Cryptography and Applications

Hanning Yan
7th Grade
Moravian Academy Middle School

Why did I choose this project?

https://www.britannica.com/topic/code-talker

- I read ***Code Talker*** by Chester Nez and Judith Avila
  - About Navajo Code Talkers
  - Helped the U.S. and the Allies win WWII by encrypting secret messages
- ***The Code Book*** by Simon Singh
  - History of cryptography

So, what is cryptography?

By Merriam-Webster:

cryptography: noun

1. secret writing
2. the enciphering and deciphering of messages in secret code or cipher
3. the computerized encoding and decoding of information

In simpler terms: the practice and study of secure and secret communication, especially in the presence of a third party.

The main topic:

- Cryptography is a big field.
  - Deep, rich history
  - Many ciphers and applications
- I focused on basic ciphers and their applications.
- Then, I implemented one with JavaScript.

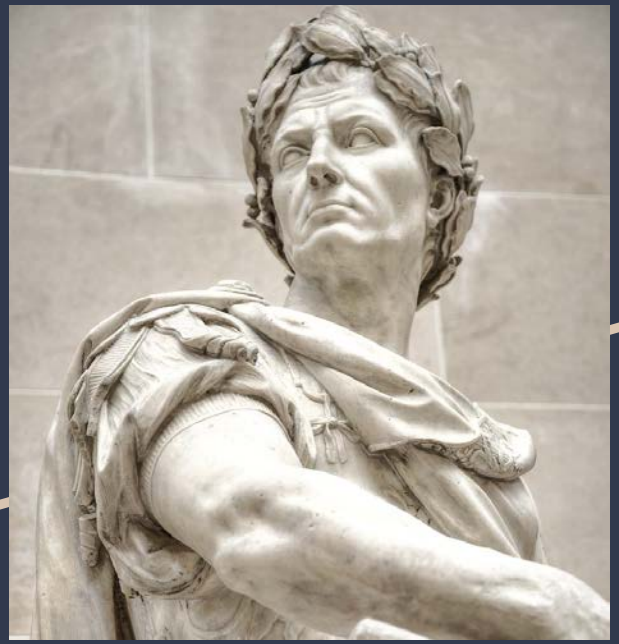
Terminology

- **Plaintext**: the message before encryption
- **Ciphertext**: the message after encryption
- **Encryption**: the process of converting plaintext into ciphertext
- **Decryption**: taking ciphertext and using the key to get plaintext
- **Key**: something that specifies the transformation of plaintext into ciphertext, and vice versa

Classic Ciphers:

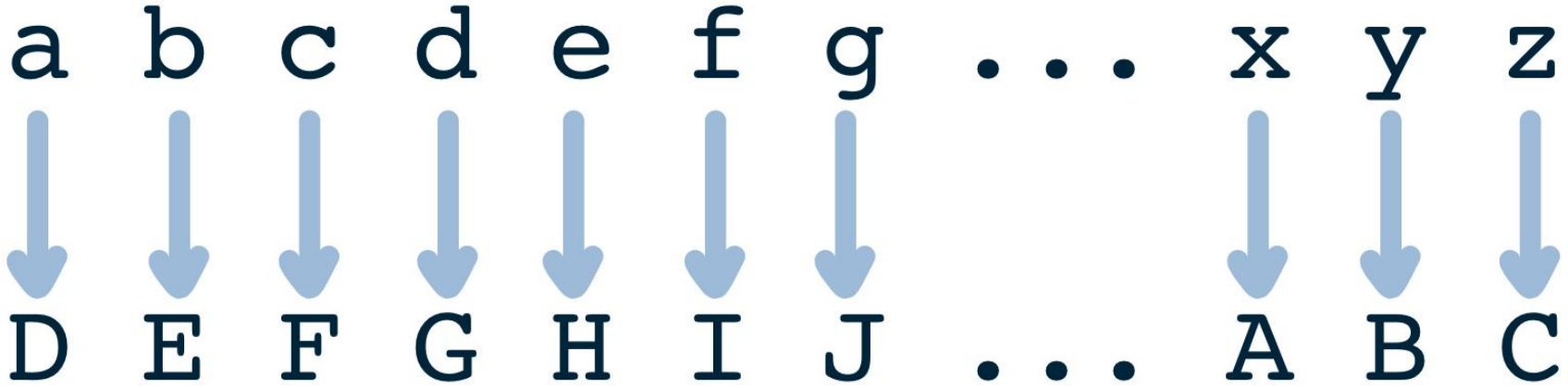
- There are many classic ciphers.
- I chose to focus on three:
  - The Shift Cipher
  - The Affine Cipher
  - The Vigenère Cipher

The Shift Cipher



- Shift ciphers work by shifting each letter in the plaintext by a specified amount of positions, the key being the amount.
- Using a shift key of 3, which is specified as the Caesar Shift Cipher, hello would be encrypted to KHOOR.

plaintext



CIPHERTEXT

Representation of Alphabet

- The letters of the alphabet need mathematical representation.
- The integers 0-25 are used to represent the letters a—z respectively.
- The arithmetic operations are modulo, or mod, 26 so that the results are all letters.

- x: a plaintext letter, y: a ciphertext letter, n: the key
- The encryption is:

$$y = e(x) = (x + n) \bmod 26$$

- The decryption is:

$$x = d(y) = (y - n) \bmod 26$$

- Example: x = 7 (h), n = 3, y = (7 + 3) mod 26 = 10 (K)

The Affine Cipher

- The Shift Cipher is like a shift.
- The Affine Cipher is like a linear function.

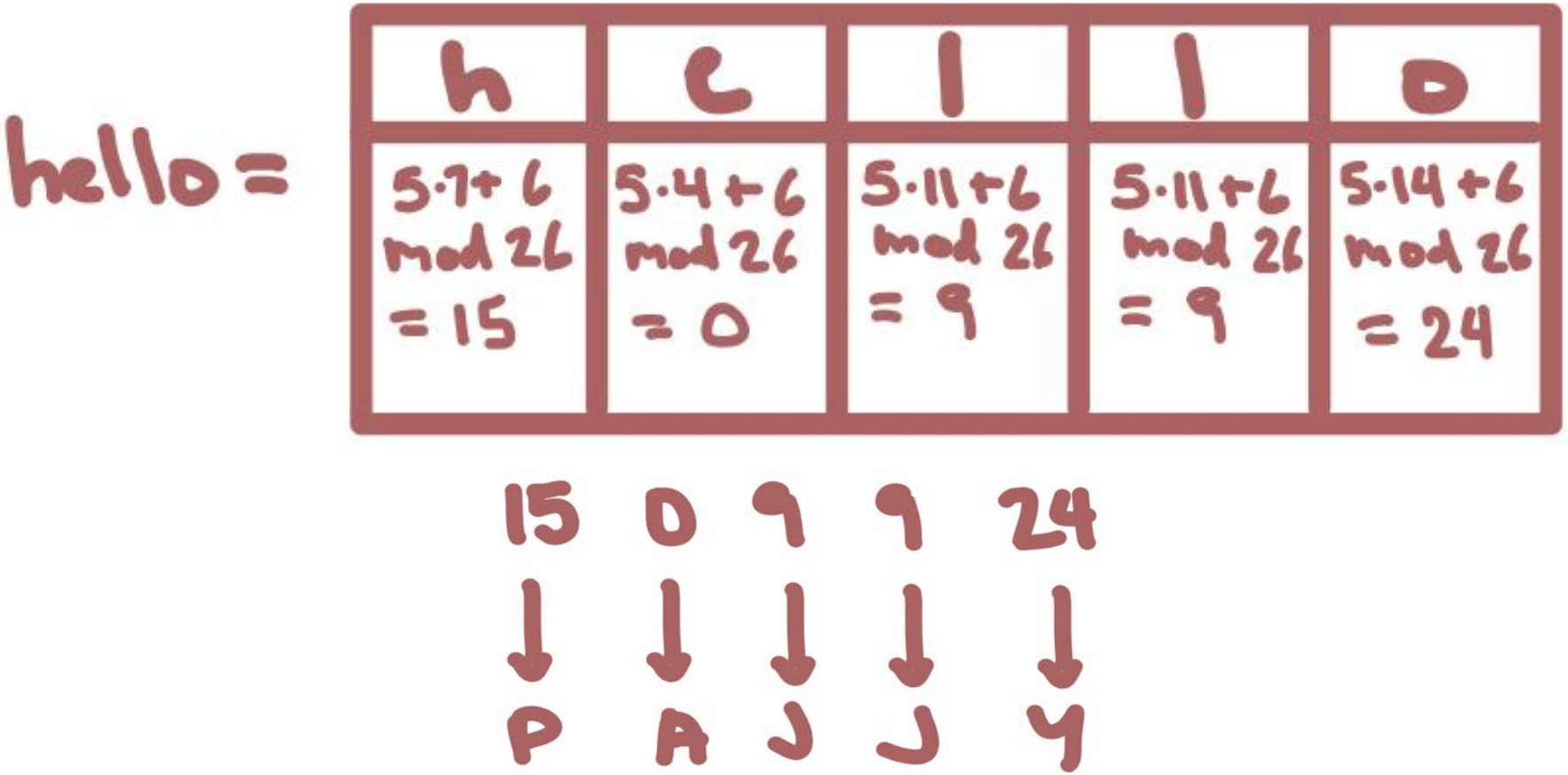
- The encryption function is:

  $y = e(x) = (ax+b) \bmod 26$, where (a, b) is the key and a and 26 are co-prime.

- The decryption function is:

  $x = d(y) = (a^{-1})(y - b) \bmod 26$,
  where a^{-1} is the modular inverse of a.

- Example: $a = 3$, so $a^{-1} = 9$, since $3 \times 9 = 1 \bmod 26$



Affine Cipher Example

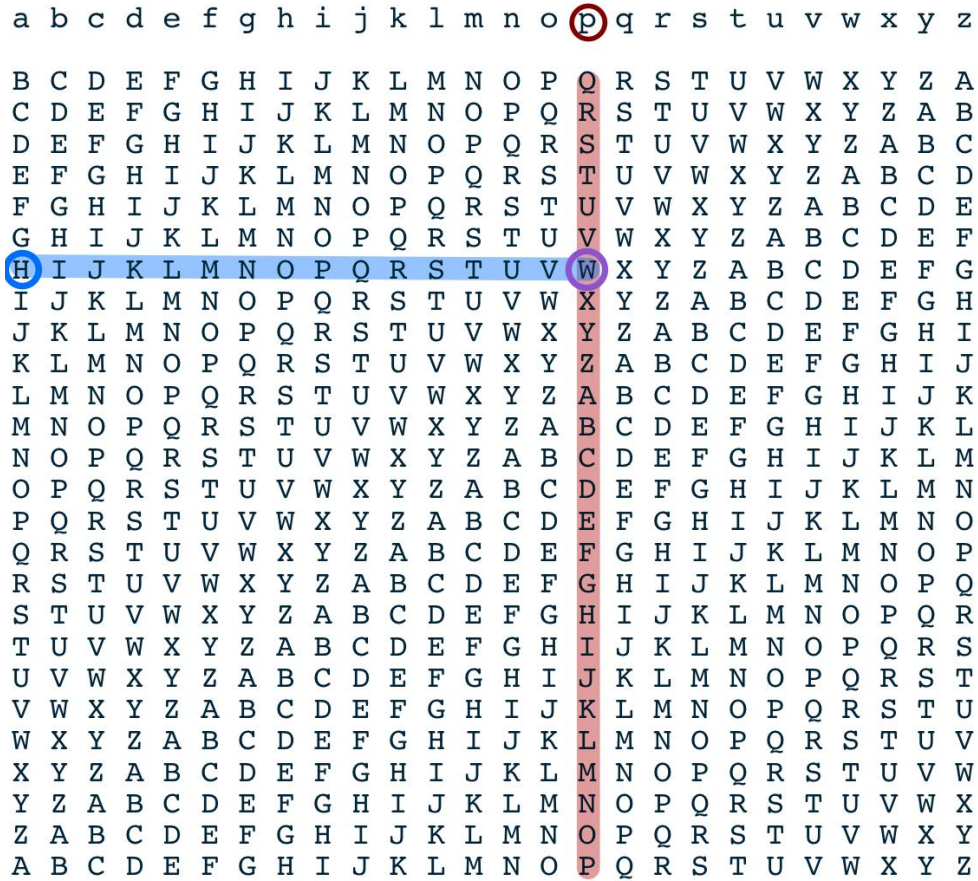
The Vigenère Cipher

- In the Affine Cipher, all l's are encrypted to J.
- Same with the Shift Cipher: all l's are encrypted to O.
- This makes these ciphers vulnerable to frequency analysis.
- In the Vigenère Cipher, mapping depends on position of the plaintext letter in the message.

The Vigenère Cipher: History

Photo in public domain in U.S.

- Before the Vigenère Cipher, most ciphers were **monoalphabetic**: they only used one alphabet.
- Blaise de Vigenère was a French diplomat born in 1523, and he built on the ideas of others to create a new cipher using 27 alphabets and a keyword.
- The 1st alphabet is referred to as the plain alphabet, and the next 26 are alphabets with shifts of keys increasing in increments of 1.



keyword: p j a s p
plaintext: h e l l o
ciphertext: W N L D D

Vigenère Cipher Example

Implementation

- I picked the Shift Cipher, and used JavaScript, a coding language, to implement it.

```java
import java.util.*;
public class CaesarShiftCipher {
    public static void main(String args[]) {
        Scanner cs = new Scanner(System.in);
        System.out.println(" Input the plaintext message : ");
        String plaintext = cs.nextLine();
        System.out.println(" Enter the number of positions being shifted: ");
        int shift = cs.nextInt();
        String ciphertext = "";
        char alphabet;
        for(int i=0; i < plaintext.length();i++)
        {
            // Shift one character at a time
            alphabet = plaintext.charAt(i);

            // if alphabet lies between a and z
            if(alphabet >= 'a' && alphabet <= 'z')
            {
             // shift alphabet
             alphabet = (char) (alphabet + shift);
             // if shift alphabet greater than 'z'
             if(alphabet > 'z') {
                // reshift to starting position
```

Input: plaintext and key
Output: ciphertext

EX. Input: HELLO, 3
Output: KHOOR

```
24                alphabet = (char) (alphabet+'a'-'z'-1);
25               }
26               ciphertext = ciphertext + alphabet;
27              }
28
29              // if alphabet is between 'A'and 'Z'
30              else if(alphabet >= 'A' && alphabet <= 'Z') {
31               // shift alphabet
32               alphabet = (char) (alphabet + shift);
33
34               // if shift alphabet is greater than 'Z'
35               if(alphabet > 'Z') {
36                   //reshift to starting position
37                   alphabet = (char) (alphabet+'A'-'Z'-1);
38               }
39               ciphertext = ciphertext + alphabet;
40              }
41              else {
42               ciphertext = ciphertext + alphabet;
43              }
44
45      }
46      System.out.println(" ciphertext : " + ciphertext);
47    }
48  }
```

Private Key vs. Public Key

- Ciphers seen above are private key

.

Private key cryptography:

- Two communicating parties know and use one secret key.

Public key cryptography:

- Uses two keys, one public and the other private.
- Public key is made public and used to encrypt.
- Private key is known to recipient and used to decrypt.

So, Why Public Key?

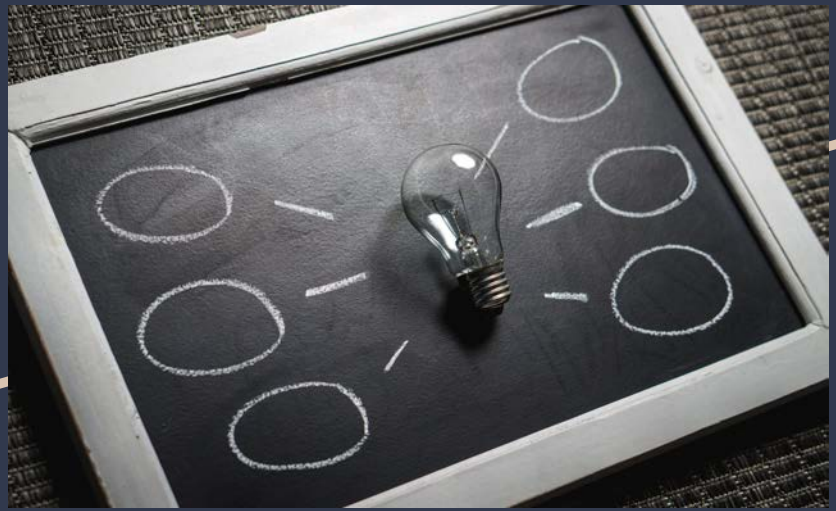
- You need a secure channel to transmit the private key.
- This becomes infeasible in many situations.
  - Sometimes there is no secure channel to transmit key information.
  - Other times, many people want to communicate, and so many keys are hard to keep track of.
- In these instances, public key is used.

RSA: Rivest, Shamir, and Adleman

Photo from https://www.usc.edu

- These three men are Ron Rivest, Adi Shamir, and Leonard Adleman.
- They invented RSA, one of the first and most well-known forms of public key cryptography.
- RSA works by taking advantage of the immense difficulty of factoring large numbers.
- The public key, belonging to the recipient, is based on 2 large primes.
- The primes are the secret key.

What I Learned + What Should I Do Next?



I learned about:

1. Different ciphers and applications
2. Terminology

I plan to expand my code to implement other ciphers.

Bibliography

Works Cited

Koblitz, Neal. A Course in Number Theory and Cryptography. 2nd ed., New York, Springer-Verlag, 2012.

Menezes, A. J., et al. Handbook of Applied Cryptography. 5th ed., Boca Ratón, CRC Press, 2001.

Paterson, Maura B., and Douglas R. Stinson. Cryptography. 4th ed., Boca Raton, CRC Press, 2019.

Singh, Simon. The Code Book. New York, Doubleday, 1999.

Nez, Chester, and Judith Schiess Avila. Code Talker. New York, Dutton Caliber, 2018.

Stock Images from www.Pexels.com: photos from other sources have captions.

Thank you!

Thank you to:

- My dad, for suggesting the topic and helping me understand concepts.
- My advisor Mrs. Daniels: she put up with all my questions and gave me good advice.