An Introduction to Cryptography

Lainey Watlington

University of California - Santa Barbara

The Beginnings of Cryptography

Cryptography is the study of methods of sending messages in a disguised form so that only the intended recipients can remove the disguise and read the message.

At the most basic level, a **cryptosystem** is the process of converting plaintext to a cyphertext using encryption and subsequently converting that cyphertext back to plaintext using decryption.

One of the earliest cryptosystems was created using **digraphs**, which map two characters in a message to a number. Let us consider the 27 letter alphabet which contains letters A-Z and a blank. Then, given any message, the following digraph can be used as an enciphering function where x and y are two characters which occur in succession in the message:

$$27x + y = C$$

The deciphering function is given by:

$$\begin{cases} C \mod 27 = x \\ C - x = y \end{cases}$$

Most early cryptosystems were based on a similar idea of using a rule, or a **key**, to shift the letters in a message to a different location. The idea was that only the person with the key would be able to decipher the message.

Breaking a Cryptosystem

Cryptosystems were developed in order to help protect sensitive information. In modern times, cryptography is widely used in the field of cybersecurity to protect people's

- passwords
- credit card information
- identity information
- other sensitive forms of data

In an increasingly digital world, cryptosystems have become extremely important in protecting this information.

Cryptanalysis is the science of "breaking" the code of cryptosystems. People do this in order to gain access to data that is not intended for them. This begs the question, "How does one break a cryptosystem?". To do so, one needs two types of information

1. The general nature, or the **structure** of the system
2. The specific choice of certain parameters connected with the given cryptosystem, like the shift parameter, also known as the **enciphering key**

An Example in Python

Let us extend the idea of a digraph to a cryptosystem which enciphers a message of length n from an alphabet of any size. Let N represent the size of the alphabet. Then, the enciphering function will be represented by

$$N^{n-1}x_1 + N^{n-2}x_2 + \cdots + Nx_{n-1} + x_{n-1} = C$$

The Python code for an enciphering transformation of this form is as follows: The deciphering transformation will subtract $C \mod N$ from C n times and update C after each iteration. The Python code for a deciphering transformation of this form is:

Primality and Factorization

Cryptosystems have evolved over time to prevent people from breaking them.

- The easier it is to guess the enciphering key of a cryptosystem, the easier it is to break the cryptosystem.
- So, methods of creating difficult to guess keys were developed

Public Key Cryptography: the enciphering and deciphering algorithms are publicly known, but the enciphering and deciphering keys are concealed. Gaining access to the keys allows you to break the system.

How do we create difficult to guess keys?

- **Factoring primes** is really difficult once we start dealing with very large numbers. So, if we multiply two large primes together, factoring them becomes almost impossible without having access to a key.
- The **discrete logarithm** problem is an idea based on the fact that if we know $y = b^x$, it is extremely difficult to solve for

$$x = \log_b y$$

Fermat Factorization provides a way of "breaking" some public key cryptosystems. If two primes are close enough together, this algorithm allows one to efficiently calculate the two primes that have been multiplied together. This form of factorization is used to break RSA cryptosystems.

The Foundations of Modern Cryptography: Elliptic Curves

Elliptic Curve Cryptography

- An approach to public key cryptography which utilizes elliptic curves over finite fields to create keys.
- It is essentially impossible to find the discrete logarithm of a random element of an elliptic curve with respect to a publicly known base point.
- The larger the elliptic curve, the more secure the cryptosystem is since the discrete logarithm becomes more difficult to compute.

An Elliptic Curve Over the Real Numbers Insert Image

- Elliptic curves over the reals form an abelian group. Thus, if we perform operations on two elements of the curve, we will end up with another element on the curve.

An Elliptic Curve Over the Complex Numbers

- Elliptic curves over the complex numbers form a torus.
- We can think of plotting elements of the curve over the integer lattice and then connecting all of the edges together.

Acknowledgements

Reference Material: "A Course in Number Theory and Cryptography" by Neal Koblitz

Thank you to the UCSB Directed Reading Program and to my mentor Katherine Merkl for making this project possible.