Public Key Cryptography

Brynn Bergeson

Contents

1 Introduction

Public key cryptography is becoming a necessity in today's society with all the technological advances of modern communication. Important bank transactions and the transfer of sensitive information would be at risk without anything in place to protect the information because of the lack of security. Thus, public key cryptography uses concepts from abstract algebra to safe guard data transfers to allow security on the internet. Some of the abstract algebra concepts used in public key cryptography include group theory, modular arithmetic, and number theory. Number theory of prime numbers specifically and modular arithmetic is heavily used in RSA encryption and decryption.

2 RSA Encryption

The RSA Public Key Cryptosystem was invented by Ronald Rivest, Adi Shamir and Leonard Adleman, hence the name RSA from their last names, at MIT in 1977[1]. They formed a way of public key encryption that is secure in a way that it would take around thousands of years for a hundred million personal computers working together to crack this in a form of a bank transaction which uses unfathomably big numbers for this algorithm. So how does this algorithm use abstract algebra concepts? RSA uses modular arithmetic and prime number utilization to create a secure public key encryption[2].

2.1 RSA Algorithm

The RSA algorithm is so effective because of the fact that it uses the notion that it is easy to generate a prime number, it is easy to multiply numbers, and that factoring a number into its prime factors is hard. Furthermore, since modular arithmetic is fairly simple when

given what is needed and is difficult when certain factors are not given this creates a secure system for public key encryption.

RSA Encryption Formula

If m is the **message** to be sent, e is the **public exponent**, and n being the product of two prime numbers, then

$$c \equiv m^e \bmod n$$

gives the **ciphertext** c, where both m and c are between 0 and $(n-1)$.

The message is typically in a numerical format as well as the ciphertext, which is essentially the encrypted message. The public exponent, or public key, is used to both encode and decode the encrypted message and is made public. To get the values of n and e, it requires the use of prime numbers. Let p and q be two prime numbers. It is then so that $n = p \cdot q$ and the public exponent e is between 3 and $n-1$ such that e is relatively prime to $(p-1)(q-1)$.

Example 1
Suppose you want to send a message of the value 48. Choosing two prime numbers, set $p = 11$ and $q = 19$. Thus $n = 11 \cdot 19 = 209$. To choose a value of e, take $(p-1)(q-1) = (11-1)(19-1) = 180$ and thus find a number relatively prime to 180. Notice $gcd(13, 180) = 1$ and thus by the definition of relatively prime these two integers are relatively prime so we can set $e = 13$. To get the ciphertext, we compute

$$\begin{aligned} c &\equiv m^e \bmod n \\ &\equiv 48^{13} \bmod 209 \\ &\equiv 108 \bmod 209 \end{aligned}$$

and our encrypted message is now the value of 108.

Note: these values are typically very large but for the purpose of the example smaller values were used.

RSA Decryption Formula

If c is the ciphertext, d is the **private exponent**, and n is the product of two primes, then

$$m \equiv c^d \bmod n$$

gives the original message m.

To compute the private exponent d, which is the private key and is only known to the decryption user, is by finding the inverse of the public key e in modulo $(p-1)(q-1)$. The way the public and private key interact is by how the public key is know to everyone and the private key is only known to a specific user. Thus, when sending a message, a user encrypts

it using the recipient's public key so the recipient who can decode it with their private key can access the message[3].

Example 2
Using the Example 1's ciphertext value, we are going to recompute the original message. Calculating the inverse of 13 mod 180, it is found that the inverse is 97, thus the value of d is 97. Using the decryption formula,

$$\begin{aligned} m &\equiv c^d \bmod n \\ &\equiv 108^{97} \bmod 209 \\ &\equiv 48 \bmod 209 \end{aligned}$$

and thus the original message of $m = 48$ is recovered.

3 Exercises

1. *Exercise 1:* Given two primes $p = 7$ and $q = 17$, the public key $e = 11$(check to make sure this is an appropriate choosing for the public key), and the message to be sent is $m = 56$; calculate the ciphertext c and verify that the message can be recovered.

4 Citations

1. Kaliski, B. (n.d.). The mathematics of the RSA public-key cryptosystem. https://www.nku.edu/ c tensen/the mathematics of the RSA cryptosystem.pdf. Accessed 28 April 2024

2. patrickJMT. (2016, August 26). Cryptography: The math of the public private key of RSA. YouTube. YouTube. https://www.youtube.com/watch?v=mf7x9IiJndY. Accessed 28 April 2024

3. Simplilearn. (2023, February 13). What is RSA algorithm in cryptography?: Simplilearn. Simplilearn.com. Simplilearn. https://www.simplilearn.com/tutorials/cryptography-tutorial/rsa-algorithm. Accessed 29 April 2024