# Descifrado de contraseña

*Keywords: combinatoria, probabilidad y estadística, combinatoria, regla del producto*

Con el desarrollo de Internet y la comunicación a larga distancia surgió la necesidad de verificar si la persona que está al otro lado del monitor es realmente la persona con la que nos comunicamos o sólo alguien que finge ser un conocido. De forma similar, cuando se presentan dos espías amigos en un territorio extranjero, se ofrece la posibilidad de utilizar una contraseña. Hoy en día, uno se encuentra a diario con contraseñas en el ciberespacio, al entrar en el correo electrónico, las cuentas de la escuela o el trabajo, o la banca en línea.

Pero, ¿garantiza la mera existencia de contraseñas la autenticación segura de los usuarios? Los continuos informes sobre nuevos hackeos y cuentas robadas nos dicen que no. Los métodos por los que los atacantes llegan a la contraseña de un usuario pueden dividirse básicamente en dos grupos, dependiendo de si es robada o adivinada. Como el siguiente problema trata del segundo caso, vamos a examinarlo más detenidamente.

*El ataque de fuerza bruta*, que conoceremos en la tarea, consiste en probar todas las contraseñas posibles. Dependiendo de la potencia de cálculo del ordenador y del software utilizado, la velocidad de las pruebas puede oscilar entre unos pocos miles y varios cientos de miles de millones de contraseñas por segundo. Así, contraseñas muy cortas pueden ser adivinadas por el ordenador en un tiempo relativamente corto (es decir, instantáneamente o en cuestión de horas).

Una forma más sofisticada de ataque de fuerza bruta es el *ataque de diccionario*, en el que el ordenador no prueba contraseñas al azar, sino que las selecciona de un diccionario de palabras preparadas. Además de palabras reales, éste contiene contraseñas de uso común como `password1234` o `password`. Si la contraseña de la víctima está en el diccionario del atacante, el tiempo de descifrado se reduce significativamente en comparación con un ataque de fuerza bruta convencional.

Una protección esencial contra ambos tipos de ataques es el uso de contraseñas suficientemente largas (al menos 12 caracteres) compuestas por letras mayúsculas y minúsculas, números y otros caracteres especiales.


**Figura 1:** Hackear

## Tarea

El programa hacker, en un ataque de fuerza bruta, tiene garantizado descifrar una contraseña de ocho caracteres formada por letras mayúsculas y minúsculas del alfabeto inglés en unos 22 minutos. (Supongamos que el conjunto de caracteres del teclado que se van a probar se puede establecer en la configuración del programa).


The portal Math4U is developed within the international projects of the Department of Applied Mathematics (VSB-Technical University of Ostrava) and other institutions in Czechia, Poland, Slovakia, and Spain.
Funded by the European Union

**Ejercicio 1.** ¿Cuántas contraseñas intenta el programa en 1 segundo?

**Ejercicio 2.** ¿Cuánto tardaría el programa en descifrar una contraseña de ocho caracteres si también permitimos utilizar dígitos?

**Ejercicio 3.** ¿Cuántos caracteres debería tener una contraseña formada por números y letras minúsculas o mayúsculas del alfabeto inglés para ser lo suficientemente fuerte, es decir, para garantizar que se tarda al menos 100 años en descifrarla? ¿Cómo cambia el resultado si permitimos el posible uso de otros 40 caracteres especiales del teclado?

# Referencias y literatura

## Literatura


- Raza, Mudassar & Iqbal, Muhammad & Sharif, Muhammad & Haider, Waqas. (2012). A Survey of Password Attacks and Comparative Analysis on Methods for Secure Authentication. *World Applied Sciences Journal*. 19. 439–444.
- National Cyber and Information Security Agency. *Bezpečný pohyb v kybersvětě* [online]. Accesible de `https://www.nukib.cz/cs/kyberneticka-bezpecnost/vzdelavani/verejnost/` [cit. 30. 6. 2023].


## Fuentes de imágenes


- Hacking password, Santeri Viinamäki, CC BY-SA 4.0, accesible de `https://commons.wikimedia.org/wiki/File:Hacking_password_illustration.jpg` [cit. 30. 6. 2023].



The portal Math4U is developed within the international projects of the Department of Applied Mathematics (VSB-Technical University of Ostrava) and other institutions in Czechia, Poland, Slovakia, and Spain.

Funded by the European Union