























2>RSA算法的攻击方法:

RSA 算法的安全性依赖于大整数分解的困难性。 最直接的攻击方法是分解 n 得到 p,q，进而基于 e 计算 d，随着计算机运算能力的不断提高，通过二次筛法已能分解 180 多位的十进制素数，增加 p,q 的长度已成为许多安全应用系统的加密要求。 另一方面，利用系统设计和实现的缺陷， 人们也提出了一些基于非因子分解方式破解 RSA 算法的方案。 目前，对 RSA 算法的攻击主要有以下几种：

2.1 对模数 n 的因子分解

分解模数 n 是最直接的攻击方法，也是最困难的方法。 攻击者可以获得公钥 e 和模数 n；如果 n=pq 被成功分解，则攻击者可以计算出φ(n)=(p-1)(q-1)，进而从 ed≡1modφ(n)解得私钥 d。

2.2 对 RSA 的公共模数攻击

若一个多用户系统中只采用一个模数 n，不同的用户拥有不同的e 和 d，系统将是危险的。 在此系统中，若有同一消息用不同的公钥加密，这些公钥共模且互质，那该信息无需私钥就可解密。 举例来说，设P 为信息明文，两个加密公钥为 e1和 e2，公共模数是 n，有：C1=Pe1modn 和 C2=Pe2modn。如果攻击者获得 n、e1、e2、C1和 C2，就能得到 P。 因为 e1和 e2互质，故用欧几里德(Euclid)算法能找到 r 和 s，满足：r\*e1+s\*e2=1，设 r 为负数，则(C1-1)-r\*C2s=(Pe1modn)r\*(Pe2modn)s=(Pr\*e1+s\*e2)modn=Pmodn，如果 P

2.3 对 RSA 的小指数攻击

如果 RSA 系统的公钥 e 选取较小的值， 可以使加密和验证签名的速度有所提高。 但如果 e 取得太小，就容易受到小指数攻击。 例如，有同一系统的三个用户，分别使用不同的模数 n1，n2，n3，但都选取 e=3；另有一用户欲将同一明文消息 P 发送给以上三人，使用各人的公钥加密得：C1=P3(modn1)，C2=P3(modn2)和 C3=P3(modn3)一般地，n1，n2，n3互素（否则，会比较容易求出公因子，降低安全性），根据中国剩余定理，可由 C1，C2，C3计算：C=P3(modn1n2n3)如果 P

2.4 对 RSA 的选择密文攻击

选择密文攻击指的是攻击者能选择不同的密文，并拥有对应的明文，由此推出想要的信息。一般攻击者会伪装若干信息，让拥有私钥的用户签名，由此获得有用的明文-密文对，然后推算想要的信息。

例 1 攻击者想要伪造用户 u 对消息 x 的签名。 他可以先计算 x1,x2，使得 x≡(x1x2)(modn)，并骗取 u 对 x1和 x2的签名 s1=x1d(modn)和 s2=x2d(modn)， 则对 x 的签名可计算如：s=xd(modn)=(((x1x2)(modn))d)(modn)=((x1dmodn)(x2dmodn))modn=(s1s2)(modn)。

例 2 攻击者获得了用户 u 使用公钥 e 加密的密文 y=xe(modn)，想要得到 x。 他可以先计算 y′=re(modn)（r 是小于 n 的随机数），y″=(yy′)(modn)，然后骗取 u 对 y″的签名 s=y″d(modn)。 则通过计算(r-1s)(modn)可以恢复出 x，这是因为：(r-1s)(modn)=((y′dmodn)-1y″d)(modn)=(y′-dy″d)(modn)=(y′-dydy′d)(modn)=yd(modn)=x。

3对RSA算法的攻击的防御建议对于以上几种攻击，防御方案各不相同。攻击 1 源于 RSA 算法的数学安全基础， 增加初始化参数长度是有效的提高安全度的方法。而攻击 2 和攻击 3 源于应用 RSA 算法的系统的设计缺陷， 改进方法为：1）在多用户系统中必须采用多个模数；2）避免为了图求方便而使用取值太小的公钥 e。

攻击 4 最为复杂，从算法上无法解决这一问题，主要对应策略有两条：1）私钥持有者不对不信任的信息签名；2）签名信息时，先使用Hash 函数生成的摘要，再对摘要签名，避免直接对信息的签名。

以上防御方案并不能解决所有的 RSA 安全问题， 我们建议利用RSA 算法的系统仔细审核安全需求 ，投入使用先进行测试 ，并对系统安全做一个全面的审核。 必须对各种安全策略及程序进行合理优化，才能尽可能地降低风险，RSA 算法才能发挥最大的效用。