VÍDEO intypedia001es

LECCIÓN 1: HISTORIA DE LA CRIPTOGRAFÍA Y SU DESARROLLO EN EUROPA

AUTOR: Arturo Ribagorda Garnacho

Universidad Carlos III de Madrid, España

BERNARDO

Hola, bienvenidos a intypedia. Hoy te presentaremos el primer tema de la enciclopedia, un recorrido por la Historia de la Criptografía desde sus inicios hasta la Primera Guerra Mundial. ¡Acompáñanos!

1. LOS INICIOS

ALICIA

Hoy en día, la criptografía está muy presente en nuestro mundo. Así, acciones tan cotidianas como hacer, o recibir, una llamada desde un teléfono móvil, pagar con una tarjeta de crédito o débito, sacar dinero de un cajero, conectarnos a un ordenador introduciendo una contraseña, etc., hacen uso de técnicas que se aposentan en esta ciencia.

BERNARDO

¿En qué momento inventó el hombre estas técnicas y cuándo empezaron las sociedades a emplearlas? ¿Cuáles fueron sus primeros usos? Creo recordar que la respuesta está en los orígenes de la escritura.

ALICIA

En efecto Bernardo. La escritura es, en opinión de muchos, el invento más importante de la humanidad. La escritura permite dejar constancia de hechos, opiniones, ideas, etc., salvando

distancias temporales o espaciales. De este modo, permite el progreso del conocimiento y el avance de la civilización. Sin embargo, tras la generalización y desarrollo de la escritura, se constató los peligros que conlleva su lectura por personas ajenas, ideándose los primeros sistemas de protección de lo escrito.

BERNARDO

Es verdad. Es más, creo recordar que habitualmente la información a proteger se conoce como la información en claro y cuando a esta información se le aplica un procedimiento de cifrado se habla en este caso de información cifrada. Sólo el destinatario que posea una información privilegiada denominada clave criptográfica o simplemente clave podrá revelar la información cifrada.

ALICIA

Así es. Históricamente tenemos que remontarnos a Esparta donde se diseña, hacia el siglo V a. C., el primer método sistemático de cifrado. Este consistía en un bastón sobre el que se enrollaba en espiral, a modo de venda, una estrecha cinta de cuero. Tras ello, se escribía a lo largo del bastón el mensaje. Al desenrollar la cinta sólo se apreciaba una larga ristra de letras sin sentido, que sólo se recobraba tras volver a enrollar la cinta sobre un bastón de igual diámetro que el primero. Ese diámetro era la clave.

2. MÉTODOS DE CIFRA MONOALFABÉTICA

ALICIA

El método conocido como escítala lacedemonia, era usado para comunicaciones entre responsables del gobierno de Esparta y sus generales. No obstante, debemos esperar aún unos siglos para encontrar el método más popular de la Antigüedad Clásica: el método César. Conocido así por ser utilizado por Julio César. Consistía en sustituir cada letra del escrito (sin cambiar su lugar en el mismo) por aquella situada tres posiciones por delante en el alfabeto. Es decir, cambiar todas las aes por des, todas las bes por es, etc., hasta llegar al final del alfabeto donde la “x”, “y” y “z” se cambian respectivamente por la “a”, “b” y “c”.

Estos métodos, la escítala y el César, ilustran los dos grandes grupos de métodos de cifrado existentes: transposición y sustitución. Mediante las técnicas de transposición las letras del texto en claro intercambian sus posiciones según un cierto patrón, de modo que en el texto cifrado aparecen las mismas letras pero con sus posiciones permutadas. Los métodos que siguen este esquema se denominan de transposición o permutación y un ejemplo es la escítala lacedemonia que hemos visto.

Por el contrario, las técnicas de sustitución hacen que las letras mantengan sus posiciones en el texto, pero cambian su apariencia, siendo sustituidas cada una de ellas por otra letra, por un número o por un símbolo cualquiera. Si a cada letra en claro sólo le corresponde un único símbolo cifrado, el método se llama monoalfabeto. Este es el caso del método César.

BERNARDO

Ya veo, pero hoy en día este método no es recomendado… ¿no?

ALICIA

Este método es completamente inseguro. La respuesta se encuentra en la ciencia del criptoanálisis.

BERNARDO

Perdona Alicia, no entiendo, ¿qué es eso del criptoanálisis?

ALICIA

Te explico. A lo largo de la historia numerosas personas han intentado revelar los secretos protegidos sin conocimiento de la clave que los protege. Esta disciplina se denomina criptoanálisis y criptoanalistas a sus practicantes. El conjunto de la criptografía y el criptoanálisis es lo que se conoce hoy día como la ciencia de la criptología.

Realmente, tras la caída del Imperio Romano y hasta el Renacimiento, la criptología sólo registró avances significativos en los califatos islámicos, singularmente el abasí. En su capital, Bagdad, nace en el siglo IX d. C. el moderno criptoanálisis, a partir del descubrimiento de que cada lengua tiene una frecuencia característica de aparición de sus letras. Así, bastaba con contar el número de veces que aparecía cada símbolo, letra o número en un texto cifrado para saber realmente cuál era la letra subyacente, independientemente de su apariencia.

BERNARDO

Ya entiendo porqué se dice que la cifra monoalfabética es insegura.

3. MÉTODOS DE CIFRA POLIALFABÉTICA

ALICIA

Obviamente, a partir de este momento los cifrados monoalfabéticos estaban rotos, habiendo ganado los criptoanalistas la batalla a los criptógrafos.

Naturalmente, los criptógrafos no podían prescindir de los métodos de sustitución, relegando toda la criptografía a la transposición, de modo que desarrollaron los métodos polialfabéticos.

BERNARDO

Entonces, ¿se podría hacer un mecanismo criptográfico más seguro si se utilizan muchos alfabetos diferentes para enmascarar la frecuencia de aparición de esas letras?

ALICIA

Exacto, y no es tan difícil. En los métodos polialfabéticos, cada vez que aparece una letra en claro se escoge un carácter cifrado (sea otra letra, número o símbolo arbitrario) de entre un conjunto finito de ellos. Así, a una letra en claro, pongamos la "a", unas veces será sustituida por ejemplo por la "x", pero otras veces lo será por la "y" o por el número 10. Todo ello siguiendo un estricto patrón para que no haya ambigüedades a la hora de descifrar. Por consiguiente, el conteo del número de veces que aparece cada símbolo cifrado no aportará ningún conocimiento al criptoanalistas.

BERNARDO

¿Y qué sistemas polialfabéticos fueron los más conocidos?

ALICIA

Los métodos que siguen este esquema fueron ideados por una de las figuras más notorias del Renacimiento: Leone Battista Alberti, inventor del primer artificio de cifrado: el cifrado de disco. Consistía en dos coronas circulares concéntricas; la interior llevaba grabado el alfabeto cifrado y era fija; la exterior llevaba impreso el alfabeto en claro y podía girar sobre su centro. Así, cada letra del alfabeto en claro se correspondía con otra del alfabeto cifrado, pudiéndose cambiar esta correspondencia al girar la corona exterior. Por tanto, se trataba de un método polialfabético.

Otro sistema muy popular fue el creado por Blaise de Vigenère basado en una tabla en la que se leía la letra de intersección del texto en claro con una clave que indicaba qué alfabeto se usaba.

4. USO EXTENDIDO DE LA CRIPTOGRAFÍA

BERNARDO

Alicia, ¿es cierto, entonces, que la consolidación de la escritura secreta fue un instrumento imprescindible de poder en la creación de los estados modernos, la comunicación entre ejércitos y la presencia de embajadas permanentes?

ALICIA

Así es. Se crearon los secretarios de cifra, responsables del cifrado de la correspondencia entre Reyes, ministros y embajadores, así como de criptoanalizar la correspondencia intervenida de otros estados.

Por ejemplo, en España, el primer Secretario de Cifra conocido es Pérez de Almazán nombrado por los Reyes Católicos. Pero es Felipe II quien renueva y da un gran impulso a las técnicas de cifrado, poniéndolas bajo la responsabilidad del Secretario de Cifra D. Luis Valle de la Cerda. Establece la Cifra General (para la comunicación entre él mismo, sus Secretarios, sus Embajadores y altos militares) y la Cifra Particular, para las comunicaciones más confidenciales

entre él y alguno de los anteriores dignatarios. Además, por seguridad, cambia frecuentemente todas estas cifras.

BERNARDO

¿Y en otros países también utilizaban estos mecanismos de protección?

ALICIA

Claro que sí. Lo mismo ocurrió con los restantes reinos europeos. Así, Walsinghan con Isabel I de Inglaterra y Viétè con Enrique III y Enrique IV en Francia hicieron de la criptología una materia imprescindible en las Cortes y embajadas europeas.

BERNARDO

Sé que hubo alguna máquina de cifrar muy famosa. ¿Cuándo comienzan a aparecer las máquinas de cifrar?

ALICIA

Aunque la criptología siguió avanzando durante el resto de la Edad Moderna y Contemporánea, hay que esperar al siglo XX para presenciar progresos sustanciales en las técnicas de cifrado. En efecto, éste es el siglo de las máquinas, acaparando una de ellas, la casi mítica Enigma, la mayor atención de cuantas máquinas han existido y existen en la actualidad.

Enigma fue una máquina de cifrado patentada por Arthur Scherbius en 1918, y adoptada por el ejército alemán en 1923, quien llegó a tener varios millares de ella durante la II Guerra Mundial, en la que jugó un papel esencial.

BERNARDO

Eso me suena. Los alemanes aprovecharon la Guerra Civil española para probarla en situaciones bélicas, para lo cual dotaron de varios ejemplares a las tropas rebeldes.

ALICIA

Cierto. La historia de esta máquina y su uso es apasionante, ya tendremos tiempo de estudiarla en detalle. De hecho, es precisamente después de la II Guerra Mundial cuando se producirán los avances teóricos más significativos de la historia de la criptología, por ejemplo en 1948 Claude Shannon establecerá las bases teóricas de la criptología, pero éste es otro tema.

BERNARDO

Bueno Alicia. Creo que por hoy es suficiente.

ALICIA

Tienes razón Bernardo ya seguiremos en otro momento. En la Web de intypedia encontrarás un documento con información complementaria sobre este apasionante tema.

Hasta el próximo vídeo… ¡Adiós!

BERNARDO

¡Hasta pronto!

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. Arturo Ribagorda Garnacho de la Universidad Carlos III de Madrid, España.

Madrid, España, septiembre de 2010

http://www.intypedia.com

http://twitter.com/intypedia