RSA I — public-key cryptography from scratch

Lesson 32 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

Practice problems

1. Given the primes $p = 7$ and $q = 13$, choose $e = 5$. Find the modulus n, the totient $\phi(n)$, the private key d, and encrypt the message $M = 2$.
2. Using the keys $n = 33$ and $e = 3$ (from the lesson), decrypt the ciphertext $C = 15$.
3. If a user chooses $p = 11$ and $q = 17$, and wants to use $e = 7$, what is the private key d? Show your work using the Extended Euclidean Algorithm.

Solutions

1. Given the primes $p = 7$ and $q = 13$, choose $e = 5$. Find the modulus n, the totient $\phi(n)$, the private key d, and encrypt the message $M = 2$.

   - Compute $n = 7 \times 13 = 91$.
   - Compute $\phi(n) = (7-1)(13-1) = 6 \times 12 = 72$.
   - Find d such that $5d \equiv 1 \pmod{72}$. Since $5 \times 29 = 145 = 2 \times 72 + 1$, we have $d = 29$.
   - Encrypt $M = 2$: $C = 2^5 \pmod{91} = 32 \pmod{91} = 32$.

   Answer: n=91, \phi(n)=72, d=29, C=32

2. Using the keys $n = 33$ and $e = 3$ (from the lesson), decrypt the ciphertext $C = 15$.

   - The private key d for $n = 33, e = 3$ was found to be 7.
   - Compute $M = 15^7 \pmod{33}$.
   - Using fast exponentiation: $15^1 \equiv 15$, $15^2 = 225 = 6 \times 33 + 27 \equiv 27 \equiv -6 \pmod{33}$.
   - $15^4 \equiv (-6)^2 = 36 \equiv 3 \pmod{33}$.
   - $15^7 = 15^4 \times 15^2 \times 15^1 \equiv 3 \times (-6) \times 15 = -18 \times 15 = -270$.
   - $-270 \pmod{33}$: $33 \times (-9) = -297$. $-270 - (-297) = 27$.

   Answer: M=27

3. If a user chooses $p = 11$ and $q = 17$, and wants to use $e = 7$, what is the private key d? Show your work using the Extended Euclidean Algorithm.

   - Compute $n = 11 \times 17 = 187$.
   - Compute $\phi(n) = 10 \times 16 = 160$.
   - Solve $7d \equiv 1 \pmod{160}$.
   - Apply Euclidean Algorithm: $160 = 22 \times 7 + 6$; $7 = 1 \times 6 + 1$.
   - Back-substitute: $1 = 7 - 1(6) = 7 - 1(160 - 22 \times 7) = 23 \times 7 - 1 \times 160$.
   - Thus, $23 \times 7 \equiv 1 \pmod{160}$, so $d = 23$.

   Answer: d=23
