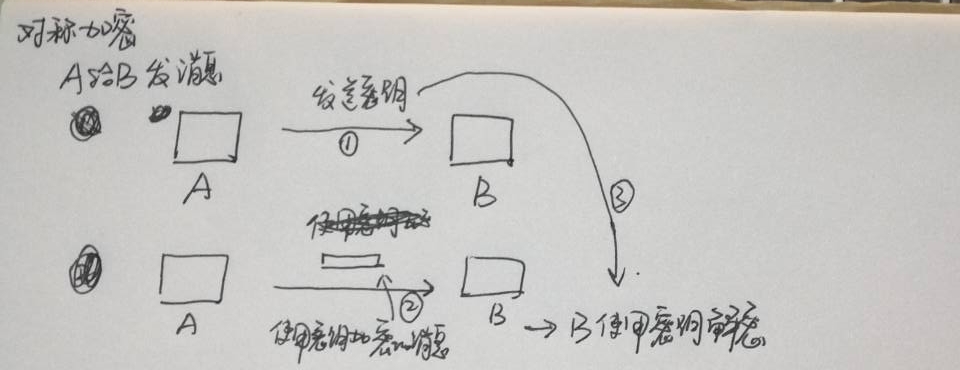
### **对称加密**

只使用一个密钥，加密和解密的过程都使用该密钥。

假设A与B之间要传送信息，首先A与B确定好密钥并保存，不能让其他人知道。若A给B发送信息，则用该密钥将信息加密，B收到密文后使用该密钥解密即可得到明文。

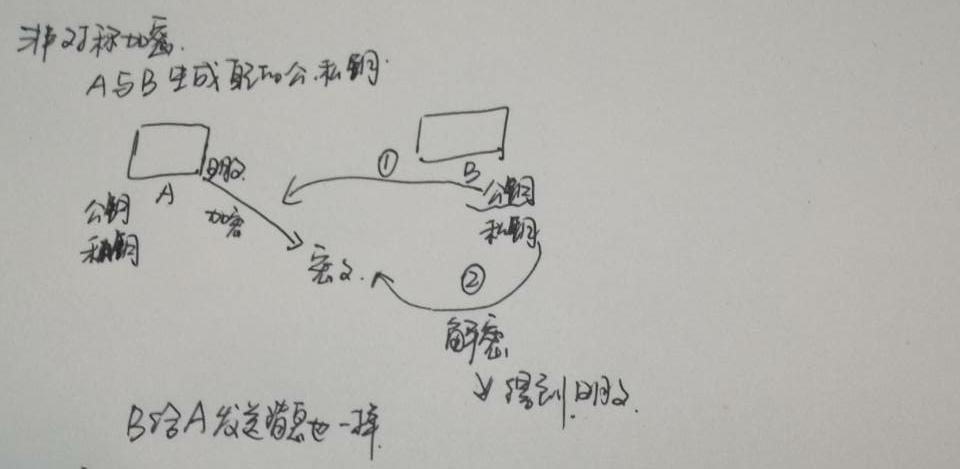


### **非对称加密**

有两个密钥，加密和解密使用不同的密钥，这两个密钥为公钥和私钥，公钥加密私钥解密，私钥加密公钥解密。

公钥是公开的，每个人都可以获得，私钥是非公开的只有本人有。

假设A向B发送消息，A与B都有公钥和私钥，A使用B的公钥将信息加密，B收到密文后用自己的私钥解密即可得到明文



### **混合加密**

混合加密吸取了对称加密和非对称加密的优点。

对称加密虽然传输的过程方便，但加解密算法相对简单同时密钥的传输不安全

非对称加密虽然没有密钥的传输同时加解密算法复杂，但是保存密钥和传输过程的成本很高

1.假设A与B之间传送消息，首先A与B确定自己的公钥和私钥

2.若A给B发送消息，A再确定一个密钥（对称），使用该密钥（对称）加密消息形成密文C1

3.再将该密钥（对称）用B的公钥加密形成C2

4.将加密的消息C1和加密的密钥C2（对称）发送给B，B使用自己的私钥解开C2得到密钥（对称），再使用该密钥（对称）解开密文即可得到明文

