Levi Seibert

lseiber1@my.athens.edu

ITE 523

Dr. Yahia Fadlalla

Monoalphabetic and Polyalphabetic Ciphers

Cryptography is the process of encoding messages into some type of ciphertext and then decoding them back into the plaintext. There are many methods of encryption and several categories of ciphers are available, including substitution and transposition ciphers, as well as symmetric and asymmetric key encryption [1]. Within each of these "genres" of cryptography, there are sub-genres. Monoalphabetic and polyalphabetic ciphers, for example, are two means of substitution ciphers. A substitution cipher is a cipher that exchanges data from a plaintext for data from a ciphertext, using some selected algorithm. The number of characters will remain the same; there will be some sort of "shifting" of letters that is going on (this can be observed most easily in the Caesar Cipher, described below) [2].

An important concept in substitution ciphers is that of assigning numerical values to letters for mathematical operations. One such operation that is used frequently in monoalphabetic and polyalphabetic ciphers is that of the modulus. Because the alphabet itself is being manipulated (shifted, for example), there has to be a way of creating a "wrap-around". This means that our alphabet will be 'A B C … Z' followed by 'A B C … Z', on for infinity, so that we are not constrained by only having 26 positions to work with. The modulus operator takes two values and divides them. The quotient is discarded and the remainder becomes the output of the operation.

Monoalphabetic ciphers use a single alphabet (mono means one or alone in Greek) for its key. In monoalphabetic cryptography, only a single alphabet is considered when encrypting a plaintext. A common example of a monoalphabetic cipher is the Caesar Cipher, which takes a normal alphabet and shifts all letters by a set number of units (typically 3). 'A' would become 'D', 'B' would become 'E', and so on. This methodology is obviously weak, and in today's cryptographic culture, has little to no purpose, except for historical reference. The algorithm is simple, so it does serve as an easy introductory example to encryption.

Another example of a monoalphabetic cipher that offers very little security is the Atbash cipher. In this algorithm (historically used for encrypting Hebrew messages), there isn't even a real key. Rather, the order of the alphabet is just reversed (so 'A' becomes 'Z', 'B' become 'Y', and so on). While this cipher may have been useful in ancient times, today it is pointless. As long as a cryptographer knows the ciphertext uses the Atbash cipher, he can immediately decrypt the message using a simple table of which ciphertext values correspond to which plaintext values (or just memorize these). This cipher is easy to use, but very weak and immature. That being said, it could definitely be used in combination with another algorithm in order to add a bit more confusion to an encryption process [3].

The monoalphabetic Affine cipher is a much more complex substitution cipher, that while still weaker than polyalphabetic ciphers, does at least some more complexity than the Caesar cipher or the Atbash cipher. For the Affine cipher, there is a key consisting of two

numbers. The first number, often called *a*, must be relatively prime to the number of characters in the source alphabet (26 in English). To encrypt a message, each letter is assigned a numerical value, starting with 'a' as 0, 'b' as 1, and so on. Each of those values are multiplied by the first number in the key (*a*) and added to the second key number (*b*). The result is then modulo-ed with the number of characters in the source alphabet (once again 26 in English). In order to decrypt an Affine-encrypted ciphertext, one would take each ciphertext letter, convert into a number, subtract the second key value (*b*), and then multiply by the multiplicative inverse of *a* (once again modulo the number of characters in the alphabet). The multiplicative inverse is simply the number that when multiplied with *a* produces the value 1 (modulo the number of characters in the alphabet). While it is more complex than the Caesar cipher and the Atbash cipher, the Affine cipher is not secure. If just two characters are known of the plaintext and what they correspond to in the ciphertext, a cryptanalyst can easily deduce the values of *a* and *b*. With frequency analysis (determining which characters appear most often), it becomes trivial to discover the key used for the cipher and thus decrypt the message [4]. Once again, however, as is the case with several other monoalphabetic substitution ciphers, this algorithm can be useful as a part of a larger algorithm and can aid in adding a level of security, but should not be relied upon as the main source of encryption.

Polyalphabetic ciphers use multiple alphabets (poly means many) in order to perform the encryption process. Polyalphabetic ciphers are significantly more complex than monoalphabetic ciphers, and as such, provide for stronger encryption. The most common polyalphabetic cipher is the Vigenère cipher [5]. The Vigenère dates back almost 500 years and was considered unbreakable for around 300 years, but it no longer lives up to such accolades. The key for the Vigenère algorithm is some keyword (the longer the better). A tableau consisting of 26 rows and columns is used to encipher the plaintext. Each row of the tableau is made up of the 26 letters of the English alphabet in a wrap-around format, such that every successive row starts with the next letter of the alphabet. For example, the first row of the tableau consists of 'A B C D …', while the second row consists of 'B C D E …', and so on until 'Z A B C …'. To encrypt a message, you write out the plaintext with the keyword repeated above. For each letter in the plaintext, find its corresponding row from the tableau (the one that begins with that letter). Search across the row until you arrive at the column that matches the corresponding value in the keyword (if the keyword value is a 'C', then we go to the third column, as 'C' is the third letter in the alphabet) [6]. To decrypt a message, one would take the ciphertext with the keyword written above. For each letter in the ciphertext, find the corresponding letter from the keyword, go to that row and determine where the ciphertext value is. Whichever column it is found on is the corresponding plaintext letter. This is a harder algorithm to break; one would likely have to guess either a portion of the plaintext or a portion of the key and use that information to deduce the rest of the algorithm. Frequency analysis can be useful in determining what the key is and where each repeated keyword begins, but it is definitely more secure than any of the monoalphabetic ciphers considered [6].

Another polyalphabetic cipher is the Running Key Cipher, which is very similar to the Vigenère cipher, except that the key is not just a keyword. Rather, it is much longer, long enough that the key never repeats. This is one of the biggest disadvantages with the Vigenère cipher, so it is significantly stronger. Other than how the key is chosen, the algorithm works basically identically to Vigenère. The long key does not make it fully unbreakable, however. Statistical analysis can be performed and patterns can be determined from both the key and the plaintext. If

the key was completely random, but still the same length as the plaintext, then the cipher would be theoretically unbreakable. This type of cipher is known as a one-time pad [7]. One-time pad ciphers are the only ciphers that are considered truly unbreakable, but the overhead of transmitting a unique key the entire length of a message, for every message sent, is unrealistic in nearly all scenarios.

As has been observed, monoalphabetic ciphers are not nearly as strong as polyalphabetic ciphers; however, they can serve a purpose in strengthening other encryption algorithms. In fact, mono- and polyalphabetic ciphers do not have to be mutually exclusive; they can be combined in order to create a more complex algorithm. As an example, a team of researchers modified the polyalphabetic Vigenère cipher by complementing it with a monoalphabetic Affine cipher [8]. This combination produced a cryptographical algorithm that provided better strength than either of the two methods could individually. Since the Vigenère cipher is prone to falling prey to frequency analysis, the Affine cipher adds multiplicative and additive procedures to the text to further encrypt the message. With the finished, combined cipher, the ciphertext is hardened by combining mathematics with the complexity of the Vigenère's polyalphabetic nature.

In addition, some of the classic ciphers have been reconsidered to aid in strengthening security. For example, Kashish Goyal and Supriya Kinger from Sri Guru Granth Sahib World University produced a modified Caesar cipher (a monoalphabetic cipher). While not necessarily making an algorithm that has real-world functionality (in modern standards of cryptography it would still likely be considered pointless), the research does prove the capability of improving traditional cryptographical concepts. Rather than shifting an alphabet by a set number of places, this new modified algorithm shifts letters by one in either the positive or negative direction, based upon whether the integer value of the letter is even or odd. If the letter under consideration is even (based upon an integer mapping table), the number is shifted one to the right. Likewise, if it is odd, then the number is shifted one to the left. This methodology is more complex than the original Caesar Cipher, but it still does little for real-world application [1].

Of the ciphers considered, Running Key is one the most secure, and while not unbreakable, corrects some of the issues found in the original Vigenère (frequency analysis, discovering where the keyword begins and ends, etc.). In addition, it is exponentially stronger than the Caesar, modified Caesar, Affine, or Atbash ciphers. That being said, the proposed modified Vigenère may be stronger yet, as it robustness is still under consideration. However, if one were to combine the Running Key algorithm with the Affine (like was done with the modified Vigenère), a cipher may be produced that approaches unbreakable-ness, since the Affine algorithm helps add an extent of randomity to the ciphertext. The modified Caesar cipher could also aid in increasing complexity.

Regardless of the algorithm under consideration, one has to make a decision and strike a balance. It was already discussed that the one-time pad cipher is the most secure cipher in existence. However, it is usually not realistic to implement. The same can be said about several algorithms, especially those that combine multiple ciphers. A Running Key-Affine cipher may provide great security, but would it slow down a computer too much? Researchers would have to investigate this topic and find out more.

This paper has only scratched the surface of monoalphabetic and polyalphabetic substitution ciphers. There are many others out there, but the ones chosen do provide a decent overview of some of the strengths and weakness of each type. Unsecured data is risky and

dangerous, so one must be thoughtful about the methodologies selected to protect their data, especially as it travels across a network.

Works Cited

[1] K. Goyal and S. Kinger, "Modified Caesar Cipher for Better Security Enhancement," *International Journal of Computer Applications*, vol. 73, no. 3, pp. 26–31, Jul. 2013, doi: 10.5120/12722-9558.

[2] "Substitution Cipher," *GeeksforGeeks*, Dec. 16, 2019. Available: https://www.geeksforgeeks.org/substitution-cipher/

[3] Practical Cryptography, "Atbash Cipher" *www.practicalcryptography.com*. Available: http://www.practicalcryptography.com/ciphers/monoalphabetic-substitution-category/atbash-cipher/ (accessed Jan. 31, 2023).

[4] Practical Cryptography "Affine Cipher", *www.practicalcryptography.com*. http://www.practicalcryptography.com/ciphers/monoalphabetic-substitution-category/affine/ (accessed Jan. 31, 2023).

[5] "Difference between Monoalphabetic Cipher and Polyalphabetic Cipher," *GeeksforGeeks*, Jun. 08, 2020. Available: https://www.geeksforgeeks.org/difference-between-monoalphabetic-cipher-and-polyalphabetic-cipher/

[6] Practical Cryptography, "Vigenère and Gronsfeld Cipher" *www.practicalcryptography.com*. Available: http://www.practicalcryptography.com/ciphers/polyalphabetic-substitution-category/vigenere-gronsfeld-and-autokey/ (accessed Jan. 31, 2023).

[7] Practical Cryptography, "Running Key Cipher," *www.practicalcryptography.com*. Available: http://www.practicalcryptography.com/ciphers/polyalphabetic-substitution-category/running-key/ (accessed Jan. 31, 2023).

[8] S. Agustini, W. M. Rahmawati, and M. Kurniawan, "Modified Vegenere Cipher to Enhance Data Security Using Monoalphabetic Cipher," *International Journal of Artificial Intelligence & Robotics (IJAIR)*, vol. 1, no. 1, p. 25, Oct. 2019, doi: 10.25139/ijair.v1i1.2029.