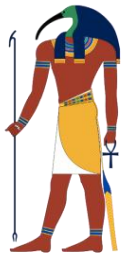

Píldora nº 19: ¿Qué es la cifra de Vigenère?

Escena 1: La figura de Blaise de Vigenère

Blaise de Vigenère fue un criptógrafo, químico y diplomático francés que nace en 1523 y fallece en 1596. En su libro *Traité des chiffres où secrètes manières d'escrire* publicado en 1586 describe de una forma detallada y estructurada la cifra polialfabética, basándose en trabajos previos de otros criptógrafos famosos como Alberti, Trithemius, Bellaso y della Porta. Por este motivo el sistema de cifra polialfabética más conocido y estudiado lleva su nombre.

Para cifrar utilizaba la tabla de Vigenère, que consiste en una matriz cuadrada con las n letras del alfabeto. En la primera fila se escribe el alfabeto desde la A hasta la Z, en la segunda fila el alfabeto desplazado un espacio a la izquierda, en la tercera fila desplazado dos espacios, y así sucesivamente hasta la última fila en que el desplazamiento será igual a n-1.

Escena 2: Cifrando con el método de Vigenère

El texto en claro se va leyendo letra a letra en la primera fila y la clave de igual manera en la primera columna. La intersección entre ambas en la tabla es el elemento cifrado. Así, si el mensaje es HERMOSO y la clave CIELO, en la columna de la letra H del texto en claro se busca la intersección con la fila de la letra C de la clave, dando como resultado el criptograma J. A continuación se repite el procedimiento con la letra E y la I, y así sucesivamente. Cuando la clave se termina, ésta se repite de forma cíclica, obteniendo el criptograma JMVWD UW.

También podemos usar las matemáticas discretas para cifrar con el método de Vigenère. Para ello escribimos la clave debajo del mensaje tantas veces como sea necesario y reemplazamos el código de las letras para realizar la operación. O bien con la siguiente expresión

$$c_i = (m_i + k_i) \bmod n$$

Escena 3: Descifrando con el método de Vigenère

Para descifrar, simplemente se realiza el proceso inverso. Si el criptograma es JMVWD UW y conocemos la clave CIELO, se busca en la fila de la primera letra de la clave C, la letra J del criptograma. Hecho esto, nos posicionamos en esa columna y se lee la letra que aparece en la primera fila como texto en claro, en este caso la letra H. Este proceso se realiza para cada una de las letras del criptograma con su correspondiente letra de la clave obteniendo HERMOSO.

Para descifrar usando matemática discreta, hacemos la misma operación que en la cifra pero en vez de sumar el valor del código de la letra de la clave al de la letra en claro, habrá que restar ya que es la operación inversa dentro del cuerpo, es decir:

$$m_i = (c_i - k_i) \bmod n$$

Escena 4: ¿Una cifra indescifrable?

La cifra polialfabética destruye la relación directa proporcional que se observaba en la cifra monoalfabética entre el texto en claro y el criptograma. Si se usa una clave con varios alfabetos diferentes, como podría ser MURCIELAGO, muchas las letras del criptograma tendrán una frecuencia similar y por lo tanto no tiene ya sentido intentar un ataque mediante análisis de frecuencias en la forma en que venía haciéndose con los sistemas monoalfabéticos.

Para aumentar la fortaleza al criptoanálisis, se usará una variante de Vigenère conocida como autoclave. Se escribe la clave como siempre, pero cuando se usa la última letra se sigue con el mensaje como si fuese parte de esa clave, por lo que al no repetirse ésta deja de ser cíclica. También puede utilizarse como clave otro texto de igual o mayor longitud que la del mensaje.

El cifrado de Vigenère y sus variantes resistieron casi 300 años al criptoanálisis y por ello se les llamó *le chiffre indéchiffrable*. Pero en 1854 el matemático inglés Charles Babbage rompe la cifra, en realidad la de autoclave, aunque no hace público su trabajo. Años más tarde, en 1863, el militar alemán Friedrich Kasiski publica un método para un criptoanálisis del sistema de Vigenère haciendo uso de la redundancia del lenguaje y su fortaleza se rompe definitivamente.

Madrid, diciembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*

creative commons
Attribution
Noncommercial
No derivative works