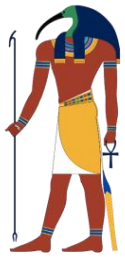

Píldora nº 20: ¿Cómo se ataca por Kasiski la cifra de Vigenère?

Escena 1: Algunos protagonistas del ataque a la cifra indescifrable

Corría el año 1854, es decir 268 años después de la invención de la cifra de Vigenère, cuando el matemático y criptógrafo inglés Charles Babbage logra criptoanalizarla, aunque en realidad lo que rompe es el sistema llamado autoclave mucho más seguro y complejo que Vigenère. Desgraciadamente, Babbage no publica sus resultados.

Quien sí lo hace público pero en 1863, nueve años después, es el militar alemán Friedrich Kasiski en el libro Escritura Secreta y el Arte de Descifrar (*Die Geheimschriften und die Dechiffrierkunst*). Kasiski muere en 1881 a los 75 años sin ser del todo consciente del importante legado que hace a la criptografía.

También juega un destacado papel el criptoanalista ruso-norteamericano William Friedman, que publica 60 años después, en 1922, el libro El Índice de Coincidencia y sus Aplicaciones en Criptografía (The Index of Coincidence and Its Applications in Cryptography), documento que se mantiene clasificado como confidencial durante 50 años.

Escena 2: Los principios del método Kasiski

Debido a la redundancia del lenguaje, si un texto en claro se lee “a saltos entre sus letras”, es decir, se observa y anota la letra que aparece cada x espacios en un documento, al contabilizar dichas letras en ese nuevo documento se observará un comportamiento estadístico similar al del texto en claro original.

En otras palabras, si la letra A y la letra E eran las más frecuentes en el texto en claro, entonces en esos otros textos que se han creado leyendo del primero las letras separadas por un espacio constante, será muy probable que la A y la E sigan siendo las más frecuentes.

Como es lógico, para que ello se manifieste y por tanto nos entregue información que permita iniciar el ataque, se deberá contar con una cantidad suficiente de texto. La pregunta obvia es, ¿cuánto texto es necesario para que funcione el método de ataque de Kasiski? Pues bien, aunque parezca increíble, en un cuerpo de cifra de 27 letras, solamente con 100 o más letras, ya se manifiesta claramente la redundancia del lenguaje. Es decir, sólo 3 veces el tamaño del alfabeto.

Por lo tanto, si una cifra de Vigenère usa una clave de 5 letras, por ejemplo BARCO, con un criptograma de 5x100 = 500 o más letras, tendremos muy buenas expectativas de que el ataque por el método de Kasiski prospere.

Escena 3: Criptoanálisis de Vigenère con el método de Kasiski

Para llevar a cabo el ataque a un cifrado de Vigenère mediante Kasiski, primero buscamos cadenas de caracteres de al menos 3 letras repetidas en el criptograma. Hecho esto, encontramos la separación que hay entre las cadenas iguales y calculamos el máximo común divisor de todas esas separaciones. Ello nos dará la posible longitud de la clave, pero no las letras que la forman. Si la clave tiene una longitud L, entonces habrá L subcriptogramas que se han cifrado con una misma letra, es decir todas son cifras monoalfabéticas.

Para encontrar las letras de la clave dividimos el criptograma en tantos subcriptogramas como sea esa longitud L encontrada. Como cada uno de estos subcriptogramas será el resultado de una cifra monoafabética, contabilizamos las veces que aparecen las letras del alfabeto en ellos y marcamos las de frecuencia mayor. Estas deberían corresponder a la cifra de la letra A, la E y la O. La posición relativa que ocupa la letra A en tabla será la letra de la clave que buscamos.

El ataque de la cifra autoclave es algo más complejo pero sigue estos mismos principios de la manifestación de la redundancia del lenguaje en el criptograma.

Madrid, diciembre de 2014

Autor del guion: *Jorge Ramió Aguirre*
Dirección Proyecto Thoth: *Jorge Ramió Aguirre, Alfonso Muñoz Muñoz*