密码学

2019年4月19日 2:46

对称密码学

加密方式和解密方式困难程度相同，可以相互推得

非对称密码学：

加密方式和解密方式困难程度不等

RSA加密解密流程：

Pick two large primes, p and q. Let $n = pq$, then $\phi(n) = (p-1)(q-1)$. Encryption and decryption keys e and d are selected such that

- $\gcd(e, \phi(n)) = 1$
- $ed \equiv 1 \pmod{\phi(n)}$

$$C = M^e \bmod n \text{ (RSA } \textbf{encryption)}$$

$$M = C^d \bmod n \text{ (RSA } \textbf{decryption)}$$

作为使用密码的一方而言： 可以很简单利用两个大的质数构造出n=pq，进而求得φ（n）=（p-1）（q-1）,寻找一个和φ（n）互质的数e，以log（e）的复杂度可以求得其关于φ（n）的逆元d，（e，n）和d分别是加密秘钥和解密秘钥，满足以上两个定律，可以进行密文和明文之间的转化。

作为想要窃取信息的一方：就算获知加密秘钥e，和n，然而想要获得解密秘钥进而将密文破译成明文是很困难的。因为求d，绕不开求φ（n）=（p-1）（q-1），但是分解质因数是一个非常困难的问题

正确性证明：

$$x^{ed} \equiv x \pmod{n}.$$

RSA签名：

$$S = M^d \bmod n \text{ (RSA } \textbf{signature)}$$

$$M = S^e \bmod n \text{ (RSA } \textbf{verification)}$$

离散对数问题是非常困难的，因此通过签名盗取秘钥得可能性极低