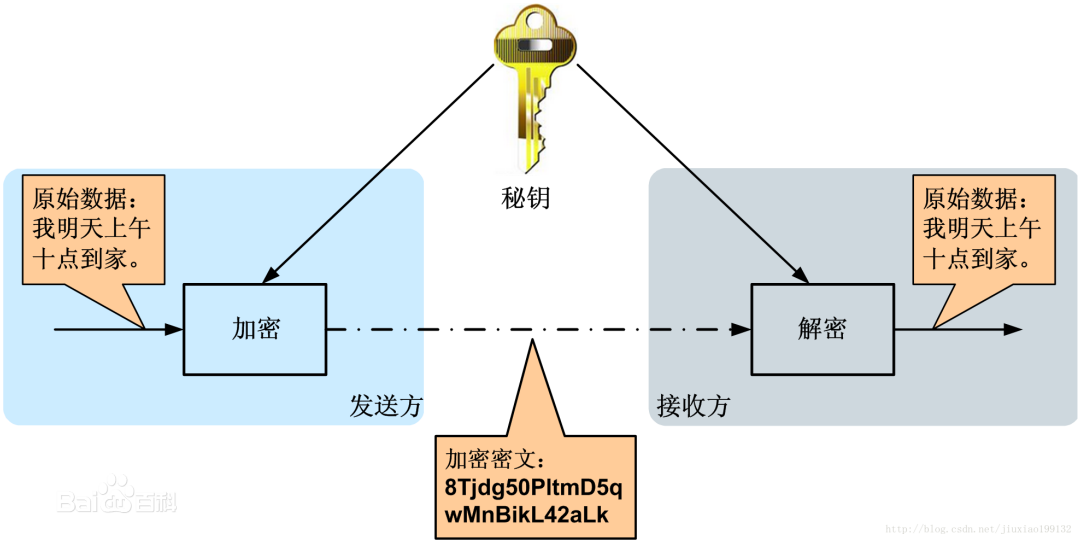
对称密码

采用单钥密码系统的加密方法，同一个密钥可以同时用作信息的加密和解密，这种加密方法称为对称加密，也称为单密钥加密。



工作过程

甲和乙是一对生意搭档，他们住在不同的城市。由于生意上的需要，他们经常会相互之间邮寄重要的货物。为了保证货物的安全，他们商定制作一个保险盒，将物品放入其中。他们打造了两把相同的钥匙分别保管，以便在收到包裹时用这个钥匙打开保险盒，以及在邮寄货物前用这把钥匙锁上保险盒。

上面是一个将重要资源安全传递到目的地的传统方式，只要甲乙小心保管好钥匙，那么就算有人得到保险盒，也无法打开。这个思想被用到了现代计算机通信的信息加密中。在对称加密中，数据发送方将明文（原始数据）和加密密钥一起经过特殊加密算法处理后，使其变成复杂的加密密文发送出去。接收方收到密文后，若想解读原文，则需要使用加密密钥及相同算法的逆算法对密文进行解密，才能使其恢复成可读明文。在对称加密算法中，使用的密钥只有一个，发收信双方都使用这个密钥对数据进行加密和解密。

常见算法

DES、3DES、TDEA、Blowfish、RC2、RC4、RC5、IDEA、SKIPJACK、AES等

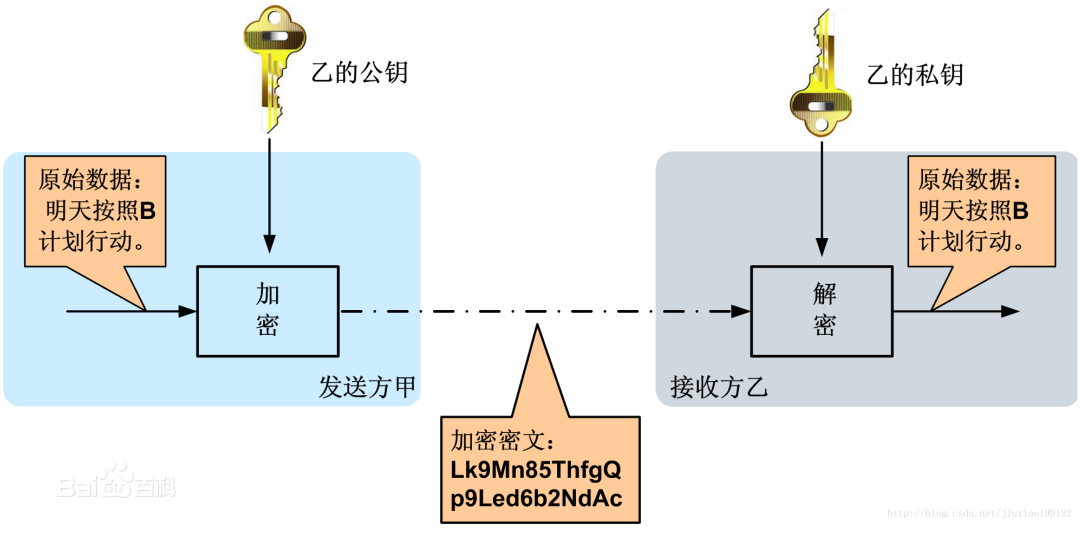
优缺点

对称加密算法的优点是算法公开、计算量小、加密速度快、加密效率高。

对称加密算法的缺点是在数据传送前，发送方和接收方必须商定好秘钥，然后使双方都能保存好秘钥。其次如果一方的秘钥被泄露，那么加密信息也就不安全了。另外，每对用户每次使用对称加密算法时，都需要使用其他人不知道的唯一秘钥，这会使得收、发双方所拥有的钥匙数量巨大，密钥管理成为双方的负担。

非对称密码

对称加密算法不同，非对称加密算法需要两个密钥：公开密钥（publickey）和私有密钥（privatekey）。公开密钥与私有密钥是一对，如果用公开密钥对数据进行加密，只有用对应的私有密钥才能解密；如果用私有密钥对数据进行加密，那么只有用对应的公开密钥才能解密。因为加密和解密使用的是两个不同的密钥，所以这种算法叫作非对称加密算法。



工作过程

1 乙方生成一对密钥（公钥和私钥）并将公钥向其它方公开。

2、得到该公钥的甲方使用该密钥对机密信息进行加密后再发送给乙

方。
3、乙方再用自己保存的另一把专用密钥（私钥）对加密后的信息进行解密。乙方只能用其专用密钥（私钥）解密由对应的公钥加密后的信息。
在传输过程中，即使攻击者截获了传输的密文，并得到了乙的公钥，也无法破解密文，因为只有乙的私钥才能解密密文。
同样，如果乙要回复加密信息给甲，那么需要甲先公布甲的公钥给乙用于加密，甲自己保存甲的私钥用于解密。

常见算法

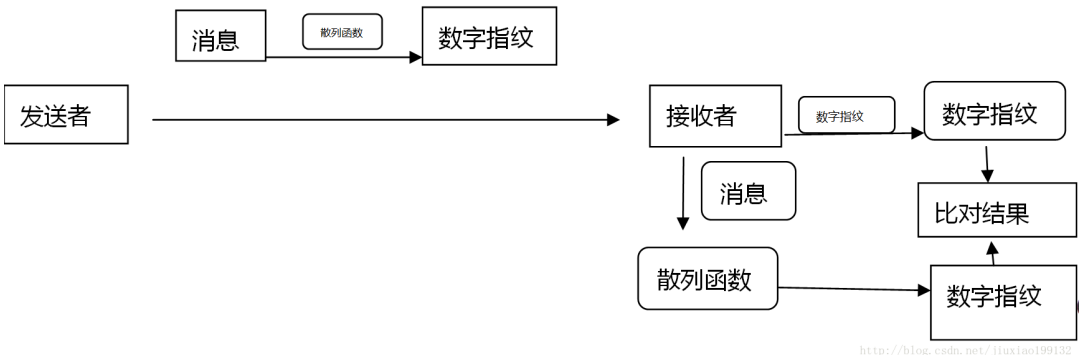
RSA、Elgamal、背包算法、Rabin、D-H、ECC

优缺点

非对称加密与对称加密相比，其安全性更好：对称加密的通信双方使用相同的秘钥，如果一方的秘钥遭泄露，那么整个通信就会被破解。而非对称加密使用一对秘钥，一个用来加密，一个用来解密，而且公钥是公开的，秘钥是自己保存的，不需要像对称加密那样在通信之前要先同步秘钥。
非对称加密的缺点是加密和解密花费时间长、速度慢，只适合对少量数据进行加密。

散列(hsah)

散列函数，也叫做哈希函数、消息摘要函数、单向函数、杂凑函数。与上面所说的密码不同，散列函数的主要作用不是完成数据加密与解密的工作，而是用来验证数据的完整性。通过散列函数，可以为数据创建“数字指纹”(散列值).



数字签名

与数据加密，解密，验证数据是否完整不同，数字签名是确认数据发送来源是否可信。

数字签名针对以数字形式存储的消息进行处理，产生一种带有操作者身份信息的编码。执行数字签名的实体称为签名者，签名过程中所使用的算法叫签名算法（signature algorithm），签名操作生成的编码称为签名者对消息的数字签名，发送者通过网络将消息连同其数字签名一起发送给接收者，接收者得到消息及其数字签名后，通过一个算法来验证签名者的真伪以及识别相应的签名者。

工作流程

1 甲方保留私钥，将公钥发布给乙方

2 甲方发送消息给乙方时，甲方使用私钥对消息做签名处理，然后将消息加密后的数据连同数字签名发送给乙方

3 乙方使用获得到的公钥对接收到的加密消息做解密处理，然和使用公钥连同获得到的数字签名对原始消息做验证处理