LESSON MAKER PRO

Secret Number Messages

Encrypt and decrypt with small RSA keys.

HIGH SCHOOL · FM.IP.A.30.a

FM.IP.A.30.a "Use modular arithmetic to apply RSA (Rivest-Shamir-Adleman) public-key cryptosystems."

NAME _____ DATE _____

HOW RSA WORKS

For n = pq, compute phi(n) = (p - 1)(q - 1), then choose d so ed leaves a remainder of 1 when divided by phi(n). Encrypt m with $c = m^e \bmod n$, and decrypt c with $m = c^d \bmod n$. The small keys on this page model RSA, but real keys are much larger.

WORKED EXAMPLE

Let p = 3, q = 7, e = 5, and m = 2. Find d, encrypt m, and check by decrypting.

1. n = 3 × 7 = 21, and phi(n) = 2 × 6 = 12. Since 5 × 5 = 25 leaves remainder 1 when divided by 12, d = 5.
2. $2^5 = 32$, so c = 32 mod 21 = 11.
3. $11^2 \bmod 21 = 16$, and $11^4 \bmod 21 = 4$.
4. $11^5 \bmod 21 = (4 \times 11) \bmod 21 = 2$.

Answer: d = 5, c = 11, and the decrypted message is 2.

PRACTICE 6 problems

1 Let p = 3, q = 11, and e = 3. Find phi(n) and a value of d between 1 and phi(n) - 1.

ANSWER _____

2 Use the public key (n, e) = (33, 3) to encrypt m = 4. Find c.

ANSWER _____

3 Use the private key (n, d) = (33, 7) to decrypt c = 31. Find m.

ANSWER _____

4 Let p = 5, q = 7, and e = 5. Find phi(n) and a value of d between 1 and phi(n) - 1.

ANSWER _____

5 Use the public key (n, e) = (35, 5) to encrypt m = 3. Find c.

ANSWER _____

6 Use the private key (n, d) = (35, 5) to decrypt c = 33. Find m.

ANSWER _____

APPLY IT Show your work

1 A coding club tests a pretend ticket app. It represents a ticket type by m = 4 and uses the public key (n, e) = (55, 3). What encrypted number should the app send?

WORK SPACE

ANSWER _____

2 In a classroom chat simulation, a student receives the encrypted number c = 26. The private key is (n, d) = (33, 7). What original number was sent?

WORK SPACE

ANSWER _____

CHALLENGE One step up

A toy RSA key uses p = 5, q = 11, and e = 3. Find d, then decrypt c = 27. Show the powers of 27 you use to find the original number.

WORK SPACE AND ANSWER

Secret Number Messages

PART 1 · PRACTICE

#	PROBLEM	ANSWER
1	Let p = 3, q = 11, and e = 3. Find phi(n) and a value of d between 1 and phi(n) - 1.	**phi(n) = 20; d = 7.**
2	Use the public key (n, e) = (33, 3) to encrypt m = 4. Find c.	**c = 31.**
3	Use the private key (n, d) = (33, 7) to decrypt c = 31. Find m.	**m = 4.**
4	Let p = 5, q = 7, and e = 5. Find phi(n) and a value of d between 1 and phi(n) - 1.	**phi(n) = 24; d = 5.**
5	Use the public key (n, e) = (35, 5) to encrypt m = 3. Find c.	**c = 33.**
6	Use the private key (n, d) = (35, 5) to decrypt c = 33. Find m.	**m = 3.**

PART 2 · APPLY IT

1. **9** Compute $4^3 = 64$. The remainder when 64 is divided by 55 is 9.
2. **5** Find $26^2 \bmod 33 = 16$ and $26^4 \bmod 33 = 25$. Then $26^7 \bmod 33 = (25 \times 16 \times 26) \bmod 33 = 5$.

CHALLENGE

phi(n) = 40 and d = 27 because 3 × 27 = 81 leaves remainder 1 when divided by 40. Modulo 55, $27^2 = 14$, $27^4 = 31$, $27^8 = 26$, and $27^{16} = 16$. Since 27 = 16 + 8 + 2 + 1, m = (16 × 26 × 14 × 27) mod 55 = 3.

Accept equivalent modular steps that lead to the stated remainders. In the challenge, students may use another correct way to evaluate $27^{27} \bmod 55$.