**VÍDEO intypedia002es**

**LECCIÓN 2: SISTEMAS DE CIFRA CON CLAVE SECRETA**

**AUTOR: Fausto Montoya Vitini**

**Consejo Superior de Investigaciones Científicas, Madrid, España**

**ALICIA**

Hola, bienvenidos a intypedia. La lección de hoy corresponde a los fundamentos de la criptografía simétrica. ¡Acompáñanos!

## 1. ANALOGÍA DE LA CRIPTOGRAFÍA CON LOS CANDADOS

**BERNARDO**

Hola, Alicia. Tengo este sobre con una carta cuyo contenido secreto quiero hacerle llegar a un amigo. Pero tengo miedo de que alguien pueda abrirla y leer el contenido. ¿Qué podría hacer?

**ALICIA**

Te servirá esta caja a prueba de robo. Puedes meter dentro tu carta y enviarle a tu amigo la caja.

**BERNARDO**

Parece muy robusta, pero ¿no podría ocurrir que alguien la abriera y robara la carta?

**ALICIA**

No te preocupes, para evitarlo la cerraremos con este candado con combinación. ¿Lo ves? De esta manera, sólo el que conozca la combinación podrá abrir el candado y leer la carta.

**BERNARDO**

¿Estás segura de que nadie podrá abrirlo aunque no conozca la combinación?

**ALICIA**

¡Por supuesto que no podrá! Ha sido diseñado por el mayor experto del mundo en candados. Es totalmente indestructible. Si alguien olvida la combinación, nadie podrá abrirlo.

**BERNARDO**

¿Y no pueden probarse todas las posibles combinaciones hasta dar con la correcta?

**ALICIA**

Tienes razón. Ése podría ser un problema. Precisamente para evitarlo, el candado usa una combinación de 8 dígitos. Eso significa que existen 10 elevado a la 8 combinaciones posibles, o lo que es lo mismo, 1 seguido de 8 ceros, o sea, 100 millones de combinaciones.

**BERNARDO**

¿Tú crees que serán suficientes?

**ALICIA**

Claro que sí. Fíjate. Si tardas 10 segundos en probar cada combinación, te llevará más de 31 años probarlas todas. En promedio, tendrías que probar la mitad de combinaciones para acertar, por lo que para dar con la combinación correcta necesitarías más de 15 años, ¡eso sin parar ni un instante para comer, dormir o ir al baño!

**BERNARDO**

¡Vaya! Sí que parece seguro. Me has convencido, Alicia. Creo que voy a enviarle la carta a mi amigo dentro de tu caja cerrada con ese fantástico candado. Ahora estoy seguro de que nadie que no conozca la combinación podrá abrirlo y leer mi carta.

## 2. FUNDAMENTOS DE LA CRIPTOGRAFÍA DE CLAVE SIMÉTRICA

**BERNARDO**

Alicia, quiero enviarle ahora un mensaje por Internet a un amigo sin que pueda leerlo nadie más, pero no sé cómo hacerlo. El método de la caja y el candado que usé para la carta creo que no me servirá para un mensaje digital.

**ALICIA**

No, un candado no te servirá en Internet, pero puedes usar el equivalente digital del candado.

**BERNARDO**

¿Ah, sí? No sabía que existieran candados digitales.

**ALICIA**

La criptografía es el equivalente de un candado y su combinación.

**BERNARDO**

¿Y cómo es eso posible?

**ALICIA**

Verás. Cuando quieres proteger un mensaje digital, puedes cifrarlo utilizando un algoritmo de cifrado. Igual que existen muchos tipos de candados, existen muchos tipos de algoritmos de cifrado. Para cifrar mensajes de correo, archivos del disco duro, registros de una base de datos, y en general para cifrar grandes cantidades de datos, se utiliza un tipo de algoritmo de cifrado conocido como de clave secreta o simétrico.

**BERNARDO**

¿Por qué se le llama simétrico?

**ALICIA**

Porque se utiliza la misma clave de cifrado para cifrar y para descifrar el mensaje.

**BERNARDO**

O sea, que si yo cifro mi mensaje usando un algoritmo simétrico, sólo podrá descifrarlo otra persona que conozca la misma clave secreta que yo he usado, ¿no es eso?

**ALICIA**

Exacto.

**BERNARDO**

¿Y no hay peligro de que pueda descifrarse el mensaje sin conocer mi clave secreta?

**ALICIA**

Eso depende de dos factores. El primero de ellos es la robustez del algoritmo.

**BERNARDO**

¿Qué es lo que hace que un algoritmo sea más o menos robusto?

**ALICIA**

Es la manera como haya sido diseñado. Como ya hemos visto en la Lección 1 de intypedia, durante muchos siglos se vinieron usando dos tipos de operaciones de cifrado: sustitución y transposición.

**BERNARDO**

Es verdad, y además la sustitución y la permutación por sí solas no eran suficientes para cifrar un texto de manera segura.

**ALICIA**

Efectivamente. La robustez del algoritmo de cifrado puede mejorarse considerablemente si se combinan ambas operaciones, usando sustitución y transposición repetidamente sobre el mismo mensaje. Algunos algoritmos modernos de cifrado, como por ejemplo el AES o el Triple DES, utilizan múltiples vueltas de cifrado en las que se combinan las dos operaciones.

**BERNARDO**

¿Por qué hacen eso?

**ALICIA**

El objetivo es conseguir lo que se conoce como difusión y confusión.

**BERNARDO**

Alicia, estoy confundido.

**ALICIA**

Idealmente, un texto cifrado debe tener una apariencia totalmente aleatoria.

**BERNARDO**

¿Como si un mono se hubiera sentado en una máquina de escribir?

**ALICIA**

Sí, eso. Debe eliminarse del texto cifrado cualquier pista o patrón, lo que significa que debe eliminarse cualquier relación estadística entre el mensaje original y su texto cifrado. La combinación de la sustitución y transposición difunde, es decir, distribuye o dispersa, la estructura estadística del mensaje sobre la totalidad del texto cifrado.

**BERNARDO**

Entiendo la difusión: oculta la relación entre el texto en claro y el texto cifrado. ¿Y para qué sirve la confusión?

**ALICIA**

Dado que normalmente el criptoanalista sólo dispondrá del texto cifrado y del conocimiento del funcionamiento del algoritmo de cifrado utilizado, intentará dar con la clave secreta. La confusión busca ocultar la relación entre el texto cifrado y la clave secreta.

**BERNARDO**

¿Qué sucedería si se cambia un solo bit de la clave?

**ALICIA**

En ese caso debería cambiar en promedio la mitad de los bits del texto cifrado. Los algoritmos de cifrado que se sirven de la confusión y de la difusión se suelen llamar cifradores de producto. Cada aplicación de la confusión y de la difusión se produce en una vuelta de cifrado. Los cifradores modernos suelen utilizar muchas vueltas de cifrado o iteraciones.

**BERNARDO**

Por tanto, si un algoritmo está bien diseñado, pasará como con el candado: un texto cifrado sólo se podrá descifrar si se conoce la clave.

**ALICIA**

Eso es. En la buena criptografía se sigue siempre el Principio de Kerckhoffs: la seguridad del sistema debe recaer en la seguridad de la clave, debiéndose suponer conocidos el resto de los parámetros del sistema criptográfico. O en otras palabras, como dijo Claude Shannon: “el adversario conoce el sistema”.

## 3. LOS ATAQUES POR FUERZA BRUTA

**BERNARDO**

Alicia, ¿y puede un atacante probar todos los posibles valores de la clave?

**ALICIA**

Si recuerdas, te había dicho que la seguridad de un algoritmo de cifrado depende de dos factores. El primero ya lo hemos visto: es el diseño del algoritmo. El segundo factor es la longitud de la clave utilizada. Cuando un criptoanalista no puede encontrar fallos en el algoritmo, siempre le queda recurrir a un ataque de fuerza bruta. Se trata de un método sin elegancia, que no ataca el algoritmo en sí, sino que busca exhaustivamente todos los posibles valores de la clave hasta dar con la correcta.

¿Te acuerdas del candado con una combinación de 8 dígitos? Eso significa que hay 100 millones de combinaciones posibles. Son tantas que probarlas todas a mano llevaría muchos años. Claro

que las claves de los algoritmos de cifrado no se prueban a mano, como con el candado, sino que se le deja el trabajo a un ordenador.

**BERNARDO**

Y como los ordenadores son mucho más rápidos que los humanos, habrá que utilizar claves más grandes.

**ALICIA**

Desde luego. Por eso es tan importante elegir claves suficientemente largas, de manera que con la potencia de cálculo actual sea imposible probarlas todas en un tiempo razonable. Éste fue el problema del algoritmo simétrico DES. Su longitud de clave fue establecida en 56 bits. Hay que tener en cuenta que DES fue diseñado en el año 1976, y que en aquellos tiempos resultaba impensable que un ordenador pudiera probar 2 elevado a la 56 combinaciones posibles de la clave. Pero claro, la informática fue evolucionando y en el año 1998 se diseñó un dispositivo capaz de obtener la clave correcta en 56 horas. Sucesivos avances en computación paralela han conseguido reducir el tiempo a menos de un día. Actualmente, una clave simétrica de ese tamaño es completamente insegura.

**BERNARDO**

¿Cómo de larga debe ser hoy una clave para estar a salvo de los ataques de fuerza bruta?

**ALICIA**

Hoy en día se estima que claves de 128 bits de longitud o más garantizarán la seguridad por muchos años. De hecho, algunos algoritmos permiten seleccionar a voluntad la longitud de la clave, como el estándar AES que se base en el algoritmo criptográfico Rijndael. Piensa que cada bit que se añade a la clave dobla el tamaño del espacio de claves posibles.

**BERNARDO**

Por consiguiente, si el diseño es robusto y la longitud de la clave es suficientemente larga, ¿podemos considerar que el algoritmo es seguro?

**ALICIA**

En teoría, sí.

## 4. EL PROBLEMA DE LA DISTRIBUCIÓN DE CLAVES

**BERNARDO**

Alicia, ya he cifrado el mensaje con la clave secreta pero me ha surgido un problema. ¿Cómo hago para enviarle a mi amigo la clave secreta que he utilizado para cifrar el mensaje?

**ALICIA**

Bernardo, acabas de toparte con el mayor problema al que históricamente se ha enfrentado la criptografía. Se conoce como el problema de distribución de la clave.

**BERNARDO**

¿De qué me sirve utilizar el mejor algoritmo de cifrado del mundo si no puedo compartir mi clave con el destinatario del mensaje?

**ALICIA**

¡Bravo! Lo has formulado perfectamente. Durante siglos la criptografía se ha enfrentado con poco éxito a este problema, hasta que en los 70 se inventó la criptografía de clave pública.

**BERNARDO**

¿Cómo funciona ese tipo de criptografía?

**ALICIA**

Paciencia. Eso lo veremos en la próxima lección. Por hoy ya hemos aprendido varias cosas básicas de lo que se conoce como cifra simétrica.

En el sitio Web de intypedia encontrarás información complementaria. Nos vemos en la siguiente lección.

**BERNARDO**

¡Adiós!

---

Guión adaptado al formato intypedia a partir del documento entregado por el Dr. Fausto Montoya Vitini del Consejo Superior de Investigaciones Científicas en Madrid, España.

Madrid, España, octubre de 2010

http://www.intypedia.com

http://twitter.com/intypedia

creative commons
Attribution
Noncommercial
No derivative works