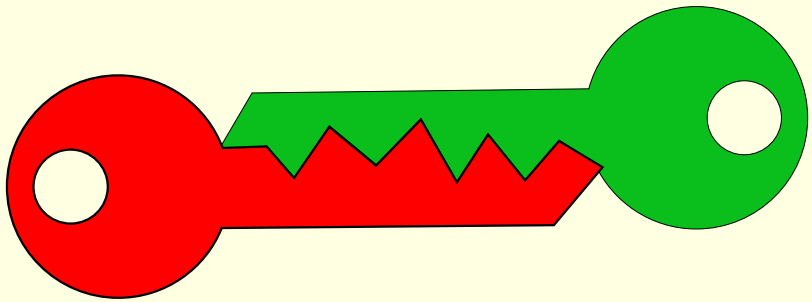


# Digital Signatures for Newbies

- Digital Signatures are a clever approach of using complex mathematics in real life work
- Let‘s see how it works…

# Setup Step 1 : Genererate your own key

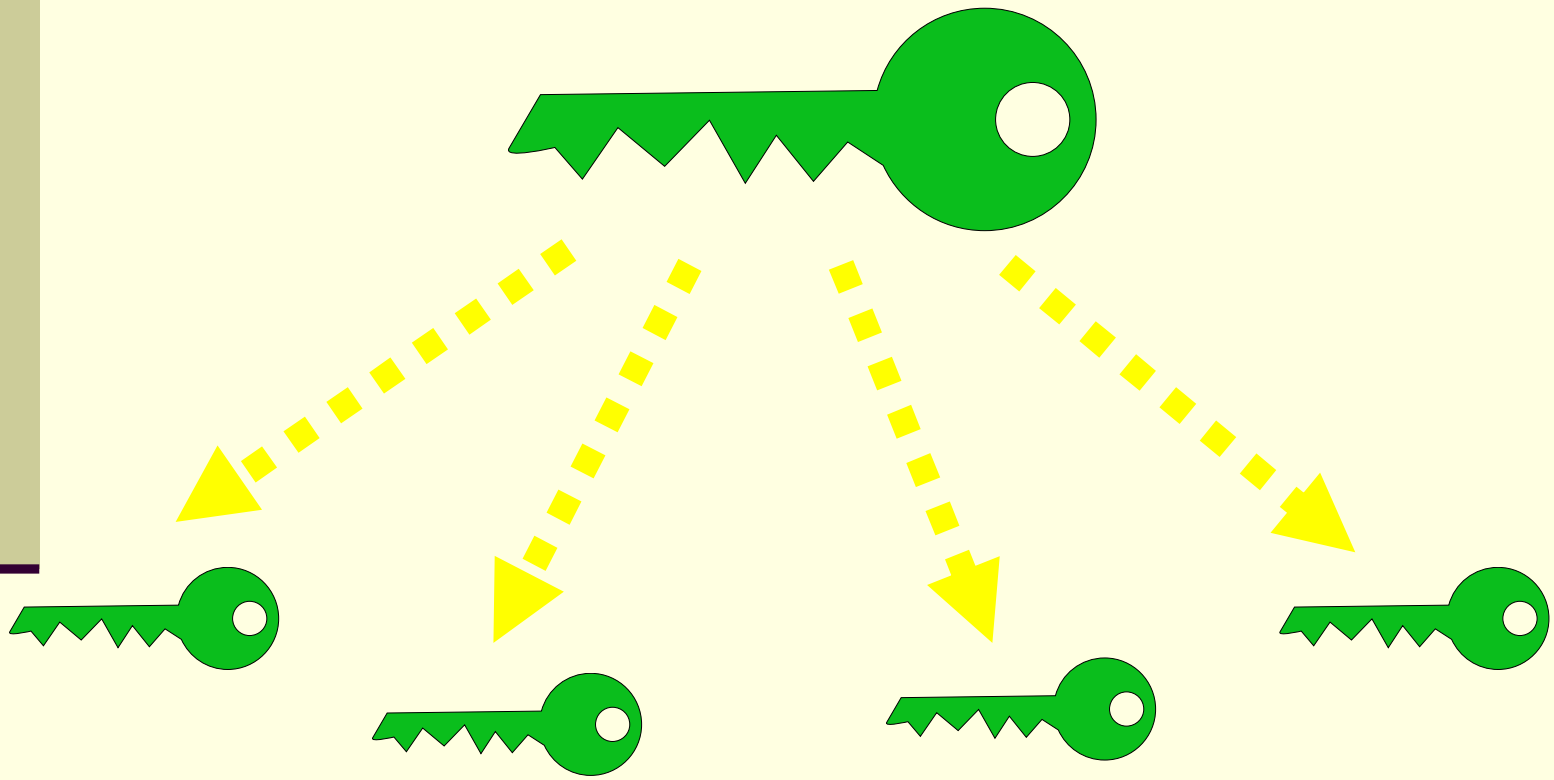
- First you create a Key pair containing a Public Key and a Secret Key.




- The access to your Secret Key is protected by a passphrase

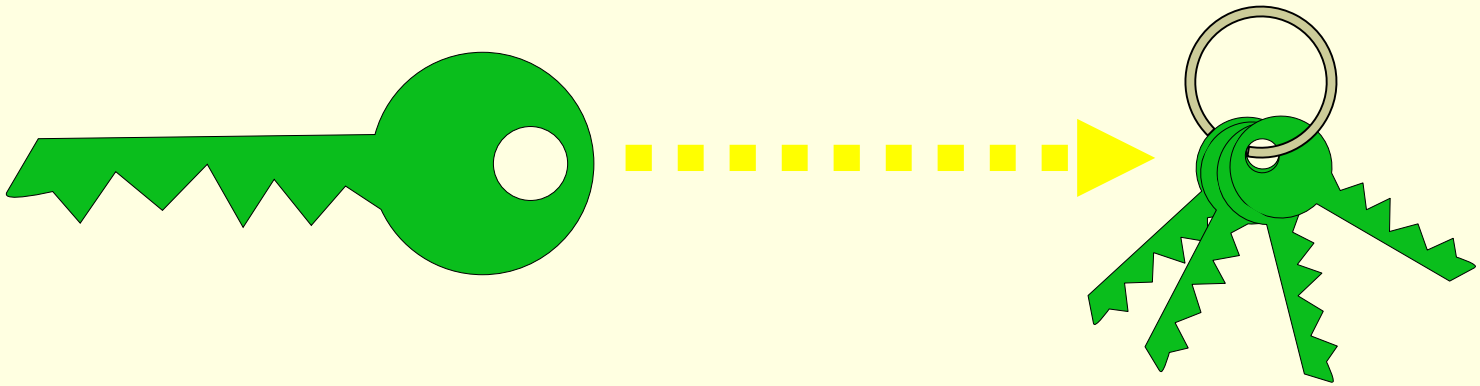
# Setup Step 2 : Distribute your Public Key

- Distribute your Public Key to other users



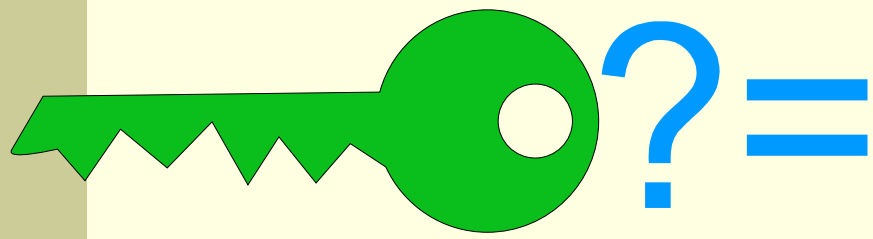
# Maintenance: Store received keys

- The users add received Public Keys to their Public Key Ring



# Maintenance: Verify received Keys

- The other users verify your Public Key with your Key Certificate

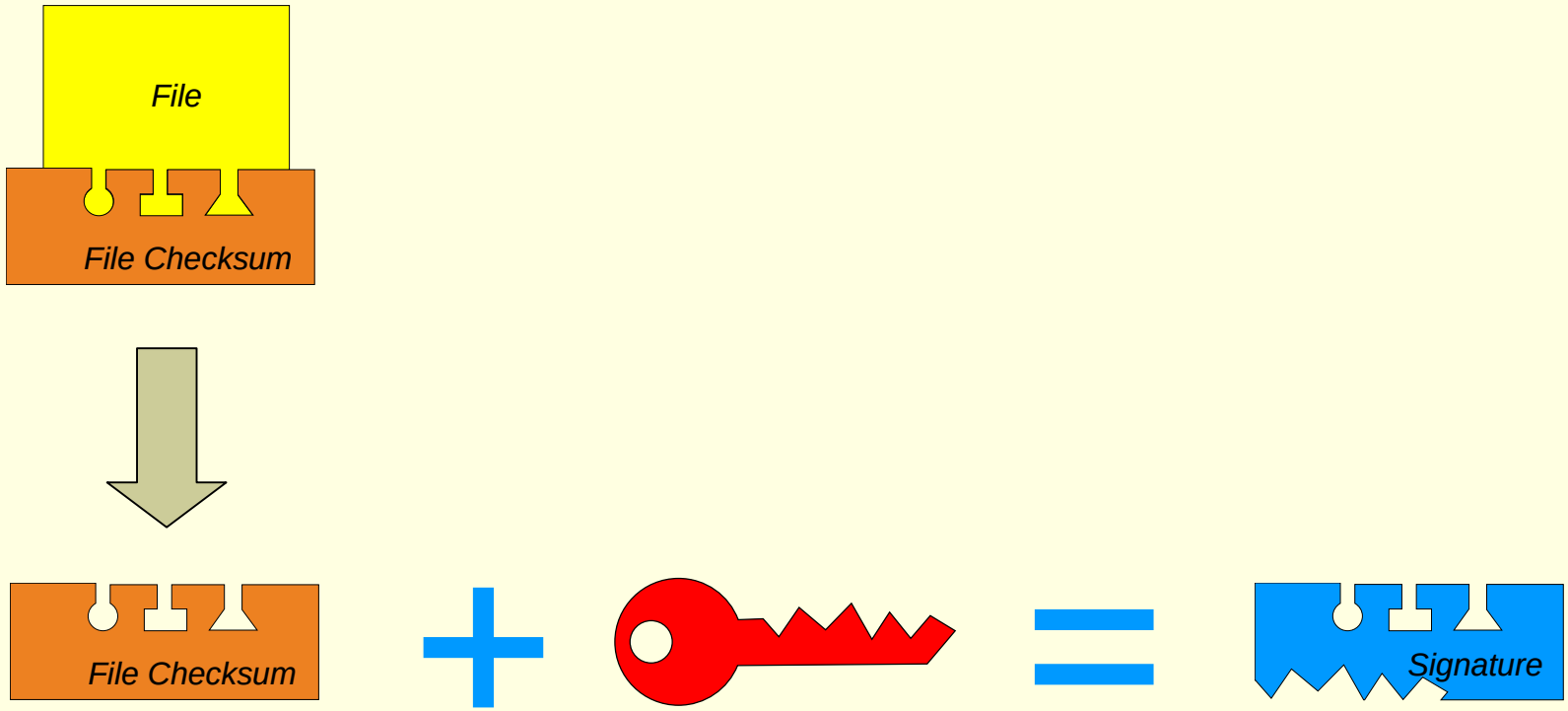


```
pub 1024D/6702661F 2003-05-04
Key fingerprint = A2E8 8737 3654 D5E2 031F 02B5 BCDE B096 6702 661F
uid Steffen Köehler (SY CS1 E)
uid Steffen Koehler
sub 1024g/FA8259DC 2003-05-04
```

- If it matches, they sign your key as valid

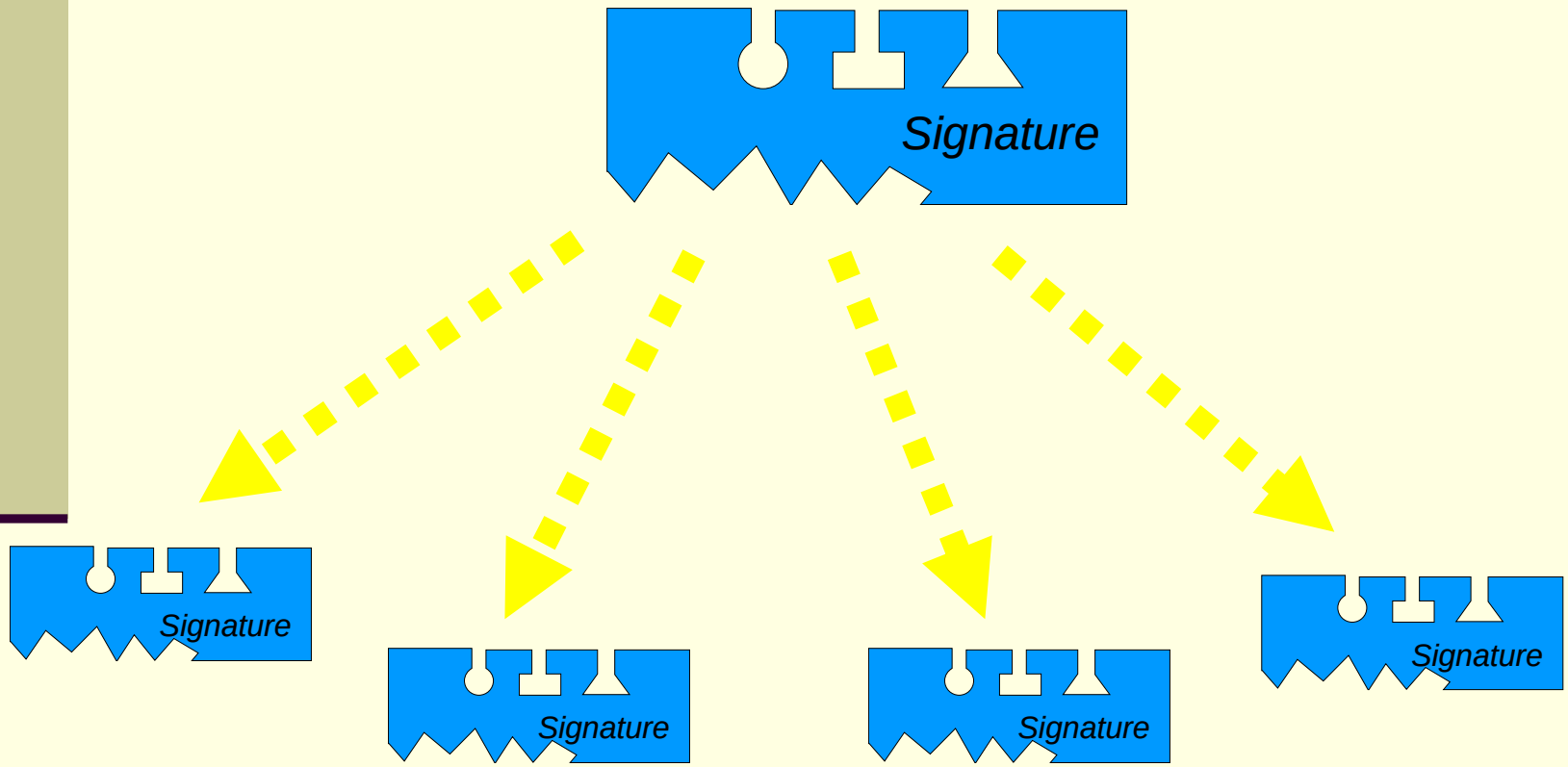
# Creating a Digital Signature

- To sign a file, you create a Signature out of your Secret Key and the file checksum



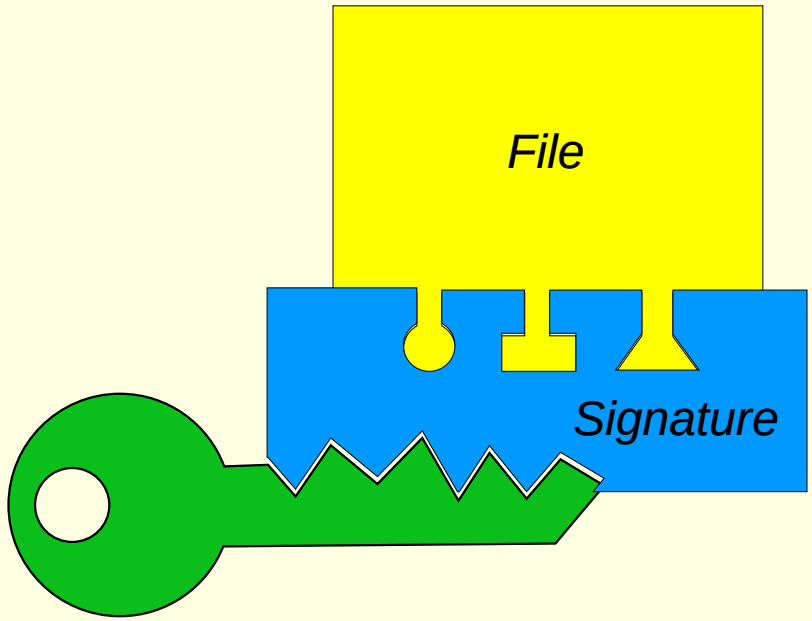
# Distributing a Digital Signature

- Distribute the Signature to whoever needs it



# Verifying a Digital Signature

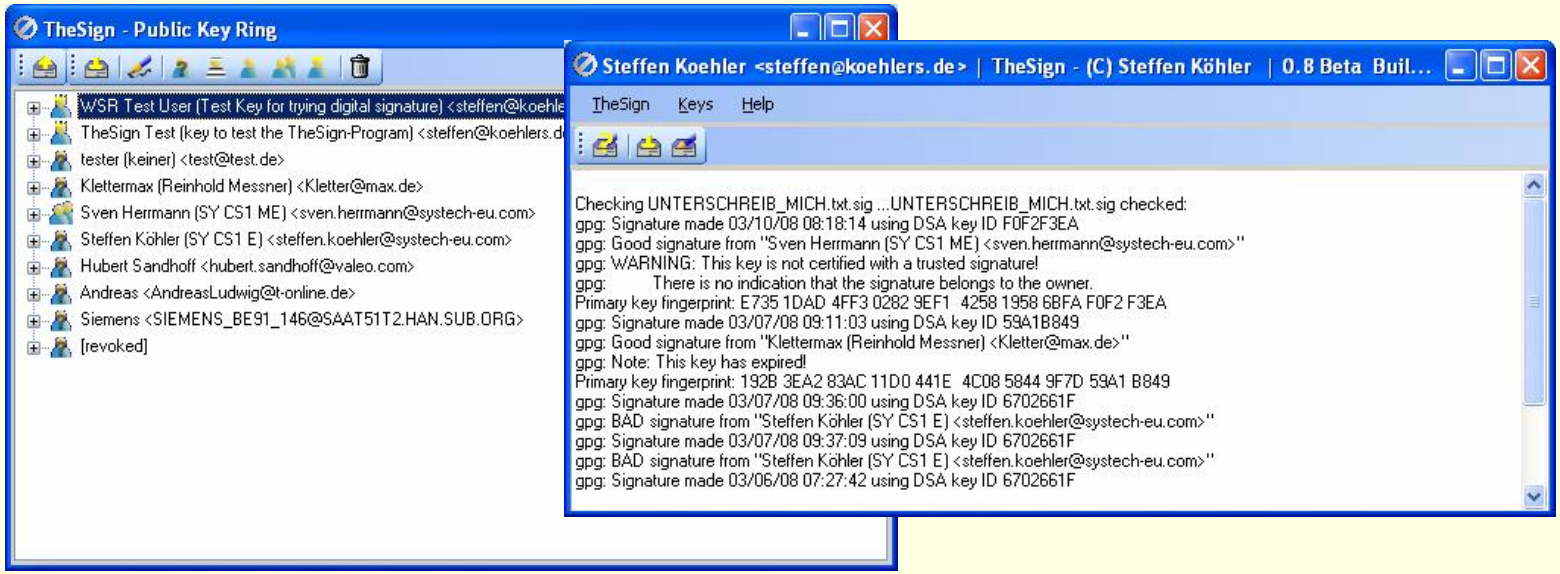
- The other users validate the Signature by compare it to the file checksum of their local file and your Public Key, stored in their Public Keyring




- Only if both matches, the Signature is valid

# TheSign – the Tool to do all this

- To perform all these tasks, TheSign is been made to make it simple




- more information can be found at http://www.koehlers.de/wiki/doku.php?id=thesign:index