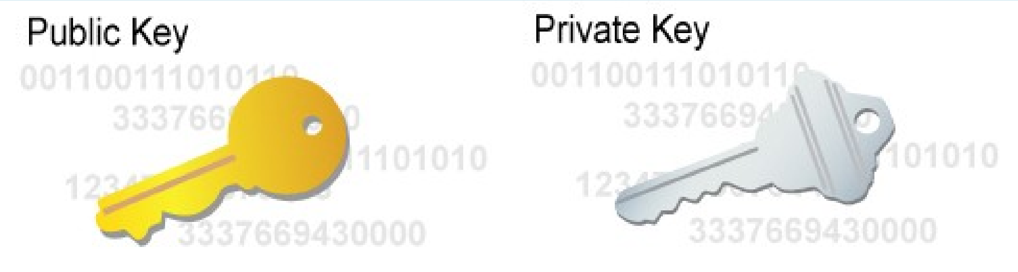
Public-Private Key Pairs Used for Other Purposes



The **keys**

- used to encrypt and decrypt
- **need not be the same**.

Other functions are parametrized by a key pair

- in which **either key** can be used **to encrypt**,
- but the **other key MUST** be used to **decrypt**.

Usually,

- **one key** is **kept private** by the owner, while
- the **second key** is **publicly** associated with the owner.

The approach is called **public-private key cryptography**.