# **Main Features**

## Automatic deciphering

* Ability to input known information about the cipher/plaintext to “help the computer”
* A dictionary that can be sorted by alphabetical & sorted for word length
* Frequency Analysis

# **Key Vocab**

* Plain Text – message being encrypted by the sender
* Cipher Text – encrypted message being sent to the recipient
* Intercept – piece of encrypted text that has been intercepted, therefore nothing is known about it.
* Hill Climbing
* Frequency Analysis
* Cipher – algorithm for encryption or decryption
* Quadgrams – groups of 4 letters (more accurate variant of frequency analysis)

l

# **Supported Ciphers/ Languages**

## Possible Languages / Alphabets

* English
* Morse code?
* NATO phonetic alphabet?
* Pigpen cipher?

## Substitution ciphers

* Caesar cipher
* Affine cipher
* Kama cipher
* Vigenère cipher
* ADFGVX Cipher
* Playfair Cipher

## Transposition ciphers

* Rail fence cipher (zigzag cipher)
* Scytale
* Route cipher
* Columnar transposition
* Frequency analysis

# **Feature Breakdown/Explanation**

## **Substitution Ciphers**

* Replacing characters / bits with alternate characters/ bits to produce ciphertext

**Monoalphabetic substitution** (homophonic substitution)

* Replacing each letter with a different letter (susceptible to frequency analysis)
* E.g., Caesar & Atbash ciphers

**Polyalphabetic substitution**

* Uses multiple substitution alphabets
* E.g., Vigenère cipher, Enigma, Playfair Cipher

Caesar Cipher

* **Monoalphabetic cipher**
* 26 possibilities
* **Susceptible to frequency analysis**
* Involves “shifting” every letter in the plaintext along by a standard value

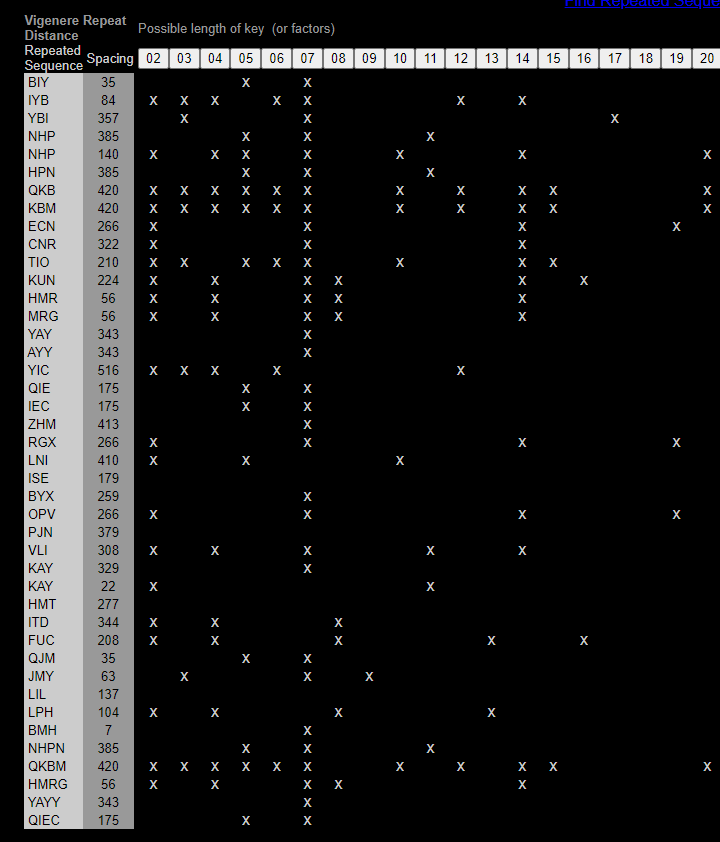
Kama Cipher

* **Monoalphabetic cipher**
* Swaps pairs of letters around, eg replace A with D and D with A
* **Susceptible to frequency analysis**

Affine Cipher

* **Monoalphabetic cipher**
* Equation based monoalphabetic cipher
* **Susceptible to frequency analysis**
* Can be decrypted if any 2 letters are known, therefore can be partially decrypted with frequency analysis and all other letters can be found by solving simultaneous equations.
* C = ap +b (mod M)

Vigenère cipher

* Uses a keyword to shift letters by the value of the letter in the keyword
* 
* Repetition in the ciphertext indicates repetition in the plaintext,
* Length of space between repetitions is most likely a multiple of the keyword length.
* **Susceptible to frequency analysis**, run frequency analysis on every letter, then every 2, then every n etc, once n = length of keyword, you will see a matching distribution.
* 
* Images clipped from <https://www.simonsingh.net/The_Black_Chamber>

ADFGVX Cipher

* Uses a 5x5 polybius square
* Example text FAXDF ADDDG DGFFF AFAX AFAFX

## **Transposition Ciphers**

Changing the position of characters/ bits to produce a ciphertext which is a permutation of the plaintext.

# **Related Notes**

Shannon

# **Sources**

1. <https://en.wikipedia.org/wiki/Transposition_cipher>
2. <https://en.wikipedia.org/wiki/Substitution_cipher>
3. <https://en.wikipedia.org/wiki/Claude_Shannon>
4. <https://en.wikipedia.org/wiki/Kerckhoffs%27s_principle>
5. <https://en.wikipedia.org/wiki/D%27Agapeyeff_cipher>
6. <https://www.geeksforgeeks.org/cryptanalysis-and-types-of-attacks/>
7. <https://cryptii.com/>
8. <http://www.civilwarsignals.org/cipher/kamasutra.html>
9. <https://www.cipherchallenge.org/wp-content/uploads/2020/03/BOSS-Cryptanalyst-Handbook.pdf>
10. <http://practicalcryptography.com/ciphers/>
11. <https://www.techtarget.com/whatis/definition/ciphertext>
12. <https://www.dcode.fr/en>
13. <https://www.nsa.gov/portals/75/documents/news-features/declassified-documents/friedman-documents/publications/FOLDER_437/41751269079046.pdf>
14. <http://practicalcryptography.com/cryptanalysis/text-characterisation/quadgrams/>
15. <https://github.com/jameslyons/pycipher>
16. <https://crypto.interactive-maths.com>
17. <https://crypto.interactive-maths.com/conventions-in-cryptography.html>
18. <https://crypto.interactive-maths.com/frequency-analysis-breaking-the-code.html>
19. <https://crypto.interactive-maths.com/adfgvx-cipher.html>

