~~现代密码学~~ 5. RSA

~~5. RSA~~

5.10.

解：$x \in Z_n$.

$d_K(y) = (x^a)^b \pmod n = x^{ab} \pmod n$

$\cancel{\equiv x^{k\cdot\phi(n)}}$ ∵ $ab \equiv 1 \pmod{\phi(n)}$

∴ $x^{ab} = x^{k\cdot\phi(n)+1} \pmod n$, $k \in Z$

$d_K(y) = x^{k\phi(n)+1} \pmod n$

$= x \cdot x^{k\phi(n)} \pmod n$

当 $\gcd(x, n) \neq 1$，即 $(x, pq) \neq 1$，$\begin{cases} x = kp \\ \text{or} \\ x = kq \end{cases}$ $k \in Z$

不妨设 $x = mp$ ($m \in Z$)

1° $x \bmod p$ 的情况：

对 $x^{k\phi(n)+1} = (mp)^{ab} \equiv 0 \equiv x \pmod p$.

2° $x \bmod q$ 的情况：此时 $(x, q) = 1$.

$(mp)^{(p-1)(q-1)} = ((mp)^{q-1})^{p-1}$

由欧拉定理，$(mp)^{q-1} \equiv 1 \pmod q$.

∴ $x^{\phi(n)} = (mp)^{(p-1)(q-1)} \equiv 1 \pmod q$

~~$x^{\phi(n)} \equiv 1 \pmod p$~~ $x^{k\phi(n)+1} \equiv x \pmod q$.

∴ $\begin{cases} x^{ab} \equiv x \pmod p \\ x^{ab} \equiv x \pmod q \end{cases} \xrightarrow[\text{lcm}(p,q)=pq]{(p,q)=1} x^{ab} \equiv x \pmod{pq}$

∴ 综上，得证。

5.14.

解：若已知 $y = x^b \pmod n$，目标为恢复 x.

选择随机数 r，$\gcd(r, n) = 1$.

$y' = y \cdot r^b \pmod n$

将 y' 解密，获得 $x' = (y')^a \bmod n = y^a r^{ab} \bmod n$

∵ $ab \equiv 1 \pmod{\phi(n)}$

∴ $r^{ab} \equiv r \pmod n$

又 ∵ $y^a = x^{ab} \equiv x \pmod n$

∴ $x' = x \cdot r \pmod n$ $\Rightarrow x = x' \cdot r^{-1} \bmod n$

5.34. 证明：$\text{half}(y) = \text{parity}((y \times e_K(2)) \bmod n)$ ①

$\text{parity}(y) = \text{half}((y \times e_K(2^{-1})) \bmod n)$ ②

解：~~对①式：$y \times e_K(2) = e_K(2x) \cdot e_K(2)$~~

~~$y \times e_K(2) = (2x)^b = 2^b x^b = 2^b \cdot y$~~

~~$y \times e_K(2) \bmod n = e_K(2x) \bmod n$~~

~~∵ e_K 中已经 mod n 过了~~

~~∴ $y \times e_K(2) \bmod n = e_K(2x)$.~~

~~即证 $\text{half}(y) = \text{parity}(e_K(2x))$~~

~~parity(~~

对①式：$\text{parity}((y \times e_K(2)) \bmod n)$

$= \text{parity}((2^b y) \bmod n)$ ~~$= \text{parity}(e_K(2x)) = 0$~~

~~对②式 $\text{half}((y \times e_K(2^{-1})) \bmod n)$~~

~~$= \text{half}(e_K(2^{-1} \cdot x))$ ∵ $\frac{x}{2} < \frac{n}{2}$ ∴ $\text{half}(e_K(2^{-1}x)) = 0$~~

$= \text{parity}(e_K(2x \bmod n))$.

当 $2x \geq n$，$2x \bmod n = 2x - n$，∵ n 为奇 ∴ parity=1

当 $2x < n$，$2x \bmod n = 2x$ ∴ parity=0

∵ $\text{half}(y) = \begin{cases} 0, & 0 \leq x < \frac{n}{2} \\ 1, & \frac{n}{2} \leq x < n \end{cases}$

∴ ①得证。

对②式：$\text{half}((y \times e_K(2^{-1})) \bmod n)$

$= \text{half}(e_K(x \cdot 2^{-1} \bmod n))$

当 x 为偶，$x \cdot 2^{-1} \bmod n = \frac{x}{2} \bmod n$，half = 0.

当 x 为奇 $f(x) = x \cdot 2^{-1} \bmod n - \frac{n}{2} = (2^{-1} \cdot x - \frac{n}{2}) \bmod n$

~~$2 \cdot x \cdot 2^{-1} \bmod n = x \bmod n$~~

$2f(x) = (2 \cdot 2^{-1} x - n) \bmod n = x \bmod n > 0$

∴ $f(x) > 0$. $\Rightarrow$ half = 1

∵ $\text{parity}(y) = \begin{cases} 0, & x \text{偶} \\ 1, & x \text{奇} \end{cases}$

∴ ②得证