RSA密码体系

- 过程
  选取大素数p,q(p!=q)
  令n=$p*q$,则 phi(n)=$(p-1)*(q-1)$
  选取e， 使得gcd(e,phi(n))=1
  解同余方程组e*d=1 (\%phi(n))
  则公钥为<e,n>
  私钥为<d,n>
- 性质
  c_i=m_i^e%n
  m_i=c_i^d%n