COLLEGE of CHARLESTON

MATH MEET 2019

RSA Encryption All-Day Sprint

The RSA encryption system is a way to securely transmit secrets. It's based on properties of prime numbers. Here's the basic setup.

Let p and q be distinct prime numbers. Define $n = pq$ and $\lambda = \text{lcm}(p-1, q-1)$. Choose a number e that is relatively prime to λ, and define d to be a number for which $de \equiv 1 \pmod{\lambda}$.

The important theorem is that for any integer m, $m^{de} \equiv m \pmod{n}$.

The RSA cipher is asymmetric. That means each agent using the cipher has two keys, a public key (n, e) that everyone knows, and a corresponding private key (n, d) that only its owner knows. If I want to send you a message that only you can read, I express it as an integer m, and transmit the integer $m^e \bmod n$. You decipher my message back to m by computing $(m^e)^d \bmod n$, which works because of that theorem. Anyone who overhears my message to you and tries to decipher it would need to know d, but finding d is very difficult if p and q are large enough. I'll guide you through some calculations with small p and q so you can see how it works.

Let's get some practice. Suppose we agree to represent letters of the alphabet by numbers, so $1 = A$, $2 = B$, $\ldots 26 = Z$. Let's use $27 =$ space, $28 =$ period, and $29 =$ comma.

Let's use $p = 3$ and $q = 11$, so $n = 33$ and $\lambda = 10$. Let's pick $e = 7$. Then since $7 \times 3 = 21 \equiv 1 \pmod{\lambda}$, we know $d = 3$. So the public key is $(n = 33, e = 7)$ and the private key is $(n = 33, d = 3)$.

If I want to send you the letter "D," I translate that to a number and us that as the message $m = 4$. I then compute

$$m^e = 4^7 = 16384 \equiv 16 \pmod{33}$$

so I broadcast the cipher text $c = 16$ to you. You recover the original message by computing

$$c^d = 16^3 = 4096 \equiv 4 \pmod{33}$$

Let's continue with the same public key $(n = 33, e = 7)$ and private key $(n = 33, d = 3)$.

1. Decipher the following sequence of messages, corresponding to the letters of a single English word: $2, 14, 12, 12, 27$

HELLO

2. Encrypt the word "WORLD" to a sequence of integers.

23,27,6,12,16

For the next several questions, use $p = 17, q = 11, e = 3$.

3. What is d?

   27

4. Encrypt the word "PIZZA" as a sequence of integers.

   169, 168, 185, 185, 1

5. Decipher the word $27, 168, 35, 27, 45, 125$.

   CIRCLE

For the next several questions, suppose you intercept a message. You know that the receiver's public key is $(n = 323, e = 5)$.

6. Crack the private key: What is d?

   29

7. Decipher the message: $304, 2, 122, 263, 55, 89, 304$

   SOLIDUS