RSA暗号

- 鍵の生成

  1. 50 桁程度の素数 p と q を選び $n = pq$ を計算する
  2. $\Phi(n) = (p-1)(q-1)$ と互いに素な整数 e を決める (gcd(e,(p-1)(q-1))=1)
  3. $ed \equiv 1 mod\ \Phi(n)$ を満たす d を求める
  4. n と e を公開、p と q、d を秘密にする

- 暗号化　$C \equiv M^e\ mod\ n$
- 復号化 $C^d = M^{ed} = M\ mod\ n$