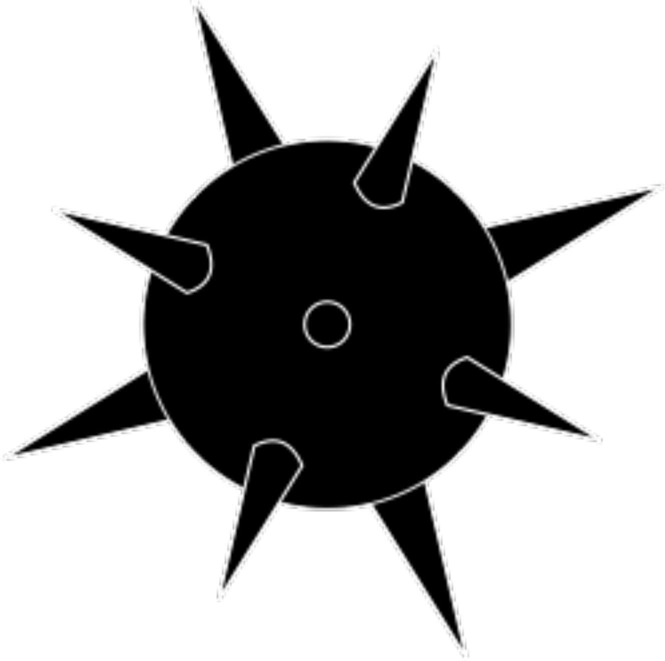


Hierarchical

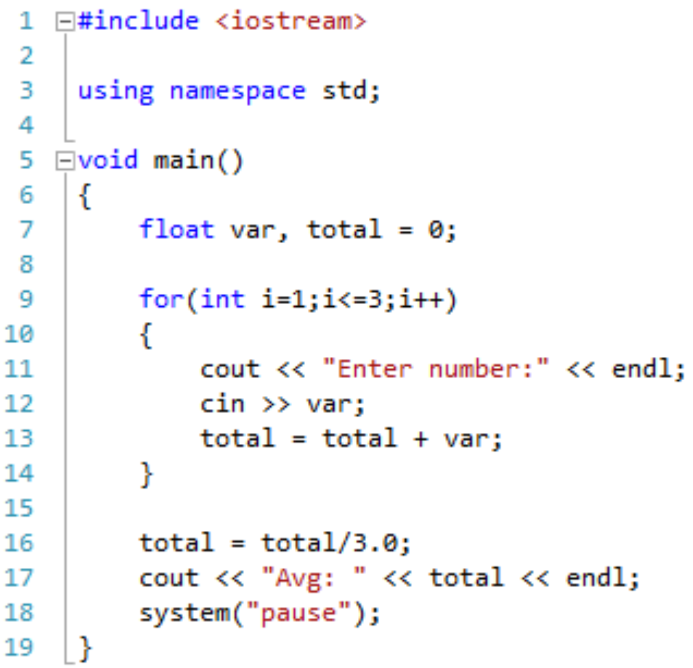


Web of Trust

Security Limitations



Installation



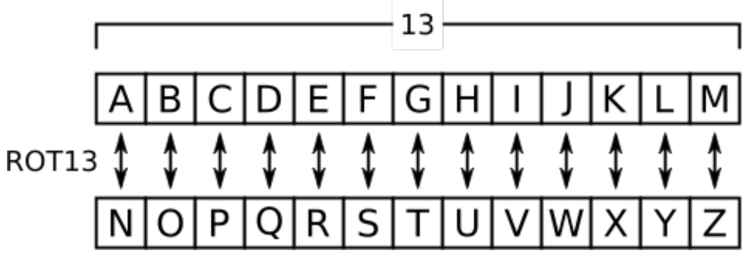
```
#include <iostream>

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

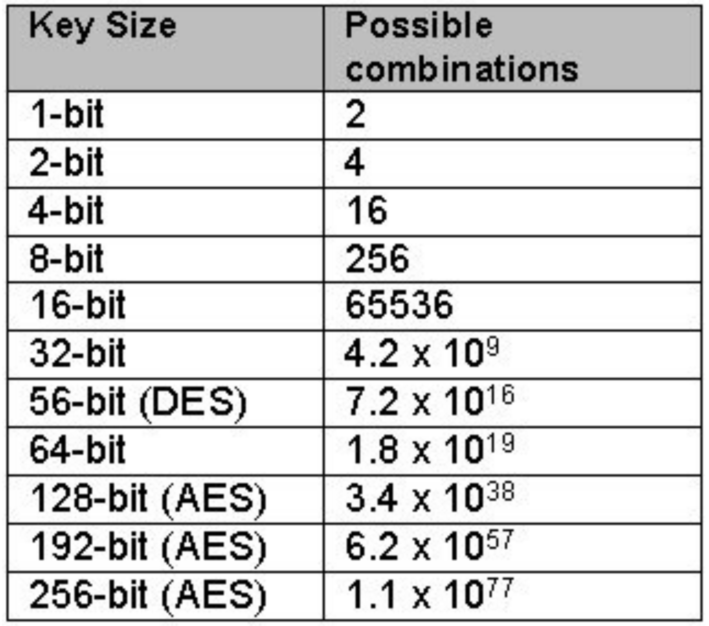
Package Management

Download

Key Creation

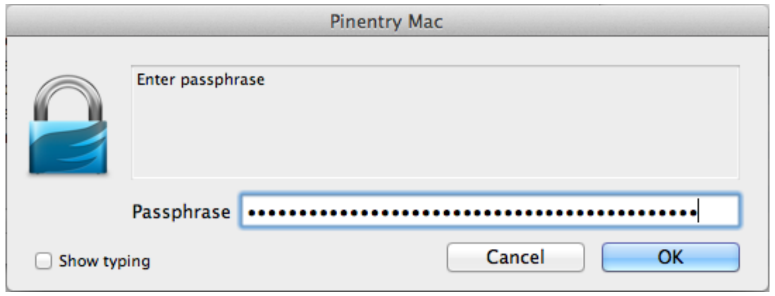


Cipher



Key Size	Possible combinations
1-bit	2
2-bit	4
4-bit	16
8-bit	256
16-bit	65536
32-bit	4.2 x 10^{9}
56-bit (DES)	7.2 x 10^{16}
64-bit	1.8 x 10^{19}
128-bit (AES)	3.4 x 10^{38}
192-bit (AES)	6.2 x 10^{57}
256-bit (AES)	1.1 x 10^{77}

Key Size



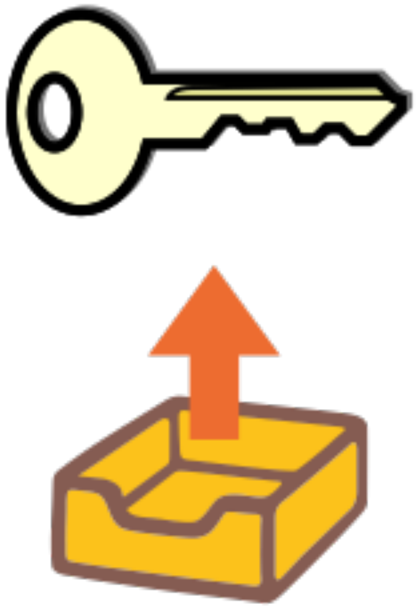
Pinentry Mac

Enter passphrase

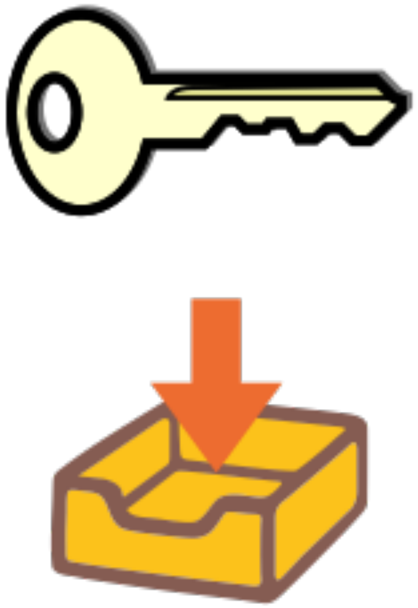
Passphrase ••

Passphrase

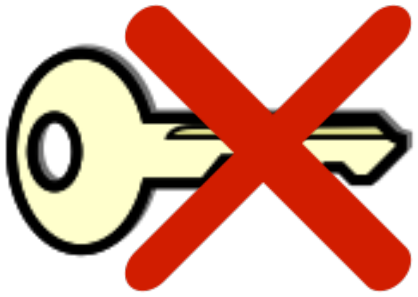
Using Keys



Exporting



Importing



Revoking

Keyring Administration

List

Fingerprint

Edit

Delete

Building Your Web of Trust

Key Signing Parties

Front End Tools

Further Study

- Homepage: https://www.gnupg.org/
- Keyservers: http://pgp.mit.edu
- Applied Cryptography (ISBN: 978-0471117094)