If you can’t explain it to a six-year-old, you don’t understand it yourself

--Albert Einstein

# 计算机通信安全

负责人: 孟政元

编写时间：2017年5月17日

## 前提要求

无

## 课程概览

带领同学们从一个具体的情景出发,

探讨一个简单场景中的通信存在的安全隐患和解决方法

## 课程内容

小明和小雨是一个班的同学,小明想约小雨放学之后去看电影,现在他需要把这个消息安全的传达给小雨

但是,现在没有手机,没有网络,而且在课堂上，小明不能直接跑到小雨旁边去直接告诉她，他只能通过传纸条的方式来和小雨对话

于是,小明在纸条上写上了他想说的话,然后把纸条折叠起来,交给了旁边的同学,让他们帮忙传给小雨

把纸条折叠起来这种方式虽然有一定的防止他人查看的作用,但是,这样是非常的不安全的,因为虽然纸条被折叠了起来,但是任何一个人都可以把纸条打开,看过里面的内容之后再把纸条折叠好,继续传下去.

更严重的是,传纸条的人可以随意的篡改纸条上的内容,但是小明不知道自己的纸条在传递的过程中被人篡改了,而且小雨在收到纸条之后也不知道他看到的是被篡改之后的纸条

这种通信方式就是完全没有安全措施的明文通信

现在仍有很大一部分通信是这种情况

比如吉林大学的官网就是明文传输,访问者无法确保自己看到的是没有经过篡改的网页



注意网址旁边的那个叹号,这是在提示用户当前访问的内容是不安全的

通信时需要经过的的个体一般被称为中间人

现在,小明该怎么防止纸条的内容被篡改呢(不考虑每个人字迹不一样的问题, 即假设每个人写的字都是一样的, 无法分辨字是谁写的)?

嗯,有办法了,小明可以和小雨约定,每张纸条上最多写20个字,如果不够20个字,就在后面加上圆圈凑够20个.小雨在收到纸条之后就可以通过这种方式来检测纸条的内容是不是被篡改了.

这样虽然防止了信息在传播的过程中被篡改，但是传播的信息仍然不是保密的

为了达到这个要求，小明必须选择一种方式，把他想要告诉小雨的话进行做一些处理，保证只有他们俩能够看懂纸条上的内容，纸条传递过程中经过的人即时看到了纸条上的内容也无法看懂纸条上的内容

现在，小明决定用一种除了她和小雨之外没有人懂的语言来写，这样的话，就可以确保她俩的通信不会被别人监听到，因为即使中间传递纸条的同学看到了纸条上的内容，也没办法弄明白纸条上的内容表达的是什么意思。

这种加密方法一般称为对称加密，因为加密和解密用的都是同一个秘钥，就是这里的那种只有他俩才懂的语言。

但是，要发明一种这样的语言对于小明来说太难了，而且教会小雨这种语言也很不容易，这种情况再实际场景中就是秘钥的传递和保管问题，这是对称加密的一个弱点。

现在，有一种更好的方法，那就是非对称加密。

还是小明的例子，如果小明采用非对称加密的方式来达到他的目的，那么他该怎么做呢？

所谓非对称加密就是加密和解密时候用的东西不一样

比如，小明和小花各有一个带锁的盒子，钥匙都在他们自己手里，然后把盒子交给同桌传到对方手里，然后把纸条放进箱子里锁好，再传递回去。由于在传递的过程中箱子是锁着的，中间的同学没有办法看到纸条，这样自然就保证了通信的安全性。

但是，在访问网页的时候，这样仍然不是安全的。这时候，向同学们讲解中间人攻击的原理。

## 课后总结

总结本节课讲解的内容