RSA II — a full worked encryption/decryption

Lesson 33 · Module 2 — Number Theory & Cryptography · Discrete Mathematics · daily-maths.uk/discrete

Practice problems

1. Given $p = 3$ and $q = 11$, and a public exponent $e = 3$, find the private key d and encrypt the message $M = 5$.
2. Using the keys from the previous problem ($n = 33, d = 7$), decrypt the ciphertext $C = 26$ to verify the original message.
3. Suppose an attacker knows the public key ($e = 17, n = 3233$) and manages to factor n into 61×53. Show how they can find the private key d.

Solutions

1. Given $p = 3$ and $q = 11$, and a public exponent $e = 3$, find the private key d and encrypt the message $M = 5$.

   - Compute $n = 3 \times 11 = 33$.
   - Compute $\phi(n) = (3-1)(11-1) = 2 \times 10 = 20$.
   - Find d such that $3d \equiv 1 \pmod{20}$. Since $3 \times 7 = 21 \equiv 1 \pmod{20}$, we have $d = 7$.
   - Encrypt $M = 5$: $C = 5^3 \pmod{33} = 125 \pmod{33}$.
   - Since $33 \times 3 = 99$, $125 - 99 = 26$.

   Answer: d=7, C=26

2. Using the keys from the previous problem ($n = 33, d = 7$), decrypt the ciphertext $C = 26$ to verify the original message.

   - Compute $M = 26^7 \pmod{33}$.
   - Use repeated squaring: $26^1 \equiv 26 \equiv -7 \pmod{33}$.
   - $26^2 \equiv (-7)^2 = 49 \equiv 16 \pmod{33}$.
   - $26^4 \equiv 16^2 = 256$. $256 = 33 \times 7 + 25$, so $26^4 \equiv 25 \equiv -8 \pmod{33}$.
   - $26^7 = 26^4 \times 26^2 \times 26^1 \equiv (-8) \times 16 \times (-7) \pmod{33}$.
   - $-8 \times 16 = -128$. $-128 = 33 \times (-4) + 4$, so $-128 \equiv 4 \pmod{33}$.
   - $4 \times (-7) = -28$. $-28 \equiv 5 \pmod{33}$.

   Answer: M=5

3. Suppose an attacker knows the public key ($e = 17, n = 3233$) and manages to factor n into 61×53. Show how they can find the private key d.

   - The attacker calculates $\phi(n) = (61-1)(53-1) = 60 \times 52 = 3120$.
   - They now solve $17d \equiv 1 \pmod{3120}$ using the extended Euclidean algorithm.
   - Step 1: $3120 = 183 \times 17 + 9$.
   - Step 2: $17 = 1 \times 9 + 8$.
   - Step 3: $9 = 1 \times 8 + 1$.
   - Back-substituting: $1 = 9 - 8 = 9 - (17 - 9) = 2(9) - 17 = 2(3120 - 183 \times 17) - 17 = 2(3120) - 367 \times 17$.
   - Thus, $d \equiv -367 \pmod{3120}$.
   - Adding the modulus: $d = 3120 - 367 = 2753$.

   Answer: d=2753
