El cifrado de Vigenère es un método de sustitución polialfabética que utiliza una palabra clave para determinar el desplazamiento de cada letra en el mensaje original. Aunque suele atribuirse a Blaise de Vigenère, este cifrado fue descrito inicialmente por Giovan Battista Belasso en 1553, aunque con un método ligeramente distinto. Fue Vigenère quien, en 1586, popularizó una versión más avanzada del sistema en su tratado Traicté des Chiffres.

Elegí el cifrado de Vigenère porque fue uno de los primeros en emplear una clave para el cifrado, introduciendo el concepto de sustitución polialfabética y mejorando la seguridad en comparación con métodos anteriores como el cifrado César.

Ventajas:

- **Mayor seguridad que los cifrados de sustitución simples:** Al utilizar múltiples alfabetos de sustitución basados en una clave, dificulta los ataques de análisis de frecuencia.
- **Simplicidad y facilidad de implementación:** Es fácil de entender y aplicar, lo que lo convierte en una herramienta educativa útil.

Vulnerabilidades:

- **Ataque de Kasiski:** Si un atacante determina la longitud de la clave, puede aplicar análisis de frecuencia a segmentos del mensaje, facilitando su descifrado.
- **Claves débiles o cortas:** El uso de claves cortas o repetitivas reduce la seguridad, ya que pueden emerger patrones en el texto cifrado que los atacantes pueden explotar.

Ejemplo de uso

Cifrar el mensaje "NUBLADO" utilizando la clave "SOL".

1. Asignar valores numéricos a cada letra (A=0, B=1, ..., Z=25):

    - Mensaje: N (13), U (20), B (1), L (11), A (0), D (3), O (14)
    - Clave: S (18), O (14), L (11)

2. Repetir la clave hasta igualar la longitud del mensaje:

    - Clave extendida: S (18), O (14), L (11), S (18), O (14), L (11), S (18)

3. Sumar los valores correspondientes del mensaje y la clave, aplicando módulo 26:

    - N (13) + S (18) = 31 → 31 % 26 = 5 → F
    - U (20) + O (14) = 34 → 34 % 26 = 8 → I
    - B (1) + L (11) = 12 → 12 % 26 = 12 → M
    - L (11) + S (18) = 29 → 29 % 26 = 3 → D
    - A (0) + O (14) = 14 → 14 % 26 = 14 → O
    - D (3) + L (11) = 14 → 14 % 26 = 14 → O
    - O (14) + S (18) = 32 → 32 % 26 = 6 → G

El mensaje cifrado resultante es "FIMDOOG".

Referencias

- Universidad de Granada. (s.f.). *El cifrado de Vigenère*. Recuperado de ugr.es
- Universidad Nacional Autónoma de México. (s.f.). *¿Cómo hacer citas y referencias en formato APA?*. Recuperado de bibliotecas.unam.mx