Daniel Alejandro Osornio López
0244685@up.edu.mx 2 / Oct / 2023

La importancia de la criptografia

En la película pudimos ver un poco sobre el trabajo que realizó Alan Turing durante la segunda guerra mundial. Junto con investigadores y matemáticos se dedicó a diseñar una máquina que permitiera descifrar los mensajes de los alemanes.

Las comunicaciones alemanas estaban cifradas usando una máquina conocida como *Enigma*, esta podía ser programada, dependiendo de las configuraciones se mapeaba cada letra a otro carácter, de forma que el mensaje cifrado era irreconocible.

Al inicio usaban graficas de frecuencia de los carácteres cifrados para intentar identificar cada letra en base a las tablas de carácteres más comunés (en este caso en el Alemán).

Lo que Turing logró fue que, conociendo mensajes/textos que siempre se incluían entre las muchas comunicaciones de los alemanes, podía buscar rápidamente la combinación usada en la máquina cifradora, de forma que ahora podía descifrar los mensajes, es decir, pasar de tener un conjunto de caracteres sin sentido a información.

La pelicula nos introduce a la criptografía, la cual es una técnica para lograr la confidencialidad de mensajes [1].

Para Turing, el tener información sobre los movimientos de los alemanes, permitió salvar millones de vidas, y acortar un estimado de 2 años la guerra, pues el conocimiento que obtenian podía ser usado para tomar contra-decisiones que sacaran ventaja de las posiciones del régimen Nazi.

Asi mismo, en nuestro día a día, en un mundo hyper-conectado se transmite una gran cantidad de secretos. Miles de millones de personas de todo el mundo utilizan la criptografía a diario para proteger sus datos e información. Además de ser extremadamente útil, también se considera muy frágil, ya que los sistemas criptográficos pueden verse comprometidos por errores de programación o especificación [1].

Entre los mensajes que se protegen se puede encontrar, por ejemplo, información sensible de una persona, que permite identificarla como que padece cierta enfermedad, que sigue cierta religión, o cualquier otro dato que permita discrimarla, por ejemplo, negándole un empleo, educación, o demás situaciones que atenten contra su dignidad humana.

La información, usada por partes malignas, en cualquier área, sea entre personas o instituciones, puede llevar a estos agentes a tomar decisiones egoístas que afectan de forma negativa a los demás. Por poner un ejemplo, destruyendo la competencia, formando monopolios que no mejoran sus servicios porque saben que no hay nadie más que ofrezca lo mismo.

Con la criptografía se han desarrollado sistemas complejos que permiten la distribución de secretos en forma de mensajes o la autenticación de paquetes, aplicaciones y demás entre individuos y organizaciones [2].

Por ejemplo, es gracias a la criptografía que podemos tener programas como https://www.gnupg.org/, que permiten en sistemas como https://wiki.archlinux.org/title/pacman, o https://wiki.archlinux.org/title/pacman para la dostribución de software de forma que todos los involucrados pueden estar seguros de que se reciben los paquetes de forma integra, y que no contienen código maligno que puede afectar los sistemas de la organización.

Firmas digitales, cifrado de mensajes, sistemas de llaves publicas, e infinidad de algoritmos y sistemas nos permiten tener un mundo donde se puede intercambiar secretos entre personas e

instituciones. Es asi que podemos asegurar la integridad de la información, su confidencialidad, o tener formas de autenticación. De manera que se forma una seguridad de red y de datos fiable, sólida y robusta [1].

Bibliografía

[1] A. M. Qadir, and N. Varol, "A review paper on cryptography," in *2019 7th Int. Symp. Digit. Forensics Secur. (ISDFS)*, vol. 0, 2019, pp. 1–6, doi: 10.1109/ISDFS.2019.8757514.

[2] G. C. Kessler, "An overview of cryptography," 2003.