**Łamanie haseł archiwum .zip metodą brute force**

Zdarza się że czasem z różnych powodów nie znamy / pamiętamy hasła do zaszyfrowanego archiwum .zip.

Najprostszym sposobem na „odgadnięcie” hasła jest próbowanie po kolei wszystkich możliwych haseł. Jako ludzie w praktyce nie jesteśmy jednak w stanie wypróbować ich ręcznie: dla 6 znakowego hasła liczba możliwych haseł to aż około 730 000 000 000.

**Pytanie na ocenę celującą**: ile jest możliwych haseł 5 znakowych składających się z małych i dużych liter (bez polskich znaków) i cyfr?

Zakładając (dość optymistycznie) że sprawdzenie jednego hasła zajęłoby sekundę, skończylibyśmy po 23 latach.

Wykorzystamy komputer, żeby spróbował wyszukać to hasło za nas. Skorzystamy z programu **John the Ripper** dystrybuowanego na licencji Open Source. Program ten jest bardzo rozbudowany i pozwala na odzyskanie haseł do wielu różnych rozszerzeń plików.

1. Wchodzimy na stronę <https://www.openwall.com/john/>
2. Pobieramy plik (wersja zip) **1.9.0-jumbo-1 64-bit Windows binaries in**[**7z, 22 MB**](https://www.openwall.com/john/k/john-1.9.0-jumbo-1-win64.7z)**(**[**signature**](https://www.openwall.com/john/k/john-1.9.0-jumbo-1-win64.7z.sign)**) or**[**zip, 63 MB**](https://www.openwall.com/john/k/john-1.9.0-jumbo-1-win64.zip)**(**[**signature**](https://www.openwall.com/john/k/john-1.9.0-jumbo-1-win64.zip.sign)**)**
3. Wypakowujemy archiwum w wybranym przez siebie katalogu
4. Za pomocą 7zip stwórz 6 plików .zip: jeden z hasłem 1 cyfrowym, drugi z 2 cyfrowym, …, szósty z 6 cyfrowym. Hasła wybierz losowo