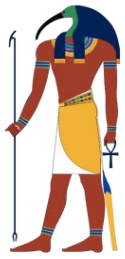

# Píldora nº 9: ¿Por qué busca la criptografía la confusión y la difusión?

## Escena 1: Principios básicos de la cifra

Los algoritmos de cifra, tanto clásica como moderna, usan dos principios básicos para enmascarar el texto en claro y proteger el secreto de la información, convirtiéndola en un criptograma imposible de descifrar si no se conoce una clave. Estas técnicas son la difusión y la confusión.

Dichos principios, que se usaban ya en los orígenes de la criptografía, son refrendados en 1949 por Claude Shannon en el artículo Communication Theory of Secrecy Systems.

## Escena 2: Técnica de difusión

Como su nombre lo indica, la difusión pretende difundir las características del texto en claro en todo el criptograma, ocultando así la relación entre el texto en claro y el texto cifrado.

Para lograr la difusión se aplicarán al texto en claro operaciones de transposición o permutación de caracteres, bytes o bloques determinados, de manera que los elementos del mensaje aparecerán dispersos o desordenados en el criptograma, naciendo de esta manera los algoritmos de cifrado por transposición.

Observa que tras aplicar transposición al texto en claro, el criptograma tendrá sus mismos elementos, aunque lógicamente en posiciones diferentes.

## Escena 3: Técnica de confusión

Por su parte, la confusión pretende confundir al atacante, de manera que no le sea sencillo establecer una relación entre el criptograma y la clave de cifrado.

Para lograr esta confusión, se aplicarán al texto en claro operaciones de sustitución de un carácter, byte o bloques determinados, por otros elementos similares, naciendo de esta manera los algoritmos de cifrado por sustitución.

Observa que tras aplicar sustitución al texto en claro, los elementos del criptograma no serán los mismos que los del mensaje original.

## Escena 4: Sustituciones y permutaciones

Dado que un texto cifrado debe tener una apariencia aleatoria, deberá eliminarse cualquier relación estadística entre el mensaje original y su texto cifrado. Esto se logra con la permutación y la sustitución; sin embargo, ambas por sí solas no son suficientes para cifrar un texto de manera segura.

La combinación de la sustitución y la transposición dispersa la estructura estadística del mensaje sobre la totalidad del texto cifrado, dando así fortaleza al secreto.

En los algoritmos modernos de cifrado simétrico o de clave secreta como por ejemplo AES, IDEA y 3DES, se usan estas dos técnicas simultáneamente y por ello se les conoce como cifradores de producto.

Madrid, septiembre de 2014

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