RSA 公钥加密体制

找一个加密函数 f，使得解密函数 d 不容易算

对于 M，$d(f(M)) = M$

① 找到 $n = pq$，p, q 为素数，但将 n 合并为 2 个素数集求很难做

↓ 安全性假设：将 n 合并为 p, q 无法在 k^t 次算法内算出，$k = \log n$（大数合解）

② $\varphi(n) = (p-1)(q-1) = n - p - q + 1$

③ 找 e，s.t. $(e, \varphi(n)) = 1$，e 是公开的，可以找一些小素数

④ 求解 $ed \equiv 1 \bmod \varphi(n)$，$d$ 在 $[\varphi(n)]$ 中唯一

公开：n e
私有：$p, q, \varphi(n), d$

使用 n, e 用来加密，$\varphi(n), d$ 用来解密

加密：M：$f(M) = M^e \bmod n$

（N）

解密：$d(f(M)) = M$

希望 $N^t \equiv M \bmod n$

$(M^e)^d \equiv M \bmod n$

$M^{ed} \equiv M \bmod n \Rightarrow M^{ed-1} \equiv 1 \bmod n$

已知 $M^{\varphi(n)} \equiv 1 \bmod n$

目标：找 t s.t. $M^{ed} \equiv M \bmod n$ → 只要 $ed = k\varphi(n) + 1$ 即 $ed \equiv 1 \bmod \varphi(n)$

证：加密：$N = f(M) = M^e \bmod n$

解密：$M = d(N) = (M^e \bmod n)^d \bmod n = M^{ed} \bmod n = M$