12 w 2024 (12)

Szyfruj jak Cezar – koło szyfrowe

Data publikacji: 30.12.2024 / Autor: Michał Topolski

Koło szyfrowe to jedno z najprostszych, a jednocześnie najbardziej fascynujących narzędzi do szyfrowania. Na początek zmagań z zaawansowanymi zagadnieniami z dziedziny kryptografii wydaje się lepsze (i ciekawsze!) niż proste szyfry sylabowe, które pewnie poznałeś w ramach pierwszych zajęć z sygnalizacji. W tym artykule dowiesz się, jak działa koło szyfrowe oparte o szyfr Cezara, jak je własnoręcznie skonstruować, a także, jak wzbogacić je o dodatkowe funkcje.

Źródło: Zintegrowana Platforma Edukacyjna (ZPE)

Jak działa koło szyfrowe?

Koło szyfrowe to genialne i proste narzędzie. Składa się z dwóch obręczy – większej i mniejszej – które można obracać względem siebie. Na każdej z obręczy zapisany jest alfabet. Gdy ustawisz koło w wybranej pozycji startowej (np. przesunięcie o trzy

litery w prawo), każda litera tekstu jawnego zostaje przypisana do danej litery w alfabecie szyfrowanym (zakładamy w nim brak polskich znaków).

Przykład dla przesunięcia o 3:

- Litera **A** w tekście jawnym staje się **D** w szyfrze.
- Litera **B** staje się **E**.
- Litera **Z** przechodzi na początek alfabetu i staje się **C**.

Proste, prawda? To właśnie jest szyfr Cezara – jedna z najstarszych metod kryptograficznych.

Jak zrobić własne koło szyfrowe?

Oto, co potrzebujesz:

1. Dwa kawałki sztywnego kartonu lub tektury.
2. Nożyczki.
3. Cienkopis lub marker.
4. Spinacz biurowy lub pinezka (do połączenia obręczy).
5. Linijka i cyrkiel (opcjonalnie, ale przydatne ze względów estetycznych).

Krok 1: Tworzymy obręcze

- Na kartonie narysuj dwa koła – jedno większe, drugie mniejsze. Większe powinno mieć średnicę około 15 cm, a mniejsze około 10 cm. Do tego przyda się cyrkiel!
- Wytnij oba koła nożyczkami.

Krok 2: Rysujemy alfabet

- Na większym kole, wzdłuż krawędzi, równomiernie zapisz cały alfabet (A-Z).
- Na mniejszym kole zrób to samo.

Krok 3: Łączymy obręcze

- Połóż mniejsze koło na środku większego i przebij oba w centrum pinezką lub spinaczem biurowym. Teraz obręcze mogą swobodnie się obracać względem siebie.

Jak szyfrować za pomocą koła?

1. Ustaw koło w pozycji startowej. Na przykład: litera A na małym kole powinna odpowiadać literze D na dużym.
2. Znajdź literę tekstu jawnego na mniejszym kole.

3. Odczytaj odpowiadającą jej literę szyfru z większego koła.

Przykład: Jeśli chcesz zaszyfrować słowo „KOT” przy przesunięciu o 3:

- K → N
- O → R
- T → W
  Wynik: „NRW”.

Dekodowanie działa w analogiczny sposób – wystarczy odwrócić proces, czytając litery w przeciwnym kierunku.

A może by tak zrobić to jeszcze lepiej?

Standardowe koło szyfrowe to świetne wprowadzenie do kryptografii, ale można je znacznie ulepszyć, tworząc jego zaawansowaną wersję. Oto kilka pomysłów:

Koło z dodatkowymi obręczami

Zamiast dwóch obręczy, stwórz koło z trzema (lub więcej) warstwami. Każda kolejna obręcz może zawierać inny zestaw znaków – np. cyfry, symbole specjalne albo alfabet w odwrotnej kolejności. Możesz też po prostu wykorzystać wiele kół z alfabetem o różnym przesunięciu i przyjąć jakąś zasadę odczytywania liter z kół, na przykład sekwencję: dla pierwszej litery patrzę na pierwsze koło, dla drugiej drugie, dla trzeciej na trzecie, dla czwartej znów na pierwsze. Takie szyfrowanie określamy mianem polialfabetycznego – jest ono dużo bardziej odporne na ataki statystyczne (o których może kiedyś napiszę).

Losowe ustawienia alfabetu

Zamiast zapisywać alfabet w standardowej kolejności (A-Z), ułóż litery w losowej kolejności na jednym z kół. Dzięki temu otrzymałeś szyfr alfabetyczny z kluczem. Jeżeli dołożysz dodatkowe obręcze, jak w poprzednim punkcie, otrzymasz szyfr polialfabetyczny z kluczem (a tak naprawdę dwoma kluczami, bo jednym kluczem jest już sekwencja odczytywania liter z obręczy).

Pamiętaj, że powyższe podejścia wymagają zapisania klucza, a także ustalenia jednakowej budowy kół szyfrowych. Informacje te należy bezpiecznie wymienić między sobą, żeby rozpocząć szyfrowaną komunikację.

Szyfrowanie kombinacji znaków

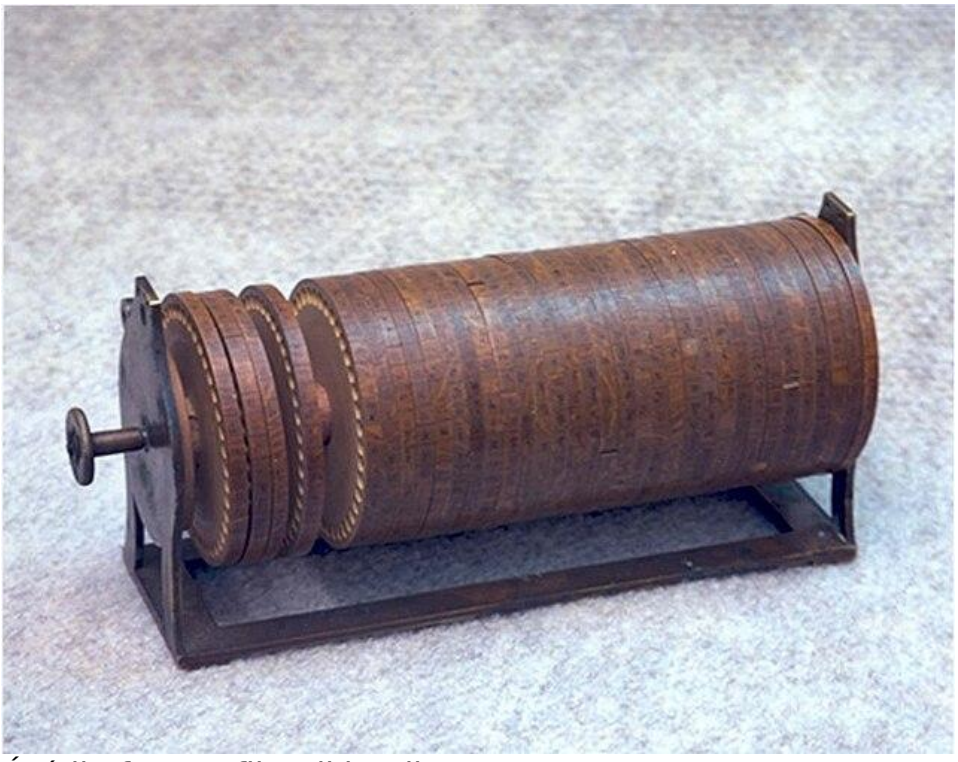
Często koła szyfrowe zawierają także jako jeden „znak” całe wyrazy czy sekwencje liter często występujące w danym języku. W przypadku angielskiego często bywała

to cząstka „ing”, czy słowo „and”; należy wtedy pamiętać, żeby zawrzeć dodatkowe symbole na drugim kole – zawsze liczba symboli na każdej z obręczy musi być taka sama, żeby urządzenie działało.

Jak to w historii bywało…

Wróćmy do początków! Przyjmuje się, że koło szyfrowe wynalazł w 1470 włoski architekt Leon Battista Alberti. Od tego czasu wykorzystywane było szeroko w ramach wojska czy dyplomacji do przekazywania tajnych wiadomości. Szczególną popularnością rozwiązanie to cieszyło się w trakcie wojny secesyjnej.

W XVIII wieku Thomas Jefferson skonstruował urządzenie składające się z 26 drewnianych dysków, z których każdy miał na obwodzie litery alfabetu w losowej kolejności. Dyski te można było obracać niezależnie, co pozwalało na tworzenie skomplikowanych szyfrów. To urządzenie, znane jako „koło szyfrowe Jeffersona”, używane było aż do 1942 roku w amerykańskiej armii i marynarce.



Źródło fotografii: Wikipedia

Tego typu rozwiązania w późniejszym czasie doprowadziły do powstania zaawansowanych maszyn szyfrujących takich jak Enigma, która także opiera swoje działanie na obrotowych tarczach, choć poziom ich złożoności jest znacznie większy – rotory zmieniają swoją pozycję po każdej zaszyfrowanej literze, a ich położenie jest wzajemnie zależne od siebie.

A na koniec – posłowie!

Koło szyfrowe to prosty, ale niezwykle efektywny sposób na naukę kryptografii. Możesz dzięki niemu w interaktywny sposób zapoznać siebie i swoich harcerzy z podstawowymi zagadnieniami tej jakże ważnej dziedziny nauki. Jakby nie patrzeć, gdyby nie takie wynalazki jak koło szyfrowe wynalezione ponad pół millenium temu, to dziś nie mógłbyś czytać tych treści na stronie internetowej (stronie, która też zresztą jest na wiele sposobów zabezpieczona i zaszyfrowana – patrz: protokół https, którym się łączysz ze stroną). Może to też być po prostu dobrą zajawką i wyłamaniem się ze schematu używania w harcerstwie podstawowych sylabowych szyfrów,czekoladki, bądź też Morse'a. Jeśli zechcesz, możesz włączyć koło szyfrowe w coś większego np. warsztaty poświęcone kryptografii albo spotkanie z osobą zajmującą się tą sztuką (25 stycznia obchodzimy Dzień Kryptologii, może to dobra okazja, by zagłębić się w temat?).

Powodzenia w zmaganiach z kołem szyfrowym!

Zdjęcie z nagłówka: zasoby Zlotu Harcerskiego w rocznicę Powstania Warszawskiego

Michał Topolski

Urodzony w Kluczborku, tam też się wychował, w pewnym momencie został harcerzem, a potem instruktorem. Obecnie kierownik Wydziału Zuchów GKHy. Zawodowo zajmuje się cyberbezpieczeństwem i szkoleniami, a w wolnych chwilach uczy też debatowania. Posiada całkiem pokaźną kolekcję piór wiecznych, lubi pisać (nie tylko piórami). Zastępca redaktora naczelnego Pojutrza.