

2020年2月13日 星期四 下午4:15

让对方任意想一个3位数，并把这个数和91相乘，然后告诉我积的最后三位数，我就可以猜出对方想的是什么数字啦！比如对方想的是123，那么对方就计算出 123×91 等于11193，并把结果的末三位193告诉我。看起来，这么做似乎损失了不少信息，让我没法反推出原来的数。不过，我仍然有办法：只需要把对方告诉我的结果再乘以11，乘积的末三位就是对方刚开始想的数了。可以验证一下， $193 \times 11 = 2123$ ，末三位正是对方所想的秘密数字！

其实道理很简单，91乘以11等于1001，而任何一个三位数乘以1001后，末三位显然都不变（例如123乘以1001就等于123123）

[illegible]

要解决这个问题，真实世界就不是使用乘法了，比如RSA算法使用的是指数和取模运算，但本质上就是上面这套思想。