UNDERSTANDING RSA ENCRYPTION

Introduction

How can you communicate a secret when everyone can hear you? For thousands of years, people have devised methods to communicate with each other secretly. Many of these methods rely on a secret code that the sender and receiver have shared in advance. The study of these codes is called *cryptography*. Transforming a message using the code is called *encryption*. The process of decoding the message is *decryption*.

But what if the sender and receiver never have a chance to communicate privately about the code they will use? If they communicate without any encryption, then their messages will be out in the open, for anyone to read. But if they first establish an encryption method, that method too will be out in the open—and then an *adversary* could use it to understand any messages that are transmitted.

The *RSA encryption algorithm* described here represents one solution to this seemingly insoluble problem. Using RSA encryption, two parties can communicate secretly even though they have never privately established a secret code.

RSA encryption is special because the method of decryption cannot be determined from the method of encryption. Even though the encryption method can be observed by anyone, only the intended recipient possesses the decryption method. Since the decryption method is never communicated, it stays a secret. And since the decryption method is secret, no one but the intended recipient can decode the message.

Understanding RSA encryption requires some knowledge of modular arithmetic and some of the special properties of prime numbers. After reviewing the math, we'll examine step-by-step how to encode and decode using RSA encryption.

Mathematics warm-up

One of the key ideas behind RSA encryption is *modular arithmetic*. When we evaluate an expression using modular arithmetic, we divide its value by a special number, called the *modulus*. What we care about is the remainder after that division.

For example, we could write $7 + 8 \equiv 3 \pmod{12}$. That's because $(7 + 8) \div 12 = 1 \text{ r } 3$, and it's the remainder that counts in modular arithmetic.

> *Check for understanding*
>
> One way to think about the sentence $9 + 5 \equiv 2 \pmod{12}$ is that it explains what time it is 5 hours after 9:00. Write a modular arithmetic sentence to represent the time 11 hours after 4:00.
>
> On Saturn, a day is about 10 hours. If we divide Saturn's day into two equal-length periods, called AM and PM, what time would be 7 hours after 2 AM? Explain your reasoning using modular arithmetic.

The remainder after dividing 9,857 by 379 is 3. Write a modular arithmetic sentence that states this.

A *prime* number is a whole number with exactly two factors: itself, and 1. (One is not prime, since it has only 1 factor: itself.) The first few prime numbers are $\{2, 3, 5, 7, 11, 13, 17 \ldots\}$. Because there are infinitely many primes, we can always find a prime as big as we like.

Check for understanding

Is 27 prime? How do you know?

$w = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17$. Is w prime?

The fundamental theorem of arithmetic states that any whole number greater than 1 that is not prime can be written as the product of primes. For example, 100 is not prime, since it has lots of factors: $\{1, 2, 4, 5, 10, 20, 25, 50, 100\}$. But 100 can be written as the product of primes: $100 = 2 \times 2 \times 5 \times 5$. Moreover, there is only one, unique way to write a *composite* number as the product of primes. There are no other groups of prime numbers other than $\{2, 2, 5, 5\}$ that multiply together to make 100.

Check for understanding

Write 256 and 99 as the product of primes.

Consider w described above. Express w as a product of 3 prime factors and 2 composite factors.

The RSA encryption algorithm

This section will describe the procedure for encoding and decoding a message, as well as the steps to generate d, e, and n, which are used in each step of the process. On the left we'll describe the algorithm in general terms. On the right we'll show a numeric example.

Encoding

To encrypt a message using RSA, you will need to know two numbers: e, the public exponent, or the encryption exponent n, the modulus. Both these numbers are given to the sender by the recipient. We'll discuss how to calculate these numbers later on. For now, let's use them to create an encrypted message, or *cyphertext*.	Message for encryption: "B" $e = 5,$ $n = 14.$
1. Convert your message to an integer, m, using some previously chosen procedure. This conversion method is not a secret—it's just a way to turn your message into something that can be manipulated mathematically. We will transmit just one letter, and we'll assign it a number that represents its position in the alphabet.	"B" is the 2nd letter, so it's encoded as 2. $m = 2.$

2. Use the formula $m^e \bmod n = c$ to create c, the cyphertext that you will send to the recipient. To anyone other than the recipient (including the sender!) this message will just look like a meaningless number. But your recipient will be able to transform it into a meaningful message from you. 3. Send your message! Don't worry about anyone intercepting it. Even if someone does see your message, they won't be able to decode it, even if they know e and n.	$m^e \bmod n = c$ $2^5 \bmod 14 = 4$

Check for understanding

Practice encoding by determining the cyphertext for the messages "D," "G," and a third letter of your choice.

Sangmin and Jonathan are communicating using RSA encryption. They want to be able to send messages of two-letters each. The public key for their encryption includes $n = 350$. Do you foresee any challenges for their plan?

Decoding

To decrypt a message using RSA, you will need to know two numbers: d, the secret exponent, or the decryption exponent n, the modulus. The modulus, n, is the public number that was also used to encode the message. The decryption exponent, d, is a secret that's never transmitted or shared. Only the person who knows d can decrypt the message.	Message to be decrypted: 4. $d = 11,$ $n = 14.$
1. Use the formula $c^d \bmod n = m$ to decode the cyphertext.	$c^d \bmod n = m$ $4^{11} \bmod 14 = 2$
2. Convert the decoded integer back into a letter of the alphabet.	The 2nd letter of the alphabet is "B," so that's the message.

Check for understanding

Practice decoding by determining the plain text message for the cyphertexts 3, 9, and 0.

Check out wolframalpha.com. How many decimal digits are there in 55^{132}?

Now that we have practiced encrypting and decrypting, let's examine how to determine three numbers, d, e, n, that make RSA encryption possible.

Calculating the modulus, n

The RSA algorithm requires three related numbers that you have already worked with: d, the decryption exponent, e, the encryption exponent, and n, the modulus. We will start by calculating n.	
1. Choose two prime numbers, p and q. In practice, these would be very large: hundreds of digits.	We'll calculate d, e, and n as used in the examples above, so we won't need very large p and q. Let's choose $p = 2$, $q = 7$.
2. $n = pq$. That was easy!	$\boldsymbol{n = 14}$.

Calculating the encryption exponent, e

1. To calculate e, we first must determine the number of integers less than n that do not share any common factors with n. The function that relates an integer to the number of its *coprime predecessors* is called Euler's totient function, $\varphi(n)$, pronounced "phi of n." It turns out that $\varphi(n) = (p-1)(q-1)$.	$\varphi(n) = (p-1)(q-1)$ $\varphi(14) = (7-1)(2-1)$ $\varphi(14) = 6$
2. Search for e by looking for a number that satisfies a few conditions: a. e must be greater than 1 and less than $\varphi(n)$. b. e must not share any factors with n or $\varphi(n)$.	Condition (a) means we can choose from $\{2, 3, 4, 5\}$. Condition (b) rules out 2, 3, and 4, which all share a factor with $\varphi(n) = 6$. So $\boldsymbol{e = 5}$ is our only choice.

Calculating the decryption exponent, d

1. To calculate d, we need to search for a number that satisfies the condition $de \bmod \varphi(n) = 1$.	Recall that $e = 5$, and $\varphi(n) = 6$. We're looking for a multiple of 5 that is one greater than a multiple of 6. Some searching reveals that $(5 \times 11) \bmod 6 = 1$. So choose $\boldsymbol{d = 11}$.

Check for understanding

In order to determine d, e, and n, we also needed to use the numbers p, q, and $\varphi(n)$. How can p, q, and $\varphi(n)$ help us understand how d, e, and n are related to each other? Another way to ask this question is, What did our methods for determining d, e, and n have in common, mathematically? What was different about them?

Imagine that you are attempting to break an RSA encryption code so that you can save the world. You know the values of e and n, but you do not know the value of d. At this point, you encounter two wizards, Theodophilus the Taupe and Acidophilus the Beige. Theodophilus offers to tell you the values of p and q. Acidophilus offers to tell you the value of $\varphi(n)$. Which wizard would you find more helpful? Why?

Just as The Beige Wizard begins inscribing the value of $\varphi(n)$ on the mountainside, he slips and falls to his doom. (This is common, because useful wizards tend to be very, very old.) You are left alone with the burden of your quest, and only The Taupe Wizard to help you. Can you still save the day? How?

Acknowledgements and resources for further study

Thank you to Eddie Woo, whose YouTube videos on the RSA algorithm provided the example above. Check out https://youtu.be/4zahvcJ9glg.

"RSA-129 – Numberphile." https://youtu.be/YQw124CtvO0.

"RSA Algorithm." https://www.di-mgt.com.au/rsa_alg.html.

Rivest, Shamir, and Adleman. "A Method for Obtaining Digital Signatures and Public-Key Cryptosystems." https://people.csail.mit.edu/rivest/Rsapaper.pdf. This is the original paper presenting the RSA algorithm, published in 1977.