

Zrób sobie szyfr

Za miesiąc, 9 lutego, będziemy obchodzili Dzień Bezpiecznego Internetu. Przy tej okazji warto zadbać o hasła, których używamy do logowania się na licznych portalach. Powinny być one silne, czyli spełniać kilka warunków:

- być długie na przynajmniej 8 znaków
- być złożone, zawierać małe i wielkie litery, cyfry, znaki specjalne
- składać się z kilku słów
- nie zawierać 3 kolejnych znaków na klawiaturze (np.qwe)
- być nieoczywiste, tj. inne niż nazwa użytkownika czy danymi osobowymi jego rodziny

Najgorsze (i najczęściej używane) hasła:

123456

password

qwerty

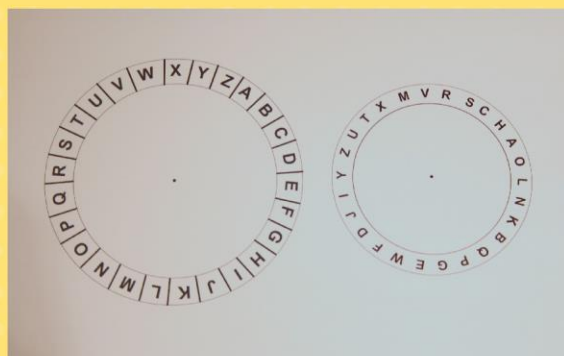
11111

123456789

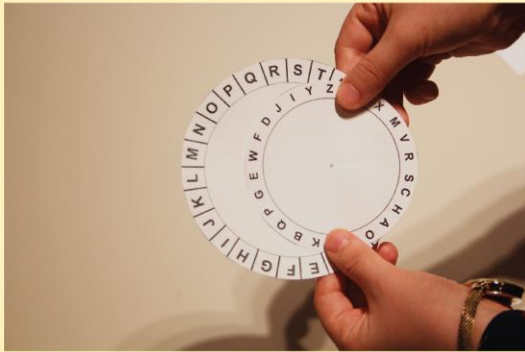
Dobrze, jeśli do każdej witryny mamy osobne hasło i nie jest ono zapisane w wyszukiwarce. Jak zatem wszystkie zapamiętać? Z pomocą przychodzi prosta maszyna szyfrująca.

Jak ją zrobić?

Potrzebujesz dwóch kół z literkami. Możesz je zrobić samemu lub wydrukować z ostatniej strony naszej karty pracy. Kolejność liter nie ma znaczenia (mogą to być także cyfry).



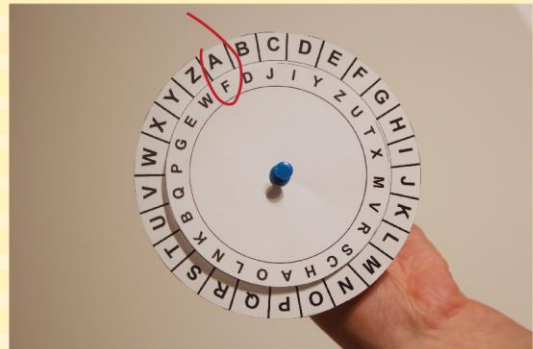
1. Gdy przygotujesz już dwa koła z literkami, to musisz je wyciąć. Pamiętaj, że jedno kółko jest większe, a drugie mniejsze.



2. Następnie nałóż mniejszą tarczę na większą.



3. Przebij środek obu kół pinezką.



4. Zatykaj pinezkę korkiem [może to być też gumka do zmywania lub inny podobny przedmiot].

4. Urządzenie jest już gotowe, trzeba teraz wymyślić szyfr!
Np. Hasło niech brzmi: **AKWARELA**.
Na dużym dysku odnajdujemy literę **A**. Następnie obracając dysk wewnętrzny, szukamy litery, którą chcemy ją zaszyfrować, np. **F**.
Widzimy, że **A** odpowiada **F, K -V, W-P** itd.

Nasze zaszyfrowane hasło brzmi wówczas tak : **FVPFLYRF**.

Nazwę strony, do której się odnosi również, możemy tak utajnić. Musimy jednak pamiętać, żeby obok umieścić wskazówkę, która pomoże nam w odczytaniu szyfru, poprzez odpowiednie zsynchronizowanie dysków.. Można to zrobić w ten sposób: AF (czyli A na dużej tarczy odpowiada F na małej). Jest to tzw. **szyfr Cezara** – rzymski wódz używał go w korespondencji, gdzie każdą literę alfabetu zastępował inną, położoną 3 pozycje dalej. Jest to co prawda najprostsza metoda szyfrowania, jednak z drugiej strony żaden, nawet najbardziej skomplikowany system nie może uchodzić za w pełni bezpieczny. Przekonali się o tym Niemcy, kiedy to Polacy – Marian Rejewski, Jerzy Różycki, Henryk Żygalski i inni złamali kod maszyny szyfrującej Enigma, co miało wpływ na losy II wojny światowej.

