Levi Seibert

00086809

lseiber1@my.athens.edu

ITE 523 – Dr. Yahia Fadlalla

Vigenère and One-Time Pad Ciphers

Safe, secure, and efficient cryptography is of the utmost importance. It allows for private communications and protected access to information. Cryptography is the tool that allows us to be secure in an unsecure world. While cryptography is so important, there is no complete standardization of how it should take place. There are numerous algorithms and ciphers available for cryptography and their usefulness and strength varies dramatically across the spectrum of cryptographic ciphers.

Within the realm of substitution ciphers, algorithms that substitute plaintext values for ciphertext values, cryptography is often broken into two main categories: monoalphabetic and polyalphabetic ciphers. Monoalphabetic ciphers only use a single plaintext-to-ciphertext correlation (like the traditional Caesar cipher), and are, more often than not, weak and vulnerable by today's standards. Polyalphabetic ciphers, on the other hand, use multiple alphabets that randomize the encryption more decently, thus strengthening their results. Polyalphabetic ciphers are not perfect, but they add significant improvements to monoalphabetic techniques.

The Vigenère cipher is a fairly simple polyalphabetic algorithm; it was considered the golden standard for cryptography for almost 300 years. Until modern cryptographic times, it was thought be unbreakable, but that is no longer the case. In fact, because of its well-known vulnerabilities, the Vigenère cipher is not considered safe for encryption. Originally, the algorithm used a tableau full of columns and rows of alphabets in order to encrypt and decrypt messages; however, an easier method involves some simple arithmetic (the tableau version is well published and can be referenced in order to gain a better understanding of the algorithm). Each of the letters of the plaintext and the key (a single word or phrase repeated enough times to match the length of the plaintext) is translated to numeric values: 'A' becomes 0, 'B' becomes 1, 'C' becomes 2, and so on. To encrypt a message, the corresponding plaintext and key values are added, and, if the resulting value is greater than 26, then it is divided by 26 and the remainder is returned (this is known as the modulus operation). For example, if a plaintext 'Y' corresponds to a key 'D' the result of the encryption would be 'C', since 'Y' = 25, 'D' = 3 and (25 + 3) mod 26 = 2, or 'C'. The same process works for decryption, just with the key value being subtracted from the ciphertext value, instead of being added to the plaintext value (once again, with the modulus operation if the result does not lie between 0 and 25). For example, consider the ciphertext 'C' (equivalent to 2) and the key 'D' (equivalent to 3), the result of decryption is (2 – 3) mod 26 = 25, which is equivalent to 'Y'.

The problem with the Vigenère cipher is that the keyword is repeated. This makes it vulnerable to certain attacks, such as the Kasiski method [1]. Cryptoanalysis techniques like this can be used to determine where the key repeats, and then analysists can deduce more information about the key, potentially leading to an unwanted decryption the message. As such, it can no longer be considered unbreakable, or even secure.

The Running Key Cipher is an improvement on Vigenère in that the key is not just a single, repeated word. Rather, it is a long stream that is as long as the plaintext message. This key is usually an extended quotation from a book. This Running Key cipher does avoid some of the frequency analysis issues that make Vigenère vulnerable; however, because the key is not randomized, there is still a potential of it being statistically deduced (one methodology uses higher order language models to break the encryption) [2].

While the Vigenère and Running Key ciphers are fairly resistant to cryptanalysis by the everyday, common person, they do have some serious safe risks that must be considered. Obviously, a fully secure and private algorithm would be the preference compared to vulnerable methodologies. That being said, the only real "unbreakable" cipher discovered so far is the One-Time Pad cipher.

The One-Time Pad cipher is not technically monoalphabetic or polyalphabetic. In fact, it does not use an alphabet at all for its encryption. In a One-Time Pad cipher, the key is completely randomized and equivalent in length to the size of the plaintext. Like the Running Key cipher, the key does not repeat, and thus is not vulnerable to the frequency analysis attacks found in the Vigenère algorithm. With a completely randomized key, there is no theoretical way a cryptanalyst can decipher what the plaintext is without just fully guessing the key, an impossible feat in most all real-world scenarios.

If the One-Time Pad actually works, they why isn't it used across the board? Since the key must be equivalent in length to the plaintext, and since most plaintext messages are more than a single sentence, a lot of behind-the-scenes, overhead work has to be performed in order to make the algorithm functional, with a completely randomized, unique key. In addition, this lengthy key has to be transmitted to the receiver of the message. This is an issue with symmetric cryptography in general, however, it is exasperated by the magnitude of the size of the One-Time Pad cipher.

In terms of how the One-Time Pad algorithm works, the encryption/decryption process is incredibly simply. In order to encrypt a message, the key and plaintext are converted to binary and then each digit from each of the two resources are exclusive-OR'ed together [3]. An exclusive-OR (XOR) operation consists of comparing two binary digits. If the two digits are identical (both 1s or both 0s) then the operation results in a 0 for that digit. Only when the two digits are different is a 1 produced. The XOR operation is reversable, so decryption is just as easy. All the receiver has to do is XOR the ciphertext with the key, and the original plaintext is revealed. Obviously, this does require the key to be known to both the sender and receiver, which creates a large amount of overhead, but it is considered unbreakable (more secure than modern day algorithms like AES, RSA, and DES). As such, it is often used when complete confidentiality is a must. In fact, for a period of time, some of the communications between the governments of the United States and Russia where protected by the One-Time Pad [3]. However, as has been mentioned, the One-Time Pad is so resource heavy that is unsustainable for most scenarios.

As has been observed, each of the proposed ciphers have their problems (too weak, not fully secure, unmaintainable, etc.). This may be the reason why modern, mainstream cryptography tends to stay away from these algorithms and tend to use block ciphers, which encrypt sections of text at a time, rather than stream ciphers (like those considered so far), which encrypt each letter of a message at a time. That being said, stream ciphers, even those which are

completely ineffective by today's standards, are useful for educational purposes and for establishing the foundations of cryptography.

Works Cited

[1] A. Hananto, A. Solehudin, S. Agung, and B. Priyatna, "Analyzing the Kasiski Method Against Vigenere Cipher," *International Journal of Computer Techniques*, vol. 6, no. 6, pp. 1–8, Nov. 2019, doi: https://doi.org/10.48550/ARXIV.1912.04519.

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

[3] N. Nagaraj, "One-Time Pad as a nonlinear dynamical system," *Communications in Nonlinear Science and Numerical Simulation*, vol. 17, no. 11, pp. 4029–4036, Nov. 2012, doi: https://doi.org/10.1016/j.cnsns.2012.03.020.