* 低加密指数广播攻击

RSA的广播场景。如果一个用户使用同一个加密指数e加密了同一个密文，并发送给了其他e个用户，那么就会产生广播攻击，更进一步，如果该用户使用的加密指数为低加密指数（如e=3），那么我们把此时产生的广播攻击称为低加密指数广播攻击[8]。

考虑如下同余方程组：

由中国剩余定理可知：

其中:

注意，我们这里的讨论是有前提的，即我们假设，此时有：

* 私钥下半部分泄露攻击

对于一个较小的e来讲（例如65537）,d的上半部分可以被有效的估计出来，根据RSA定义我们有：

即：

由于：

所以我们有：

由RSA定义可知，而我们知道,因此可知。因此，当e较小时，k就落在了一个较小的搜索空间，我们就可以通过穷举k来估计d。

对于d来讲，有：

即这样估计的话，误差为，鉴于，因此。如果考虑到p、q的比特数相同的情况下，即错误为*O*)。如果我们把d看做，其中，则。所以说对于e较小的情况下，我们通过穷举k，就有很大的概率可以恢复出d的上半部分，因此，如果d的下半部分被泄露的话，我们就有可能重构出整个私钥[7]。