LE/EECS 4161: Caesar Cipher Presentation Outline and Bibliography Submission

S.Toyonaga

February 28, 2022

Contents

Abstract

A brief pitch on why you should want to learn about the Caesar Cipher will first be addressed. Special attention will be emphasized on how the cipher influenced and thus affected the proceeding cipher systems. Vigenere is one such example. Secondly, an introduction to how the cipher works, as well as some prerequisite mathematical concepts will be covered in order to understand the underlying concepts and empirically critique the system. Thirdly, the ciphers historical and technical applications will be addressed in depth. A brief discussion on the events leading up to the necessary conception of the Caesar cipher is addressed in relation to some very interesting applications of it through many generations of war and technology. Particular focus will be put on the Caesar Ciphers application by Julius Caesar, Bernardo Provenzano, Al-Kindi, the Enigma Machine, and the ROT-13 algorithm. Fourthly, a brief illustration of how to crack the Caesar Cipher given its weakness for frequency analysis will be covered. Lastly, a holisitic evaluation on the cipher will be addressed, discovering what all its weaknesses are, how they were discovered, and what makes the cipher feasible or not in today's society. The underlying principle to determine the ciphers utility is in relation to Kerckhoff's Principle.

Chapter 1

Outline of the Story

1.1 The Pitch [≈ 2 *Minutes*]

Before we go too far into the theory, one should ask, "Why should I care to learn about this cipher?" After all, the Caesar Cipher is one of the earliest cryptographic systems to date [2]. This means that it must have been cracked by now, thus having no practical uses, right?

I will certainly concede that the cipher has been cracked long ago, and is not used too much in modern day technology. However, one should still learn about the past predecessors of cryptographic systems to learn about where the particular pitfalls were, and how they were discovered.

This kind of knowledge of the strengths of past ciphers, as well as their discovered weaknesses will help one develop their own cryptographic system free of such flaws. It will also help a future cryptographer become a more well-rounded, critical thinker capable of both building systems that hide common code breaking practices, and breaking unknown ciphers.

I will leave you with a quote to hopefully convince you that learning about the past is just as important as keeping up to date with modern cryptography.

"Those who cannot remember the past are condemned to repeat it."

– George Santayana

1.2 Mathematical Background [≈ 2 *Minutes*]

The Caesar Cipher is a monoalphabetic substitution cipher. Each letter in the plaintext is mapped to another letter which is shifted n positions down the alphabet. There is a wrap-around on the alphabet, meaning that in total, there are 26 (K=1..26) possible keys to use when encrypting and decrypting inputs. However, realistically, there are only 25 such practical keys, since K=26 would do a complete wrap-around, leaving the plaintext and ciphertext as identical.

By mapping the alphabet in the following manner where A=0, B=1,to Z=25, encrypting and decrypting via the Caesar cipher with a key can trivially be implemented through the following formulas. Using modular arithmetic to implement the alphabet wraparound is the key to understanding this implementation.

$$Encryption = (Plaintext_i + k)\%26$$

$$Decryption = (Ciphertext_i - k)\%26$$

1.3 Historical Applications [≈ 5 *Minutes*]

As has previously been written, the Caesar cipher is one of the first cryptographic systems of its time [2, 4]. In fact, it came as a solution to a previous way in which the Greeks used to send secret messages [10]. Prior to this, steganography was the main use of information obfuscation. Using the predecessor method, the messengers would initially shave a slave's head [10]. After writing a message on it, they would wait for the hair to grow back, obfuscating the plaintext message. The slave would then be sent off with the message to be read, by having their head reshaved in front of the message receiver [10]. You can see why the Caesar Cipher was necessary, to replace such a risky method of communication.

Although the system is named after Julius Caesar, it is debated whether he is the original creator [1]. In the early days, Caesar used this cryptographic system to send private letters to friends and highly ranking officials on the battlefield [1, 4] As early as 50 B.C., it has been documented that the Caesar Cipher was used by Julius to write a letter to Marcus Cicero.

The original system had an implicit key assumption that K=3, so little communication between the writer of the ciphertext and receiver was necessary. During the lifetime of the Cipher, it was extremely powerful. Many people were illiterate, meaning that even if the ciphertext was somehow intercepted, it would be no use to the enemy even if they somehow managed to obtain the key.

Interestingly enough, it took almost 800 years since the conception of the Caesar cipher for its weakness to become noticeable. It was cracked by the mathematician, Al-Kindi, by observing frequency analysis [5, 6]. It was discovered that by analyzing the frequency of characters that appear in the ciphertext, one could use properties of the language in relation to the plaintext to determine the key [5, 6]. By comparing the most frequently appearing characters in the ciphertext with the most common characters in the plaintext language, shifts could be "guessed" quite easily. For example, in English, such commonly frequently appearing characters are A, E, O, T, and so on.

Firstly, there were instances of the Caesar Cipher being used in newspapers in the 19th century [5]. To be specific, it was applied to regions in the advertisement sections, most likely because few people go out of their way to look at this information, thus secrecy was maintained. Lovers would occasionally use this tactic to exchange messages as well, through newspapers [5].

Secondly, in 1915, the applications of the Caesar Cipher were still present. The Russian army was using it to communicate between each other [5]. Although, their opponents were easily able to break the cipher, for reasons that were previously discussed [5].

Thirdly, and most notably, a variant of the Caesar Cipher, with its original key (k=3) was used by an Italian Mobster, Bernardo Provenzano [12]. After encrypting his plaintext, he would replace the ciphertext characters with their indexed position in the English alphabet. The critical part that the Caesar Cipher played in this Mafioso's connection to the authorities was that this was their only connection to him. This was their only evidence that he was even alive [12]. Bernardo Provenzano had successfully avoided many attempts of capture, being a fugitive from 1963 to his eventual capture in 2006 [12]. He never communicated through telephone, only through his Caesar Cipher variant, delivered through

small handwritten ciphertext on scrap paper [12].

Lastly, one application where the ideologies that are seen to originate from the Caesar Cipher can be seen in the Enigma machine. It uses a much more complex substitution cipher with multiple rounds of re-mapping using rotors [11]. This particular machine was used by the Nazi's during the war to encrypt their secret messages [11].

1.4 Technical Applications [≈ 1.5 *Minutes*]

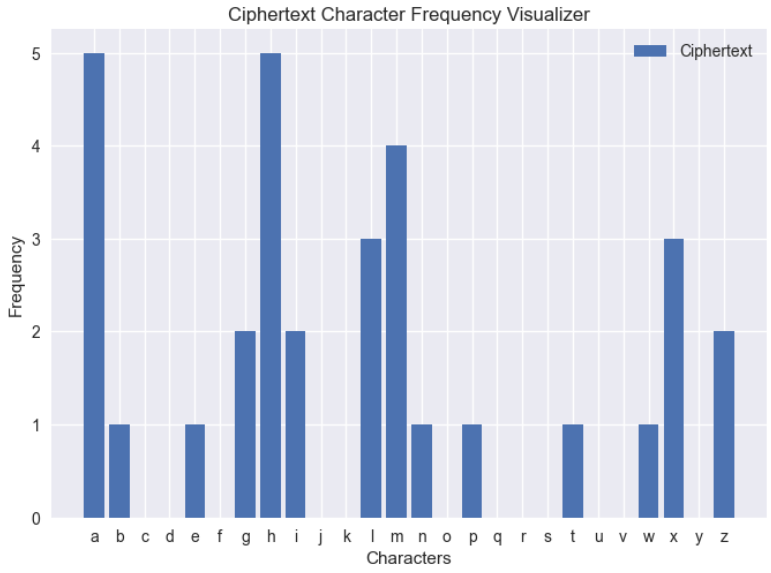
Lastly, with regards to modern day usages, one can still see the Caesar cipher deployed by the ROT13 system [5]. This system is used on blogs, forums, and discussion boards to hide spoilers. The reason that it uses a K=13, is because on each (even) successive application of the key, you are decrypting the ciphertext. On each (odd) successive application of the key, you are also encrypting. This makes for a highly convenient form of hiding spoilers, and making it very easy to crack as well [5].

1.5 Technical Demo: Cracking the Caesar Cipher [≈ 4 *Minutes*]

A demo of the Caesar cipher in the encryption and decryption process will be illustrated, using some python programs. As a disclaimer, the plaintext and ciphertext used were from the first assignment.

Say that we obtain the following Ciphertext from intercepting a Leaders' message: "ZHHWM ABGZL ATIIX GMHMA HLXPA HANLM EX"

To crack the key, we generate a graph illustrating the frequency of the ciphertext characters. We get:



We then take the most frequently-occurring ciphertext characters and try to map the key to the corresponding characters that occur the most in our plaintext language. We will try mapping as follows:

- $A \rightarrow E$ will produce the plaintext, "vddsi wxcvh wpeet cidiw dhtlw dwjhi at"
- $A \rightarrow T$ will produce the plaintext, "goodt hings happe ntoth osewh ohust le"

Thus, we see that the plaintext for K = 19 is, "Good things happen to those who hustle.

1.6 Critical Overview [≈ 5 *Minutes*]

In evaluating the Caesar cipher, it is deemed to be inadequate in today's society for serious, military use. By evaluating the cipher using Kerckhoff's principle [9], it falls short in providing adequate protection against adversaries that obtain the ciphertext, or the system. We will quickly go through each of the rules and determine whether the Caesar cipher adheres to or violates it.

1. The system must be practically, if not mathematically, indecipherable;
    - Well, we can see here that it's clearly false. The discovery and applications of frequency analysis have proven to be quite detrimental to the ciphers ability to be indecipherable.
2. It should not require secrecy, and it should not be a problem if it falls into enemy hands;
    - Again, the cipher does not adhere to this rule due to frequency analysis. If the ciphertext falls into the enemy hands, it can easily be cracked by brute force methods.
3. It must be possible to communicate and remember the key without using written notes, and correspondents must be able to change or modify it at will;
    - This does adhere to the Caesar cipher. The key is extremely simple to remember, especially if we use the original system which assumed that k=3. Changing it at will is also not a problem either, since one could easily determine the key through trial and error for k.
4. It must be applicable to telegraph communications;
    - This does adhere to the Caesar cipher. Especially if we convert the ciphertext into its numerical form.
5. It must be portable, and should not require several persons to handle or operate;
    - This cipher is very portable, and does not require more than one person to handle or operate it. In fact, by the creation of the Caesar wheel, we see that this cipher adheres to the rule.

6. Given the circumstances in which it is to be used, the system must be easy to use and should not be stressful to use or require its user to know and comply with a long list of rules.

    - This does adhere to the cipher, since it's a monoalphabetic substitution cipher. It's also not stressful to use either due to its innate simplicity.

Given the modern-day evaluation of the Caesar cipher, it's easy to dismiss it as useless. However, it is very important to remember why this cipher was so successful and useful for hundreds of years prior to frequency analysis. Back in its historical use, even if people obtained their hands on the ciphertext, a large majority of people were illiterate. No matter what, the ciphertext would remain indecipherable.

Even in the worst-case scenario, if someone were able to crack the ciphertext to a long document, by the time they had figured out the key and decrypted everything, the information would most likely be useless. This applies to the principle of timeliness. The cipher would be able to keep the adversary busy for long enough such that by the time the plaintext is discovered, its information is not useful in any capacity.

This is to say that at its time of usage, the cipher did adhere to the most important parts of Kerckhoff's principle. Like many past ciphers, they were useful for their lifetime, prior to Kerckhoff's first two design principles being broken. As our ability to become more creative and analyze ciphers more thoroughly increases, many of our past predecessor cipher systems will become obsolete.

1.7 Bibliography

[1] J. Holden, "Chapter 1: Introduction to Ciphers and Substitution," in The Mathematics of Secrets: Cryptography from caesar ciphers to Digital Encryption, Princeton, NJ, New Jersey: Princeton University Press, 2019, pp. 1–29.

[2] D. Luciano and G. Prichett, "Cryptology: From caesar ciphers to public-key cryptosystems," The College Mathematics Journal, vol. 18, no. 1, pp. 2–17, 1987.

[3] A. Jain, R. Dedhia, and A. Patil, "Enhancing the security of caesar cipher substitution method using a randomized approach for more secure communication," International Journal of Computer Applications, vol. 129, no. 13, pp. 6–11, Nov. 2015.

[4] T̈he story of Cryptography: History,T̈he Story of Cryptography : Historical Cryptography. [Online].
Available : *https* : *//ghostvolt.com/articles/cryptography*$_h$*istory.html.*
[*Accessed* : 01 − *Feb* − 2022].

[5] Caesar cipher. [Online].
Available : *https* : *//www.cs.mcgill.ca/ rwest/wikispeedia/wpcd/wp/c/Caesar*$_C$*ipher.htm.*
[*Accessed* : 01 − *Feb* − 2022].

[6] The Caesar cipher | Journey into cryptography | Computer Science | Khan Academy. YouTube, 2012.

[7] F. C. Piper and S. Murphy, "Chapter 3: Historical Algorithms, Simple Examples," in Cryptography: A very short introduction, Oxford, Mississippi: Oxford University Press, 2002, pp. 18–32.

[8] S. Sutherland and S. R. Simanca, "Simple Ciphers," Simple ciphers. [Online].
Available : *http* : *//www.math.stonybrook.edu/ scott/papers/Book*331/*Simple*$_C$*iphers.html*
[*Accessed* : 01 − *Feb* − 2022].

[9] "Kerckhoffs's principle," Wikipedia, 21-Nov-2021. [Online].
Available : *https* : *//en.wikipedia.org/wiki/Kerckhoffs*%27*s*$_p$*rinciple.*
[*Accessed* : 08 − *Feb* − 2022].

[10] R. F. Churchhouse, Codes and ciphers: Julius Caesar, the Enigma, and the internet. Cambridge, Massachusetts: Cambridge University Press, 2002.

[11] CrashCourse, "Cryptography: Crash course computer science #33 - YouTube," YouTube, 25-Oct-2017. [Online].
Available : *https* : *//www.youtube.com/watch?v* = *jhXCTbFnK8o.*
[*Accessed* : 11 − *Feb* − 2022].

[12] "Bernardo Provenzano," Wikipedia, 05-Feb-2022. [Online].
Available : *https* : *//en.wikipedia.org/wiki/Bernardo*$_P$*rovenzano.*
[*Accessed* : 11 − *Feb* − 2022].