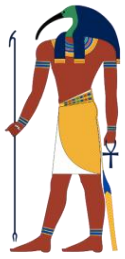

Píldora nº 18: ¿Cómo se ataca la cifra por sustitución monoalfabética?

Escena 1: Ataques por fuerza bruta

Ante un criptograma que se sospecha es el resultado de una cifra por sustitución genérica monoalfabética y monográmica, como las de decimación, de desplazamiento y afín, será fácil descubrir el alfabeto de cifrado mediante un ataque por fuerza bruta probando cada una de las posibles combinaciones de los valores válidos para a y b. Se trata de un ataque poco elegante, pero en este escenario es adecuado ya que en el peor de los casos en módulo 27 sólo se requerirían 441 intentos.

No obstante, si se incluye una clave en cualquiera de estos tres algoritmos de cifra, el número de alfabetos de cifrado posibles crece espectacularmente, llegando en el caso máximo a más de diez mil cuatrillones, que es el valor del factorial de 27, lo que hace ahora nada aconsejable un ataque por fuerza bruta. A pesar de ello, estos sistemas sucumben ante un ataque por análisis de frecuencia de las letras del criptograma como veremos a continuación.

Escena 2: Atacando con elegancia: técnicas de criptoanálisis

La primera acción que realiza cualquier criptógrafo ante un criptograma, es observar y apuntar la frecuencia con la que aparecen los caracteres en el mismo. Si la distribución de frecuencias se asemeja a la del alfabeto en claro, entonces es muy probable que la cifra sea por sustitución monoalfabética. Si éste fuese el caso, solamente queda asociar dichas frecuencias con las que se obtienen de un texto en claro con algunas centenas de letras para ir encontrando las correspondencias y nuevas posiciones que ocupan esas letras ahora en el alfabeto cifrado.

Cuando el sistema de cifra tiene una clave, y por tanto no existe una ecuación simple que represente dicha operación, habrá que ir asociando una a una las letras del criptograma de

acuerdo a sus frecuencias con una posible letra del texto en claro. El texto en claro va apareciendo de a poco como si se tratase de un crucigrama.

Sin embargo, cuando la cifra genérica tiene una expresión matemática, la solución a todo el alfabeto de cifrado se obtendrá inmediatamente tras resolver una ecuación con una incógnita en las cifras por decimación y por desplazamiento, o bien un sistema de dos ecuaciones independientes y dos incógnitas en el caso de la cifra afín.

Escena 3: Criptoanálisis de los sistemas de cifra genéricos por sustitución

Si la cifra es por decimación es decir c = a*m mod n, o por desplazamiento, esto es c = m + b mod n, buscaremos la letra más frecuente del criptograma y la asociaremos a la letra E, la más frecuente del alfabeto español. Como ejemplo, supongamos que en un criptograma la letra más frecuente es la T, el valor 20. Entonces la haremos corresponder con la letra E del texto en claro, el valor 4. Así, si la cifra es por decimación, diremos que 20 es igual a a multiplicado por 4 módulo 27. Despejando el valor de a, obtenemos 20 multiplicado por el inverso de 4 en módulo 27. Como el inverso de 4 en módulo 27 es igual a 7, la constante a será igual a 20 multiplicado por 7 módulo 27, es decir el número 5. Como se ha cifrado multiplicando por la constante 5, vamos a descifrar multiplicando todo el criptograma por inv (5, 27) = 11, y comprobamos que se recupera un texto con sentido.

En el caso de la cifra por desplazamiento, si la letra E se cifra como T, simplemente despejamos la constante b como 20 menos 4 módulo 27 igual a 16 y desciframos usando este desplazamiento b pero en sentido contrario.

Decimación	T = a*E mod 27	20 = a*4 mod 27	a = 20*inv (4, 27) mod 27	a = 20*7 mod 27	a = 5	m = c*11 mod 27
Desplazamiento	T = E+b mod 27	20 = 4+b mod 27	b = 20–4 mod 27	b = 16 mod 27	b = 16	m = c–16 mod 27

En una cifra afín habrá dos variables, a y b. Por tanto en este caso vamos a plantear un sistema de dos ecuaciones independientes, asignando la letra más frecuente del criptograma a la letra E del texto en claro, y la segunda más frecuente del criptograma a la letra A del texto en claro. Si el ataque no prospera con estas correspondencias, se intercambian los papeles, suponiendo ahora que la A es más frecuente que la E o bien se considera otra letra frecuente como la O.

En el siguiente criptograma de 424 caracteres, las dos letras más frecuentes son la W que aparece 59 veces con un 13,9%, y la K que aparece 52 veces con un 12,2%.

IJNYI WBNYF KMYLF JOYLI YBZKT WBNWN JDKNY WLUWM JTBYK EFKIW BLYFK VKQYB UWFPY EFKLW BJKWH DELKW LUKIW BLYFK VKQYB WLWMV WSYBK VJPYR EWUWF PYWFW MVEFN YUWFP YYUBK WHDEL KWLUK IWBLY FKVKQ YBWLD KIKAN WWFUW FNWBM YUYNY ZKLUK MYLMJ TBYLI KBKFJ OYLUW FPYEF KUWBD WBKWH DELKW LUKIW BLYFK VKQYB ÑJÑWW FGBKF DJKNY FNWIK LKZKV TBWQG BJYÑW BNKNW BKVWF UWFWD WLJUK DYFLE WMYLJ UYNKL WLKLW HDELK LFYTK LUKLW FTJWF IEWNY NWNJD KBWLU WMJTB YKMFJ OYREW EFKÑW AGEWW LUKIW BLYFK VKQYB UYNYL MYLVK QYBWL ZKFLJ NYIBJ VWBYF JOYL

Suponiendo entonces que la W se corresponde con la letra E del texto en claro y la K con la A del texto en claro, formamos un sistema de dos ecuaciones independientes. Resolviendo el sistema, encontraremos las incógnitas a y b.

Si el resultado nos arroja un valor de la constante a no válido, es decir que no tiene inverso en el cuerpo, cambiamos las correspondencias entre letras o bien incluimos alguna otra letra frecuente como la O.

[1] W = a * E + b mod 27 23 = a * 4 + b mod 27

[2] K = a * A + b mod 27 10 = a * 0 + b mod 27

De [2] se tiene que b = 10.

Reemplazando en [1]:

23 = a * 4 + 10 mod 27

a = (23 – 10) * inv (4, 27) mod 27 = 13 * 7 mod 27 = 10 (valor válido)

a = 10, b = 10

Luego: c = 10 * m + 10 mod 27

Por lo tanto m = (c – 10) * inv (10, 27) mod 27 = (c – 10) * 19 mod 27

Como la constante a igual a 10 es un valor válido y sabemos que constante b vale 10, desciframos el criptograma y obtenemos un texto con sentido. Se trata de la dedicatoria del El Principito.

Pido perdón a los niños por haber dedicado este libro a una persona mayor. Tengo una seria excusa: esta persona mayor es el mejor amigo que tengo en el mundo. Tengo otra excusa: esta

persona mayor es capaz de entenderlo todo, hasta los libros para niños. Tengo una tercera excusa: esta persona mayor vive en Francia, donde pasa hambre y frío. Verdaderamente necesita consuelo. Si todas esas excusas no bastasen, bien puedo dedicar este libro al niño que una vez fue esta persona mayor. Todos los mayores han sido primero niños.

Madrid, noviembre de 2014

Autor del guion: *Jorge Ramió Aguirre*

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