Classical Cryptography

By: Erick Barron

Introduction

- My topic is Classical Cryptography from chapter 4.6.2 in the textbook
- I will explain Classical Cryptography and some history and current use.
- This topic was interesting to me because I like code breaking and hacking so cryptography has always been interesting

Background

- What is Cryptography?
  - Crypt means hidden and graphy means writing. So we can see it is hidden writing more specifically in our case it is transforming information so as to not be recoverable without secret knowledge such as a passcode.
- Classical cryptography is the old methods used vs current cryptography which is more of an algorithmic approach and more advanced.
- Earliest known uses
  - Although the use of cryptography has been know earlier and may have been used before we will focus on the first use of the Caesar Cipher who Julius Caesar, the famous Roman general, is the eponym.
  - It is said that this is the most famous classical cipher.

Relevance in Discrete Mathematics

- What is Discrete Mathematics
  - “Discrete mathematics is the part of mathematics devoted to the study of discrete objects. (Here discrete means consisting of distinct or unconnected elements.)”
- Why study Discrete Mathematics?
  - Develop math maturity, gateway to more advanced courses, tests previous knowledge, boost creativity, learn to read and write proofs. All skills to improve yourself.
- Relevance of Cryptography in Discrete Mathematics
  - We know number theory is the basis of many ciphers and is a branch of mathematics and the numbers used for transforming the letters are distinct and unconnected elements.

Encryption Formulas

To express Caesar's encryption process mathematically, first replace each letter by an element of $\mathbf{Z}_{26}$, that is, an integer from 0 to 25 equal to one less than its position in the alphabet. For example, replace A by 0, K by 10, and Z by 25. Caesar's encryption method can be represented by the function f that assigns to the nonnegative integer p, $p \leq 25$, the integer $f(p)$ in the set $\{0, 1, 2, \ldots, 25\}$ with

$$f(p) = (p + 3) \bmod 26.$$

We can generalize shift ciphers further to slightly enhance security by using a function of the form

$$f(p) = (ap + b) \bmod 26,$$

where a and b are integers, chosen so that f is a bijection. (The function $f(p) = (ap + b) \bmod 26$ is a bijection if and only if $\gcd(a, 26) = 1$.) Such a mapping is called an *affine transformation*, and the resulting cipher is called an *affine cipher*.

Examples of Encryption

Encrypt “MEET YOU IN THE PARK” with encryption formula

Replace letters into corresponding number
12 4 4 19 _ 24 14 20 _ 8 13 _ 19 7 4 _ 15 0 17 10.

Input numbers for p in f(p) = (p+3) mod 26
15 7 7 22 _ 1 17 23 _ 11 16 _ 22 10 7 _ 18 3 20 13.

Finally decode with corresponding letter
“PHHW BRX LQ WKH SDUN”

Note: Letter a starts at 0

Example-Encryption + Security

For this we use affine transformation

Given f(7p+3)mod 26 which is what the book uses we will encrypt and decrypt the letter B.

f(p)=(ap+b)mod 26 so, f(1) = (7(1)+3) mod 26 =10

To decrypt we reverse engineer it

We have f=10 =ap+b so, (10-3)/7 =x

Ultimately x=1 which is correct

Decryption Formula

To recover the original message from a secret message encrypted by the Caesar cipher, the function f^{-1}, the inverse of f, is used. Note that the function f^{-1} sends an integer p from $\mathbf{Z}_{26}$, to $f^{-1}(p) = (p - 3)$ **mod** 26. In other words, to find the original message, each letter is shifted back three letters in the alphabet, with the first three letters sent to the last three letters of the alphabet. The process of determining the original message from the encrypted message is called **decryption**.

There are various ways to generalize the Caesar cipher. For example, instead of shifting the numerical equivalent of each letter by 3, we can shift the numerical equivalent of each letter by k, so that

$$f(p) = (p + k) \textbf{ mod } 26.$$

Such a cipher is called a *shift cipher*. Note that decryption can be carried out using

$$f^{-1}(p) = (p - k) \textbf{ mod } 26.$$

Here the integer k is called a **key**. We illustrate the use of a shift cipher in Examples 2 and 3.

Example of decryption

For this we will decrypt “PHHW BRX LQ WKH SDUN” from example for encryption.

Reverse process using f^-1(p) = (p-k) mod 26 since we know the key k will be 3

Change letters to numbers
15 7 7 22 _ 1 17 23 _ 11 16 _ 22 10 7 _ 18 3 20 13.

Input numbers into formula and get 12 4 4 19 _ 24 14 20 _ 8 13 _ 19 7 4 _ 15 0 17 10.

Decode to corresponding letters “MEET YOU IN THE PARK

Block Ciphers

Shift and affine ciphers are called character or monoalphabetic ciphers due to the replacement of letters and numbers. However chunking into block gives us more security and are called block ciphers.

We will now introduce a simple type of block cipher, called the **transposition cipher**. As a key we use a permutation σ of the set $\{1, 2, \ldots, m\}$ for some positive integer m, that is, a one-to-one function from $\{1, 2, \ldots, m\}$ to itself. To encrypt a message we first split its letters into blocks of size m. (If the number of letters in the message is not divisible by m we add some random letters at the end to fill out the final block.) We encrypt the block $p_1 p_2 \ldots p_m$ as $c_1 c_2 \ldots c_m = p_{\sigma(1)} p_{\sigma(2)} \cdots, p_{\sigma(m)}$. To decrypt a ciphertext block $c_1 c_2 \ldots c_m$, we transpose its letters using the permutation σ^{-1}, the inverse of σ. Example 6 illustrates encryption and decryption for a transposition cipher.

Using the transposition cipher based on the permutation σ of the set $\{1, 2, 3, 4\}$ with $\sigma(1) = 3$, $\sigma(2) = 1$, $\sigma(3) = 4$, and $\sigma(4) = 2$,

Solution: (a) We first split the letters of the plaintext into blocks of four letters. We obtain PIRA TEAT TACK. To encrypt each block, we send the first letter to the third position, the second letter to the first position, the third letter to the fourth position, and the fourth letter to the second position. We obtain IAPR ETTA AKTC.

(b) We note that σ^{-1}, the inverse of σ, sends 1 to 2, sends 2 to 4, sends 3 to 1, and sends 4 to 3. Applying $\sigma^{-1}(m)$ to each block gives us the plaintext: USEW ATER HOSE. (Grouping together these letters to form common words, we surmise that the plaintext is USE WATER HOSE.) ◀

Cryptosystems

CRYPTOSYSTEMS We have defined two families of ciphers: shift ciphers and affine ciphers. We now introduce the notion of a cryptosystem, which provides a general structure for defining new families of ciphers.

A *cryptosystem* is a five-tuple $(\mathcal{P}, \mathcal{C}, \mathcal{K}, \mathcal{E}, \mathcal{D})$, where $\mathcal{P}$ is the set of plaintext strings, $\mathcal{C}$ is the set of ciphertext strings, $\mathcal{K}$ is the *keyspace* (the set of all possible keys), $\mathcal{E}$ is the set of encryption functions, and $\mathcal{D}$ is the set of decryption functions. We denote by E_k the encryption function in $\mathcal{E}$ corresponding to the key k and D_k the decryption function in $\mathcal{D}$ that decrypts ciphertext that was encrypted using E_k, that is, $D_k(E_k(p)) = p$, for all plaintext strings p.

A way to structure a cipher

Use Cases

- Used in many cases we will focus on cases for CS my major, but could be used in many professions
- For my coding project I created a program which can encrypt and decrypt messages using the formulas provided, this can be upscaled for more experienced programmers to encrypt many ciphers.
- Used heavily in the security sector including for passwords, security of web pages, data encryption, and hashes.
- Quantum computing rapidly developing will weaken Cryptography, but new methods in the quantum realm will see cryptography including classical cryptography used.

Conclusion

- I hope you found this information as interesting and helpful as I have
- Any questions message me on canvas or comment of discussion
- If you are into security I urge you to continue to learn about cryptography
- Have a GREAT DAY!