一. 对称加密与非对称加密

按照密钥的使用形式，加密算法可以分为对称加密和非对称加密（又叫公钥加密）。对称加密在加密和解密的过程中，使用**相同**的秘钥；而非对称加密在加密过程中使用**公钥**进行加密，解密使用**私钥**。

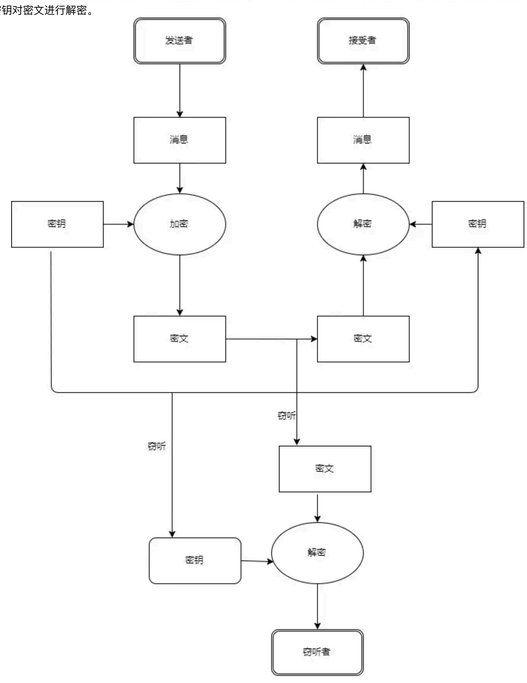
对称加密的加密和解密需要使用相同的密钥，所以需要解决密钥配送问题。非对称加密的处理速度远低于对称密钥

> 密钥：一个加密算法中，输入为明文和密钥，输出为密文。在加密算法中，密钥通常是像2384356390473975374937534539453794636236这样的 一串非常大的数字。

二. 对称加密下的密钥配送问题

发送者A想要发一封邮件给接受者B,但是不想被人看到其中的内容。A决定使用对称加密的方法。但是我们知道，对称在对称加密中，加密与解密需要使用同样的密钥。B想要看到接收到的内容必须要有A的密钥。也就是说，A需要把密钥安全地送到B的手上。

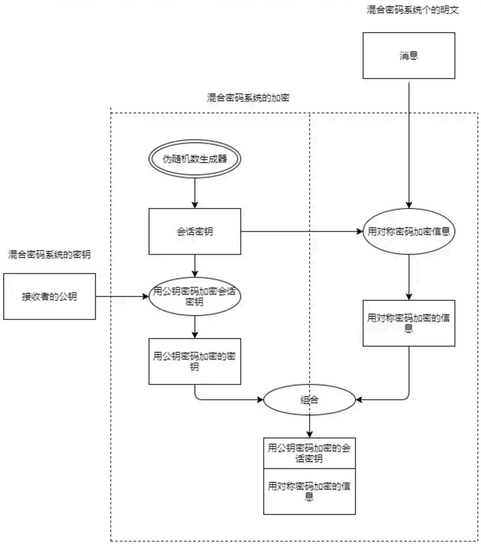
那如果把加密后的密文和密钥一同通过邮件发送给B行不行呢？答案是不行的。因为一旦被加密的密文和密钥同时落在窃听者C的手中，C就可以用密钥对密文进行解密。



三. 混合密码系统

混合密码系统，是将对称密码和非对称密码的优势相结合的方法。混合密码系统解决了对称密码的密钥配送问题，又解决了非对称密码的加密与解密速度问题。

混合密码系统中会先用快速的对称密码，对消息进行加密，这样消息就变为密文，保证消息机密性。然后，用非对称加密对对称密码的密钥进行加密，因为密钥一般比要加密的信息短，加密和解密的速度就得到保证了。这样，密码配送问题就得到了解决。



四. 单向散列函数

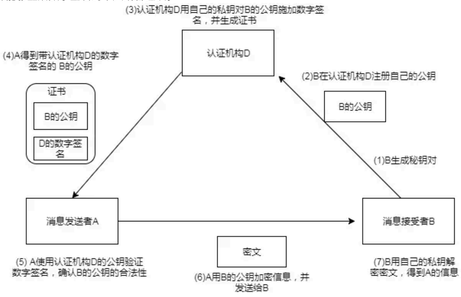
单向散列函数也称为消息摘要函数（message digest function），哈希函数，适用于检查消息完整性的加密技术。

单向散列函数有一个输入和一个输出，其中输入称为信息，输出称为散列值。单向散列函数可以根据消息的内容计算出散列值，篡改后的信息的散列值计算结果会不一样，所以散列值可以被用来检查消息的完整性 。

单向散列函数输出的散列值也成为消息摘要，或者指纹。散列来源于英文"hash"一值，单向散列函数的作用，实际上就是将很长的消息剁碎，然后混合成固定长度的散列值。

五. 证书

什么是证书: 公钥证书（Public-Key Certificate,PKC）由认证机构（CA)生成，用于确认公钥确实属于此人。认证机构，就是能确认"公钥确实属于此人"并能够生成数字签名的个人或者组织。



1. B生成密钥对
2. B在认证机构D注册自己的公钥
3. 认证机构D用自己的私钥对B的公钥施加签名并生成证书
4. A得到带认证机构D的数字签名的B的公钥
5. A使用认证机构D的公钥验证数字签名，确认B的公钥的合法性
6. A用B的公钥加密信息并发送给B
7. B用自己的私钥解密密文得到A的信息

六. 密码学对比

对称密码与非对称密码

	对称密码	公钥密码
发送者	用共享密钥加密	用公钥加密
接受者	用共享密钥加密	用私钥解密
密钥配送问题	存在	不存在
机密性	可保证	可保证