BEAUFORT CIPHER REPORT

# **Introduction**

The Beaufort cipher is a symmetric polyalphabetic substitution cipher named after Sir Francis Beaufort, an Irish hydrographer and officer in the Royal Navy. It is similar to the Vigenère cipher but differs in the way the encryption and decryption processes are handled.

# **History**

The Beaufort cipher emerged during a time when communication security was of utmost importance, especially in military and diplomatic circles. Sir Francis Beaufort, known for his contributions to naval navigation, adapted and refined existing cryptographic methods to create a robust and effective encryption technique.

# **The Basics of Beaufort Cipher**

Beaufort cipher is a symmetric encryption algorithm which essentially means that the same key is used for encryption and decryption. Each letter in the plaintext is replaced by another letter according to a specific rule. Unlike the Caesar Cipher, which shifts letters a fixed number of positions, the Beaufort cipher introduces a dynamic element. The key is a keyword or phrase that determines the letter substitutions. This makes the cipher more resistant to simple frequency analysis techniques.

# **Encryption Process**

## 1. **Prepare Plain Text and Key**

- Convert both the plain text and the key to uppercase.

- Example: `HELLO WORLD`, `KEY`

## 2**. Initialize an Empty Result**

- Create an empty string to store the encrypted text.

- Example: Result: `""`

## 3. **Loop Through Each Character in the Plain Text**

- For each character in the plain text:

- If it's a letter:

## 1. Find Positions

- Get the position of the plain text character and the key character in the alphabet (A=0, B=1, ..., Z=25).

- Example: `H` is 7, `K` is 10

## 2. Subtract and Modulo

- Subtract the plain text position from the key position, take modulo 26.

- Example: `(10 - 7) % 26 = 3`

## 3. Convert to Character

- Convert the resulting position back to a character.

- Example: 3 is `D`

## 4. Append to Result

- Add the resulting character to the result string.

- If it's not a letter, add it directly to the result.

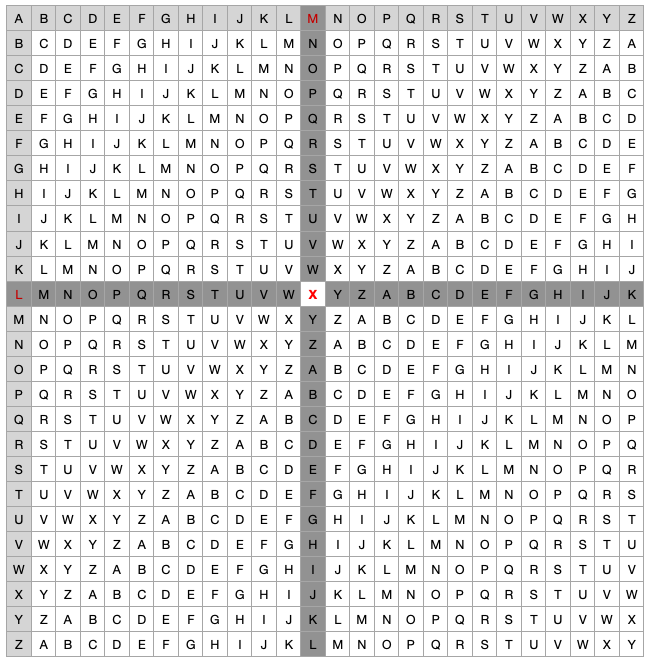
## 5. Repeat Key if Necessary

- Cycle through the key characters if the key is shorter than the plain text.

- Example: `KEYKEYKEYKE` for `HELLO WORLD`

## 6. Output Encrypted Text

- The final result string is the encrypted text.



## Example

Given plain text "HELLO WORLD" and key "KEY":

## 1. Prepare:

- Plain text: `HELLO WORLD`

- Key: `KEY`

- Repeated key: `KEYKEYKEYKE`

## 2. Encrypt:

- `H` (7) with `K` (10) → `(10 - 7) % 26 = 3` → `D`

- `E` (4) with `E` (4) → `(4 - 4) % 26 = 0` → `A`

- `L` (11) with `Y` (24) → `(24 - 11) % 26 = 13` → `N`

- `L` (11) with `K` (10) → `(10 - 11) % 26 = 25` → `Z`

- `O` (14) with `E` (4) → `(4 - 14) % 26 = 16` → `Q`

- `W` (22) with `Y` (24) → `(24 - 22) % 26 = 2` → `C`

- `O` (14) with `K` (10) → `(10 - 14) % 26 = 22` → `W`

- `R` (17) with `E` (4) → `(4 - 17) % 26 = 13` → `N`

- `L` (11) with `Y` (24) → `(24 - 11) % 26 = 13` → `N`

- `D` (3) with `K` (10) → `(10 - 3) % 26 = 7` → `H`

## 3. Result

- Encrypted text: `DANZQ CWNNH`

This results in the plain text "HELLO WORLD" being encrypted to "DANZQ CWNNH" using the key "KEY".

# **Decryption Process**

Decryption in the Beaufort cipher follows a similar process to encryption.

* The decryption process for the Beaufort Cipher is the same as the encryption process, but with the ciphertext as the input.
* The key is repeated until it is the same length as the ciphertext message.
* The ciphertext is then converted to numbers, typically using the ASCII table.
* The Beaufort Cipher uses a tabula recta, which is a grid of alphabets used for substitution.
* The key is then used to determine which alphabet in the tabula recta to use for substitution.
* The plaintext is produced by reading the corresponding alphabet in the tabula recta.

# **Security Analysis**

### Strengths

1. **Polyalphabetic Nature**: The use of multiple substitution alphabets makes frequency analysis attacks more difficult compared to monoalphabetic ciphers.
2. **Symmetric Encryption and Decryption**: The identical process for encryption and decryption simplifies implementation and reduces potential for errors.

### Weaknesses

1. **Key Repetition**: If the key is shorter than the plaintext, it will be repeated, which can potentially expose patterns and make the cipher vulnerable to cryptanalysis.
2. **Known-Plaintext Attack**: If an attacker knows or can guess a part of the plaintext, they can potentially deduce parts of the key and subsequently decrypt other parts of the ciphertext.

## More about the Beaufort Cipher

The Beaufort cipher, though not widely used today due to the availability of more secure modern encryption methods, has historical significance and niche applications:

1. **Historical Context**: The Beaufort cipher was used during the 19th century for secure communication, particularly by the British Royal Navy. It was considered secure against the cryptographic techniques of the time.
2. **Educational Tool**: It is often used in educational settings to teach the concepts of polyalphabetic ciphers and the historical development of cryptography.
3. **Puzzle and Challenge Contexts**: The Beaufort cipher appears in various puzzle contests, cryptographic challenges, and escape room games as a way to engage participants in cryptographic thinking.
4. **Cultural and Historical Studies**: Researchers and enthusiasts studying historical documents and cryptographic methods might encounter the Beaufort cipher as part of their exploration of early encryption techniques.

# Conclusion

* In conclusion, the Beaufort Cipher is a polyalphabetic substitution cipher that has been used for centuries to encrypt confidential messages.
* It is still used today in certain applications where security is important. Although it has several strengths, such as being easy to implement and use, it also has several weaknesses, such as susceptibility to known-plaintext attacks.
* Therefore, it is important to use the Beaufort Cipher judiciously and to implement appropriate measures to mitigate

# References

https://cronolock.ca/the-lock-blog/the-beauty-of-the-beaufort-cipher

https://www.youtube.com/redirect?event=video\_description&redir\_token=QUFFLUhqbWVwdzdtRVA1MGgtZWhibVVuTF9JNmVyaDR1UXxBQ3Jtc0tuY3gtNWxTamxmVldPZDFWcTNiM0FkcWQ5bUJDaTRUR0R1RGFwbjVrMXVQWHFsMTNOM2oyVEg2RXk3Wm5PTUdNeFNUY203aWxVanpmVjczUGhRZGt6TUlTOHJoR3RyQmhhRXJYZ0N4Z2ozSm95NmIwVQ&q=http%3A%2F%2Fpracticalcryptography.com%2Fciphers%2Fbeaufort-cipher%2F&v=nGJM\_UF3IpQ