AES 密钥产生过程

步骤	说明	描述
1	选择一对不相等且足够大的质数	p, q
2	计算 p, q 的乘积	$n = p \times q$
3	计算 n 的欧拉函数	$\varphi(n) = (p-1) \times (q-1)$
4	选一个与$\varphi(n)$互质的整数 e	$1 < e < \varphi(n)$
5	计算出 e 对于$\varphi(n)$的模反元素 d	$de \bmod \varphi(n) = 1$
6	公钥	$KU = (e, n)$
7	私钥	$KR = (d, n)$

计算 n 的欧拉函数，这步完成之后最好销毁 p 和 q

- 欧拉函数是小于 n 的正整数中与 n 互质的数的数目
- 互质是公约数只有 1 的两个整数，叫做互质整数
- 质数是指在大于 1 的自然数中。除了 1 和它本身以外不再有其他因数的自然数
- 如果 n 可以分解为两个互质的整数之积，那么 n 的欧拉函数等于这两个因子的欧拉函数之积

$$\varphi(n) = \varphi(p \times q) = \varphi(p) \times \varphi(q) = (p-1) \times (q-1)$$

计算模反元素 d

如果两个正整数 e 和$\varphi(n)$互质，那么一定可以找到一个整数 d，使得 ed-1 倍$\varphi(n)$整除，或者说 ed 除以$\varphi(n)$所得余数为 1

此时，d 就叫做 e 的模反元素

$$ed - 1 = k\varphi(n)$$
$$ed \bmod \varphi(n) = 1$$
$$ed \equiv 1 (mod\ n)$$

下面来证明解密过程：证明公钥加密私钥解密过程

明文 M，公钥加密$M^e \bmod n = C$

密文 C，私钥解密$C^d \bmod n = M$

$$C^d \bmod n = \left(M^e \bmod n\right)^d \bmod n$$
$$= M^{ed} \bmod n$$
$$= M^{k\varphi(n)+1} \bmod n$$
$$= \left(M^{k\varphi(n)} \times M\right) \bmod n$$

上面的证明过程有一个重要的变换，下面来进行变换

假设$M^e = an + b$，$0 < b < n$

$(M^e \bmod n)^d \bmod n = [(an+b) \bmod n]^d \bmod n$

$$= b^d \ mod \ n$$
$$= (an + b)^d \ mod \ n$$
$$= M^{ed} \ mod \ n$$

下面证明$M^{k\varphi(n)} = 1(mod \ n)$

根据欧拉定理，如果两个正整数 a 和 n 互质,

$$a^{\varphi(n)} = a \times a^{\varphi(n)-1} \equiv 1(mod \ n)$$

$M^{k\varphi(n)} = (M^k)^{\varphi(n)}$,下面只需证明$M^k$和$n$互质

n 的约数 1，n，p，q，其中 n，p，q 都非常大，M^k相比很小，因此M^k和n公

约数只有 1，因此两者互质，我们最终得到$C^d \ mod \ n = M$

下面来分析公钥加密私钥解密和私钥加密公钥解密过程

上面已经证明了公钥加密私钥解密过程

我们继续证明私钥加密公钥解密过程

明文 M，私钥加密$M^d \ mod \ n = C$
密文 C，公钥解密$C^e \ mod \ n = M$

$$C^e \ mod \ n = (M^d \ mod \ n)^e \ mod \ n$$
$$= M^{de} \ mod \ n$$

标红部分和上面公钥加密私钥解密一样，后面的证明同理，最终可以得到

$C^e \ mod \ n = M$