Extension for Classic Encryption

Introduction

- Hill Cipher refers to one of classic encryption algorithms, that operate on multiple letters at once.
- Hill cipher depends on using linear algebra through the process of encryption such as using matrix multiplication and modular arithmetic.

Advantages of Hill-Cipher

- Increase the security with multiple letters, which is difference from other conventional encryption algorithms that substitute single letter at a time.
- Hill cipher encrypts blocks of letters, typically in groups of two or three. This makes it more secure against **frequency analysis since patterns across multiple letters are masked.**
- **Mathematical Foundation**: Based on matrix multiplication, Hill cipher requires a matrix key to encrypt and decrypt messages. This makes it robust for encryption and provides a structured approach compared to other ciphers that only rely on letter shifts.
- **High Throughput for Encryption**: Due to its block-based encryption, Hill cipher can encrypt longer texts quickly by processing multiple letters at once.

What is the Type of Encryption Using Hill-Cipher

- Hill-cipher classified as a **substitution cipher**, since it depends on generating cipher text which different in the content from what is the plain text.
- The algorithm depends on replacing the plaintext blocks with ciphered blocks derived through matrix multiplication, rather than what done using transposition techniques, that do rearrange for the original content somehow!

Limitations and Enhancements

- Vulnerable to **Known Plaintext Attacks** if an attacker has a few known plaintext-ciphertext pairs.
- **Key Matrix Invertibility**: Not all matrices are invertible under mod 26, limiting key choices.
- **Lack of Nonlinearity,** which means that this algorithm depends on linear transformation, which makes it more susceptible to linear cryptanalysis. Modern ciphers often incorporate nonlinearity to make cryptanalysis more difficult, but Hill cipher lacks this property.
- **Key Size Limits the Block Size,** Larger matrices increase security but also require more complex calculations and are harder to work with due to invertibility requirements. For practical encryption, this can be limiting.

Limitations and Enhancements

- **Unsuitable for Small Block Sizes**, which means that this algorithm have limitations according to use limited key size, which required for computations. At the same time, larger block sizes are more secure but are computationally intensive and challenging to handle without specialized tools.
- **Modulo 26 Restriction**, since Hill-cipher traditionally works modulo 26 (for the English alphabet). This limits it to alphabets with exactly 26 characters and makes it less versatile for other types of data, such as binary data, Unicode text, or languages with different character sets.

Based on Limitation, What we suggest

- **Increase Block Size**: Use larger matrices (3x3 or 4x4) for added security, though this requires more computational power and invertibility considerations.
- **Combine with Other Ciphers**: Hybridize Hill cipher with non-linear ciphers (e.g., AES or a substitution cipher) to add nonlinearity.
- **Random Matrix Selection**: Use multiple matrices based on an additional key to vary encryption dynamically, making cryptanalysis harder.
- **Use Modular Adjustments**: To support various character sets, consider adjusting the modular base if implementing Hill cipher in non-English contexts, though this increases complexity.

Vigenère Cipher

- Which refers to one of the classic encryption algorithm, that uses polyalphabetic in the process of encryption.
- This algorithm depends on applies different Caeser shifts to different letters in the plain text.
- The technique of encryption depends on repeating the key in case the length of key is less than the length of secrete message.

Advantages of using Vigenère Cipher

- Simple to implement, since this algorithm is relatively easy to implement and to understood, which make this algorithm accessible and used for the purpose of education.
- Present an improvement over the original substitution algorithm (Caeser), since it depends on varied number of caeser shifting.
- Variable key length, by using longer key the algorithm can be resistant to brute force attacks, since the cipher depends on both plain text and the used key.

Disadvantages of Vigenère

- Vulnerability and Kasiski examination, since the algorithm does not have any restriction according to the used key, the short key which must repeated as the long of original algorithm will present a weak point for the algorithm.
- Known plain text attack, if any part of the plain text know, it is easy for attacker to reach to the key of the encryption process, specialy in case the key is short.

What can we do ?!

- Use None-Repeated key, which refer to the important step to enhance the algorithm, since the repeating to key make the algorithm vulnerable to different types of attacks this solution known as Vigenère Autokey Cipher.
- Key expansion, use different techniques to generate as the long of plain text, such as using PRNGs that can be applied to avoid key repetition.
- Enhance key security, such as periodically change the used key for the process of encryption.
- Use this technique as a layer of encryption with other layers.

Kasiski Attack

- Let the cipher text : ZICVTWQNGRZGVTWAVZHCQYGLMGJ
- First step refers to find the repeated sequence.
- The two occurrences of **"VTW"** are 3 characters apart (from position 4 to position 7 and again from position 13 to position 16).
- Calculate the distance between the starting points of each **"VTW"**, the first **"VTW"** starts at position 4, and the second **"VTW"** starts at position 13, based on that the distance between both is 9.
- Find common factors, the factors for 9 is 1,3,9, which represent the most likely candidate for the key length would be 3 (I think it more practical that 1 and 9).

Kasiski .. cont.

- Analyze based on the suggested key length. With a suspected key length of 3, we can now divide the ciphertext into three columns. Each column corresponds to letters encrypted with the same part of the key. For instance:
- Column 1: Z, T, G, V, Q, G, L
- Column 2: I, W, R, T, H, Y, M
- Column 3: C, Q, Z, W, C, G, J
- Use different possibility for shifting and frequency analysis attack to reach to the possible key.