Informatyka w Edukacji, XV
UMK Toruń, 2018

ŁAMIEMY SZYFR CEZARA

Maciej Borowiecki, Krzysztof Chechłacz
Ośrodek Edukacji Informatycznej i Zastosowań Komputerów
02-026 Warszawa, ul. Raszyńska 8/10
{maciej.borowiecki, krzysztof.chechlacz}@oeiizk.waw.pl

Abstract. The article discusses one of the oldest method of encryption – Caesar cipher. We present its role in the history and meaning for education. Topics related to encryption and security are important in everyday life. It is worth to know how to break Caesar cipher based on frequency analysis.

1. Wstęp

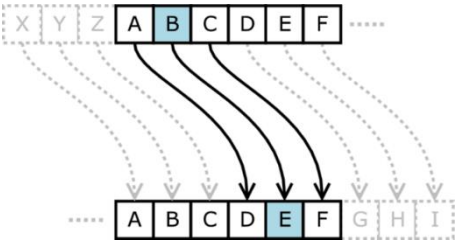
Ludzie od dawna zastanawiają się nad bezpiecznym przekazywaniem informacji. Już w starożytności pojawił się pomysł, by przesyłane wiadomości szyfrować. Jednym z najbardziej znanych był szyfr podstawieniowy zwany szyfrem Cezara. Skąd się wywodzi? Nazwa pochodzi od rzymskiego cesarza Juliusza Cezara, który szyfrował nim swoją korespondencję z Cyceronem. Swego czasu był to bardzo popularny sposób szyfrowania wiadomości, ostatnie doniesienia na temat jego używania pochodzą z 1915 roku – w armii Imperium Rosyjskiego był on stosowany jako zamiennik dla bardziej skomplikowanych szyfrów.

Szyfrowanie jest wykorzystywane przede wszystkim do zapewnienia bezpieczeństwa danych. Spotykamy się z nim na każdym kroku – logując się do poczty lub bankowości mobilnej, korzystając z profilu zaufanego, zabezpieczając dokumenty przekazywane drogą elektroniczną. Temat bezpieczeństwa jest jednym z ważnych zagadnień wymienionych w nowej podstawie programowej. W ramach omawiania go z uczniami możemy wrócić do historii i spróbować wykorzystać szyfr Cezara do kodowania i odkodowywania informacji. A może nawet uda nam się go złamać?

2. Szyfr Cezara w szkole

Szyfr Cezara jest jedną z najprostszych technik szyfrowania. Każdą literę tekstu jawnego zastępujemy inną literą, oddaloną od niej o stałą liczbę pozycji w alfabecie.

Przygotowanie z uczniami starszych klas szkoły podstawowej kilku funkcji szyfrujących lub odszyfrowujących wiadomości może stanowić interesujące zadanie.

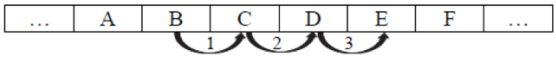


Rysunek 1 Szyfr Cezara z kluczem 3

Przy okazji pisania funkcji związanych z szyfrowaniem omawiamy takie zagadnienia, jak podział napisu na poszczególne znaki, kody ASCII, operacja modulo, pętle i instrukcje warunkowe. O tym, że warto zainteresować się w szkole zagadnieniami związanymi z szyfrowaniem może świadczyć egzamin maturalny z informatyki w 2016 roku na poziomie rozszerzonym.

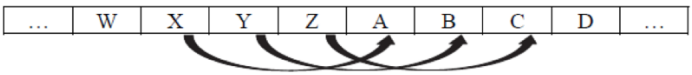
Zadanie 6. Szyfr Cezara

Podstawieniowy szyfr Cezara z przesunięciem (kluczem) k polega na zastąpieniu każdego znaku jawnego znakiem leżącym w alfabecie o k pozycji w prawo od zastępowanego znaku. Przykład: znak ‘B’ po zakodowaniu kluczem k=3 zastąpiony zostanie znakiem ‘E’.



Przy szyfrowaniu znaku należy postępować w sposób cykliczny, to znaczy, jeżeli znak nie posiada w alfabecie następnika przesuniętego o k pozycji, to alfabet „zawija się" i za literą Z następuje znów litera A.

Przykład: jawny znak ‘X’ po zakodowaniu kluczem k=3 zastąpiony zostanie znakiem ‘A’, znak ‘Y’ – znakiem ‘B’, natomiast ‘Z’ – znakiem ‘C’.



W tym zadaniu rozpatrujemy tylko słowa zbudowane z wielkich liter alfabetu angielskiego (o kodach ASCII odpowiednio od 65 do 90), o długościach nie większych niż 30 znaków.

Rysunek 2 Zadanie maturalne – szyfr Cezara

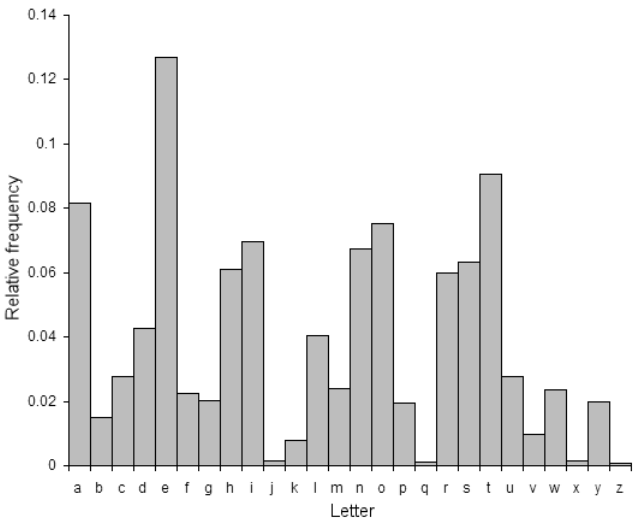
W kolejnych podpunktach zadania należało napisać program:

1. szyfrujący z kluczem k=107 słowa pobrane z pliku,
2. odszyfrowujący słowa zakodowane z podanym kluczem *k*,
3. wyszukujący i wypisujący błędnie zaszyfrowane słowa.

Plik z danymi do trzeciego podpunktu zawiera pary słów, w których drugie słowo jest szyfrogramem pierwszego z nieznanym kluczem. Oba słowa są zawsze tej samej długości, ale niektóre szyfrogramy są błędne. Oznacza to, że część liter w słowie mogła być zakodowana z różnymi przesunięciami. Zadaniem było podanie listy wszystkich błędnie zaszyfrowanych słów.

3. Łamanie szyfru Cezara

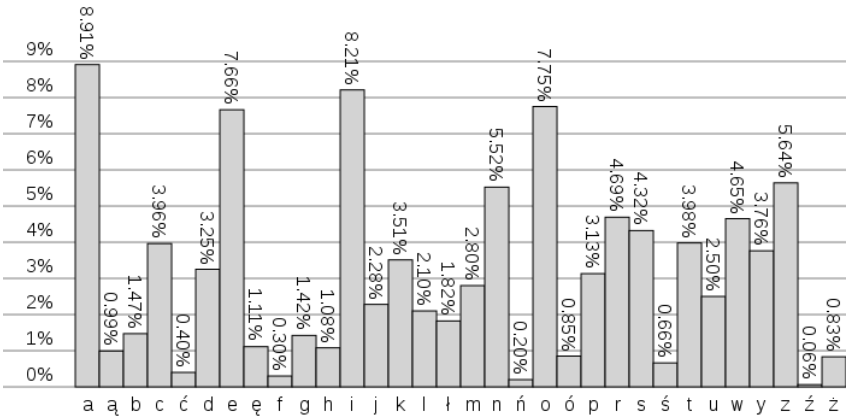
Już w IX wieku zaczęto stosować analizę częstościową tekstu i wykorzystywano ją do łamania szyfrów. Znając częstotliwość występowania poszczególnych liter alfabetu w tekstach pisanych w konkretnym języku, można było wyznaczyć rozkład znaków w zaszyfrowanym tekście i porównując ze sobą te informacje odszyfrować przekazywaną wiadomość. Niezbędnym było oczywiście posiadanie dostatecznie długich zaszyfrowanych wiadomości oraz wiedza, w jakim języku został napisany oryginalny tekst. Znając jedynie szyfrogram, do którego zastosowano szyfr Cezara z nieznanym kluczem, możemy spróbować go odczytać. Podobną technikę można zastosować do innych szyfrów podstawieniowych.



Rysunek 3 Rozkład częstotliwości liter w języku angielskim

Jeśli przyjrzymy się bliżej rozkładom częstotliwości wystąpień liter w językach polskim i angielskim zrozumiemy, dlaczego niezbędna jest znajomość języka, w jakim została napisana zaszyfrowana wiadomość. Jako dodatkowe zadanie uczniowie mogą odszukać tabele z informacją na temat częstotliwości znaków w kilku

popularnych językach, a następnie spróbować odszyfrować przesłaną przez nauczyciela wiadomość.



Rysunek 4 Rozkład częstotliwości liter w języku polskim

Próbując złamać szyfr Cezara w języku polskim powinniśmy postępować zgodnie z następującym algorytmem:

1. zlicz częstości wszystkich liter w szyfrogramie,
2. wyszukaj pozycję najczęściej występującej litery w szyfrogramie,
3. znaleziona pozycja odpowiada kluczowi z jakim zakodowano tekst (ponieważ najczęściej występującą literą w języku polskim jest litera a)

Warto zwrócić ich uwagę na fakt, że korzystanie z metody lingwistycznej łamania szyfrów miało duże znaczenie historyczne, w szczególności leżało u podstaw powstania polskiej szkoły krypto-analizy, której osiągnięciem było między innymi złamanie kodów Enigmy [3].

4. Podsumowanie

Korzystanie z szyfrów było niegdyś tak popularne, że powstawały nawet specjalne narzędzia do jego wspomagania. Za pomocą takiego przyrządu można było szybko szyfrować i odszyfrowywać nawet skomplikowane wiadomości. A w jaki sposób złamać szyfr Cezara w praktyce dowiedzą się Państwo na naszych warsztatach. Zapraszamy!

Rysunek 5 Przykład „maszyny" szyfrującej (z kolekcji M.M. Sysły)

Literatura

1. KhanAcademy, *Podróż w krainę kryptografii. Historia kryptografii*, https://pl.khanacademy.org/computing/computer-science/cryptography/crypt/v/caesar-cipher, ostatni dostęp 12.06.2018 roku.
2. Karbowski M., *Podstawy kryptografii*, Helion, Gliwice 2006.
3. Kołodziejczyk G., *Polski wywiad radiowy podczas wojny z bolszewicką Rosją 1918-1920*, http://dakowski.pl/index.php?option=com_content&task=view&id=4153&Itemid=80, ostatni dostęp 12.06.2018 roku.