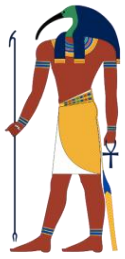

Píldora nº 16: ¿Qué es la cifra del César?

Escena 1: El dictador Julio César y la cifra

El primer uso documentado de una cifra monoalfabética por sustitución con propósitos militares aparece en "La guerra de las Galias" de Julio César. En dicho libro, Julio César describe cómo envía un mensaje cifrado a Cicerón, que se encontraba sitiado y a punto de rendirse, aplicando una sustitución simple a las letras del texto en claro de forma que el mensaje fuera ininteligible para el enemigo. En este caso, César sustituye las letras romanas por letras griegas. Sin embargo lo más característico de su método consistía en aplicar un desplazamiento de 3 espacios al alfabeto en claro.

Escena 2: Cifrando con el algoritmo del César

Gracias a la entrada 56 sobre Cayo Julio César en la obra "Vidas de los Césares" de Suetonio, sabemos que uno de los algoritmos utilizados por César consistía en aplicar un desplazamiento de tres espacios a los caracteres del texto en claro, de forma que para un alfabeto de 27 caracteres la letra A se sustituye por la letra D, la B por la E y así sucesivamente.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C

De esta manera, la famosa frase VENI VIDI VICI, atribuida a Julio César también por Suetonio, se cifraría con este método y con un alfabeto español de 27 letras como YHPL YLGL YLFL.

El cifrado del César con un desplazamiento de 3 espacios es un caso particular del cifrado genérico por sustitución con desplazamiento puro de la forma c = m + b mod n, en donde b es la constante de desplazamiento que puede tomar valores desde 1 hasta n-1, puesto que un desplazamiento de b igual a cero o b igual a n significaría enviar el texto en claro.

Escena 3: Cifrado del César utilizando una clave

Para aumentar la fortaleza de la cifra, se puede incluir en el alfabeto de cifrado una clave K, que consiste en una palabra o frase que se escribe a partir de una posición p_K del alfabeto sin repetir las letras. Hecho esto, a continuación se incluyen en orden las restantes letras del alfabeto. Así, si en la posición p_K igual a 3 se escribe la clave ESTOY ABURRIDO, el alfabeto de cifra será el que se indica.

A	B	C	D	E	F	G	H	I	J	K	L	M	N	Ñ	O	P	Q	R	S	T	U	V	W	X	Y	Z
W	X	Z	E	S	T	O	Y	A	B	U	R	I	D	C	F	G	H	J	K	L	M	N	Ñ	P	Q	V

En este tipo de cifra se deja de cumplir la condición de desplazamiento constante, que era una característica básica del sistema de cifra primario del César

Como era de esperar, al tener un mayor número de combinaciones de alfabetos posibles, existe una mayor incertidumbre respecto a la clave. De hecho, este alfabeto de cifrado podrá tener más de 10 mil cuatrillones de representaciones posibles distintas: 27! = (27*26*25*… *3*2*1) = 10.888.869.450.418.352.160.768.000.000. Se trata de un número muy alto y que hace muy poco recomendable intentar romperlo por fuerza bruta. A pesar de ello, la seguridad del sistema seguirá siendo muy baja porque la redundancia del lenguaje se sigue manifestando en el criptograma.

Escena 4: Descifrado y seguridad del algoritmo del César

Para descifrar una cifra simple del César, bastará con aplicar el algoritmo en su modo inverso, en este caso usando un desplazamiento de b espacios en sentido contrario. Por propiedades matemáticas, también será posible descifrar el criptograma desplazando el texto cifrado n-b espacios.

El algoritmo del César fue un sistema de cifra muy sencillo, ingenioso e incluso apropiado para la época. Como muy poca gente tenía acceso a la cultura y el número de analfabetos era altísimo, a pesar de su sencillez pudo utilizarse durante siglos. No obstante, presenta un nivel de seguridad muy débil y su criptoanálisis es elemental. Basta con realizar un sencillo y rápido ataque por fuerza bruta, desplazando las letras del criptograma una, dos, tres, etc., posiciones a la izquierda o a la derecha hasta dar con el mensaje en claro.

Sin embargo, el ataque a los sistemas con un alfabeto de cifrado con clave o bien un alfabeto de cifrado no secuencial, es decir con posiciones de letras cambiadas al azar, será algo más complejo y habrá que hacer uso de las estadísticas del lenguaje. Lo veremos en una siguiente píldora.

Madrid, noviembre de 2014

Con el patrocinio de Talentum Startups

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