Cryptography and Applications

Hanning Yan
7th Grade
Moravian Academy Middle School
Why did I choose this project?

- 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

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

plaintext

a b c d e f g ... x y z

CIPHERTEXT

D E F G H I J ... A B C
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:

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

The decryption is:

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

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:

\[ y = e(x) = (ax+b) \mod 26, \text{ where } (a, b) \text{ is the key and } a \text{ and } 26 \text{ are co-prime.} \]

● The decryption function is:

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

● Example: \( a = 3 \), so \( a^{-1} = 9 \), since \( 3 \times 9 = 1 \mod 26 \)
**Affine Cipher Example**

<p>| | | | | |</p>
<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>h</td>
<td>c</td>
<td>I</td>
<td>I</td>
<td>0</td>
</tr>
<tr>
<td>5·7 + 6 mod 26 = 15</td>
<td>5·4 + 6 mod 26 = 0</td>
<td>5·11 + 6 mod 26 = 9</td>
<td>5·11 + 6 mod 26 = 9</td>
<td>5·14 + 6 mod 26 = 24</td>
</tr>
</tbody>
</table>

hello =

15 0 9 9 24

↓ ↓ ↓ ↓ ↓

P A J J Y
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

- 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.
### Vigenère Cipher Example

| a | b | c | d | e | f | g | h | i | j | k | l | m | n | o | p | q | r | s | t | u | v | w | x | y | z |
| B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A |
| C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B |
| D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C |
| E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D |
| F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E |
| G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F |
| H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G |
| I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H |
| J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I |
| K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J |
| L | M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K |
| M | N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L |
| N | O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M |
| O | P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N |
| P | Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O |
| Q | R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P |
| R | S | T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q |
| T | U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S |
| U | V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T |
| V | W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U |
| W | X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V |
| X | Y | Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W |
| Z | A | B | C | D | E | F | G | H | I | J | K | L | M | N | O | P | Q | R | S | T | U | V | W | X | Y |

**Keyword:** p j a s p  
**Plaintext:** hello  
**Ciphertext:** W N L D D
Implementation

- I picked the Shift Cipher, and used JavaScript, a coding language, to implement it.
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
                    alphabet = (char) (alphabet - 26);
                }
            }
            ciphertext += alphabet;
        }
        System.out.println("Output: " + ciphertext);
    }
}
alphabet = (char) (alphabet+'a'-'z'-1);
}
ciphertext = ciphertext + alphabet;

// if alphabet is between 'A' and 'Z'
else if(alphabet >= 'A' && alphabet <= 'Z') {
    // shift alphabet
    alphabet = (char) (alphabet + shift);

    // if shift alphabet is greater than 'Z'
    if(alphabet > 'Z') {
        // reshift to starting position
        alphabet = (char) (alphabet+'A'-'Z'-1);
    }
ciphertext = ciphertext + alphabet;
}
else {
    ciphertext = ciphertext + alphabet;
}
}
System.out.println(" ciphertext : " + ciphertext);
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

- 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


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