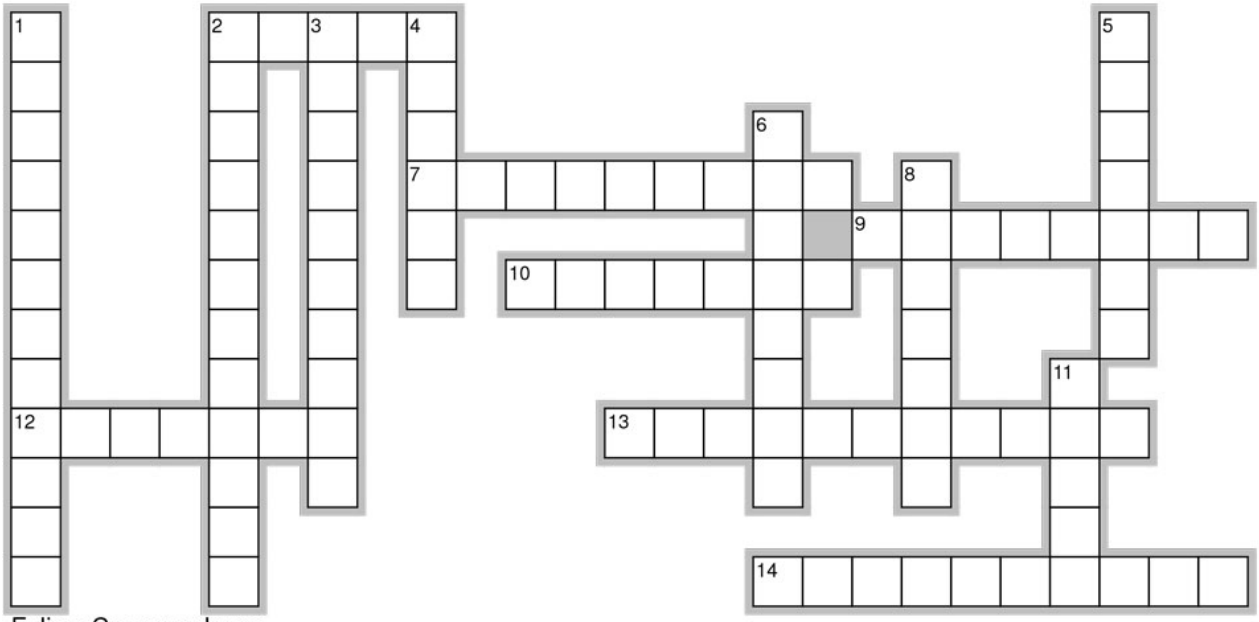
Encriptando secretos

14/05/2024

ENCRIPTANDO SECRETOS

A. REQUENA & VALLE DE ELDA © 2024



EclipseCrossword.com

HORIZONTALES

2. En el siglo XIX, el cifrado Vigenère, desarrollado en el siglo XVI, pero popularizado en el XIX, utilizaba una palabra de este tipo, para crear un cifrado polialfabético
7. En la antigüedad, uno de los primeros usos documentados de la criptografía fue el cifrado de César, utilizado por él para comunicarse con los suyos.
9. La de la encriptación es fascinante y abarca desde la antigüedad hasta la era digital moderna.
10. La de Enigma por parte de los aliados, liderada por Alan Turing y su equipo en Bletchley Park, es uno de los puntos de inflexión más famosos de la criptografía.
12. El de sustitución monoalfabética, que reemplaza cada letra del texto original por otra letra específica, fue ampliamente utilizado.
13. La "prueba de conocimiento cero", permite a una parte (el probador) convencer a otra parte (el verificador) de que posee cierta de ella, sin revelar ningún detalle sobre la información misma.
14. La criptografía cuántica y las tecnologías emergentes prometen revolucionar aún más la seguridad en estas comunicaciones.

VERTICALES

1. Durante la Edad Media, ésta se volvió más sofisticada.
2. En la primera y segunda guerra mundial, ésta tuvo un papel crucial.
3. Los de clave pública, como RSA, introducidos en la década de 1970, permitieron un intercambio de claves seguro, sin la necesidad de un canal seguro previo.
4. Durante la Segunda Guerra Mundial, esta máquina, utilizada por los alemanes, y la máquina japonesa Purple, fueron centrales en las operaciones criptográficas.
5. En esta era, con el advenimiento de la computación, la criptografía se ha transformado sustancialmente.
6. En el marasmo actual de datos digitales que casi todo el mundo maneja, resulta paradógico que se quieran mantener así.
8. En nuestro siglo XXI la criptografía es omnipresente en esta tecnología, protegiendo la transmisión de información en Internet.
11. En el Renacimiento, siglo XV, Leon Battista Alberti, diseñó un disco cifrador que utilizaba un alfabeto de este tipo.

En el marasmo actual de datos digitales que casi todo el mundo maneja, resulta paradógico que se quieran mantener secretos. Pero es una necesidad y apremiante, dadas las opciones que se han abierto a los ciberdelincuentes que están obligando a algo tan saludable como que las personas tomen conciencia y llegan a saber qué es lo que manejan cuando usan el ordenador o el propio teléfono móvil, sin ir más lejos.

La historia de la encriptación es fascinante y abarca desde la antigüedad hasta la era digital moderna. En la antigüedad, uno de los primeros usos documentados de la criptografía fue el cifrado de César, utilizado por él para comunicarse con sus generales. Este método implicaba desplazar cada letra del mensaje original por un número fijo de posiciones en el alfabeto. Durante la Edad Media, la encriptación se volvió más sofisticada. El cifrado por sustitución monoalfabética, que reemplaza cada letra del texto original por otra letra específica, fue ampliamente utilizado. Un ejemplo notable es el cifrado de Alberti, considerado uno de los primeros cifrados polialfabéticos. En el Renacimiento, siglo XV, Leon Battista Alberti, diseñó un disco cifrador que utilizaba un alfabeto móvil, lo que complicaba mucho la tarea de descifrar los mensajes sin conocer el método exacto utilizado. En el siglo XIX, el cifrado Vigenère, desarrollado en el siglo XVI, pero popularizado en el XIX, utilizaba una palabra clave para crear un cifrado polialfabético, que era mucho más difícil de romper que los cifrados anteriores. En la primera y segunda guerra mundial, la criptografía tuvo un papel crucial. En la Primera Guerra Mundial, el cifrado ADFGVX fue utilizado por Alemania. Durante la Segunda Guerra Mundial, la máquina Enigma, utilizada por los alemanes, y la máquina japonesa Purple, fueron centrales en las operaciones criptográficas. La ruptura de Enigma por parte de los aliados, liderada por Alan Turing y su equipo en Bletchley Park, es uno de los puntos de inflexión más famosos de la criptografía. En la era Moderna, con el advenimiento de la computación, la criptografía se ha transformado sustancialmente. Los algoritmos de clave pública, como RSA, introducidos en la década de 1970, permitieron un intercambio de claves seguro, sin la necesidad de un canal seguro previo. Esto ha sido fundamental para el desarrollo de Internet y el comercio electrónico. En nuestro siglo XXI la criptografía es omnipresente en la tecnología digital, protegiendo la transmisión de información en Internet, la seguridad de las transacciones bancarias, la integridad de las comunicaciones móviles y mucho más. Además, la criptografía cuántica y las tecnologías emergentes prometen revolucionar aún más la seguridad en las comunicaciones digitales. La evolución de la criptografía es un testimonio de la importancia de la seguridad de la información y refleja cómo las necesidades y los desafíos tecnológicos han impulsado la innovación en este campo a lo largo de la historia.

¿Cómo asegurarnos hoy de que el mensaje que enviamos a alguien se mantiene secreto, incluso si es interceptado? Desde los años setenta, dos personas que quieran comunicarse de forma privada deben ponerse de acuerdo, previamente en la clave para encriptar y desencripótar, lo que debe hacerse confidencialmente. Si no es así, el mensaje que contendría la clave podría ser interceptado y a partir de ahí, muy fácil de descifrar los siguientes. Esto es muy razonable, pero muy artesanal e impropio de la era de la hiperconexión en que vivimos. Ciertamente, nuestra experiencia personal, por casi todos compartida, es que cuando accedemos a Google no obtenemos ninguna clave secreta, pero la comunicación es segura. ¿Cómo es esto? La respuesta es gracias a una idea revolucionario denominada “criptografía de clave pública”.



Imagen creada con ChatGPT con DALL-E

La cosa es que, en lugar de una clave secreta, se usa un par de claves con una especial relación matemática, de forma que un mensaje encriptado usando una de ellas, solamente puede ser desencriptado usando la otra clave. No hace falta verse con el otro para pactar la clave y, en cambio, podemos probar que el mensaje es nuestro.

A finales de la década de los setenta del siglo pasado, los criptógrafos desarrollaron los métodos de encriptación con clave pública demostrando que no hay forma de “reventar” los códigos que no sea resolviendo problemas

de una dificultad elevada, como es la descomposición de números grandes en sus factores primos. Permaneció hasta la década de los ochenta el cómo compartir selectivamente información secreta, hasta que se descubrieron nuevas vías. En 1985, Shafi Goldwasser, Silvio Micali and Charles Rackoff, introdujeron la idea de un nuevo protocolo denominado "prueba de conocimiento cero", que permite a una parte (el probador) convencer a otra parte (el verificador) de que posee cierta información, sin revelar ningún detalle sobre la información misma. Este tipo de prueba es fundamental para proteger la privacidad y es ampliamente utilizado en aplicaciones de seguridad y criptomonedas, entre otros campos. Se basa en tres principios fundamentales: a) Completitud: si la afirmación es verdadera, un probador honesto siempre convencerá al verificador; b) Solidez: si la afirmación es falsa, un probador deshonesto no podrá convencer al verificador, excepto con una pequeña probabilidad; c) Cero conocimiento: si la afirmación es verdadera, el verificador no aprenderá nada más allá del hecho de que la afirmación es verdadera, sin obtener ninguna información adicional sobre la prueba misma.

Un ejemplo ilustra convenientemente: El Problema de las cuevas, conectadas por un camino secreto. Imaginemos que hay dos cuevas conectadas por un pasaje secreto. En una entrada de la cueva, se encuentra el probador (Alberto) y en la otra, el verificador (Víctor). Alberto quiere probar a Víctor que conoce el paso secreto entre las dos cuevas sin revelarle cuál es. Para hacer esto, Víctor espera fuera de una entrada y le dice a Alberto que entre por una de las entradas. Luego, elige al azar una de las dos entradas y le pide a Alberto que salga por esa entrada. Si Alberto realmente conoce el paso secreto, puede usarlo para salir por la entrada que Víctor ha elegido, demostrando que conoce el secreto sin revelar su ubicación.

Las pruebas de conocimiento cero tienen varias aplicaciones prácticas en: a) criptomonedas, utilizadas en algunos protocolos para aumentar la privacidad de las transacciones, como en Zcash, donde se pueden validar transacciones sin revelar las partes involucradas ni las cantidades transferidas; b) autenticación, ya que permiten a los usuarios probar su identidad o permisos sin revelar información sensible como contraseñas; c) en votación electrónica, ya que garantizan que los votos sean válidos sin revelar por quién votó cada persona. Estas pruebas son un ejemplo fascinante de cómo la criptografía puede ser utilizada para garantizar la seguridad y la privacidad de la información en un mundo digital.

En 2020, se propuso un esquema seguro de encriptación denominado "ofuscación indistinguible", que imposibilita llamar a otros programas para que lleven a cabo la misma tarea. El objetivo de la ofuscación indistinguible es transformar cualquier programa en otro que sea funcionalmente equivalente, pero cuya lógica interna sea imposible de discernir o revertir técnicamente. Teóricamente, si se logra una ofuscación indistinguible perfecta, sería imposible determinar cualquier cosa sobre el programa original, más allá de lo que se puede observar mediante su entrada y salida.

La primera propuesta formal de un esquema de ofuscación indistinguible fue realizada utilizando algo conocido como un "liberación gradual" de "protectores" que protegen fragmentos del código. Sin embargo, esta aproximación se reveló inviable bajo ciertas condiciones teóricas. Posteriormente, se han explorado enfoques que utilizan objetos matemáticos complejos como los "mapas multilineales" para crear ofuscadores que se acercan más a la propiedad de indistinguibilidad.

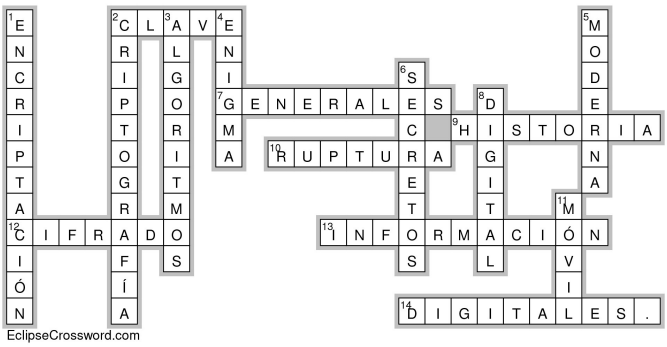
Desde el punto de vista práctico, sus aplicaciones se han dado en: a) protección de la propiedad intelectual, ya que la ofuscación indistinguible puede proteger el software contra la ingeniería inversa, preservando la propiedad intelectual; b) seguridad de software, ya que ayuda a proteger algoritmos críticos y datos sensibles dentro de las aplicaciones, especialmente en entornos hostiles donde el software puede ser examinado y c) habilitación de la computación en entornos no confiables, puesto que permite ejecutar programas en máquinas no confiables mientras se protege la lógica del programa.

Las limitaciones, que todavía se señalan afectan a aspectos como: a) rendimiento, porque la ofuscación puede introducir una sobrecarga significativa en términos de rendimiento del programa; b) la complejidad teórica y práctica, porque la creación de ofuscadores indistinguibles que sean seguros y eficientes es extremadamente retadora y c) la seguridad de los esquemas propuestos depende profundamente de supuestos matemáticos no probados y podría ser vulnerable si estos supuestos son refutados.

En resumen, la ofuscación indistinguible es una de las áreas más teóricamente intrigantes y desafiantes de la criptografía moderna, con un potencial considerable para transformar la seguridad del software, aunque aún enfrenta significativos desafíos prácticos y teóricos. Son cuestiones muy relevantes que nos implica a todos y conviene comprender el alcance.

ENCRIPTANDO SECRETOS

A. REQUENA & VALLE DE ELDA © 2024



EclipseCrossword.com