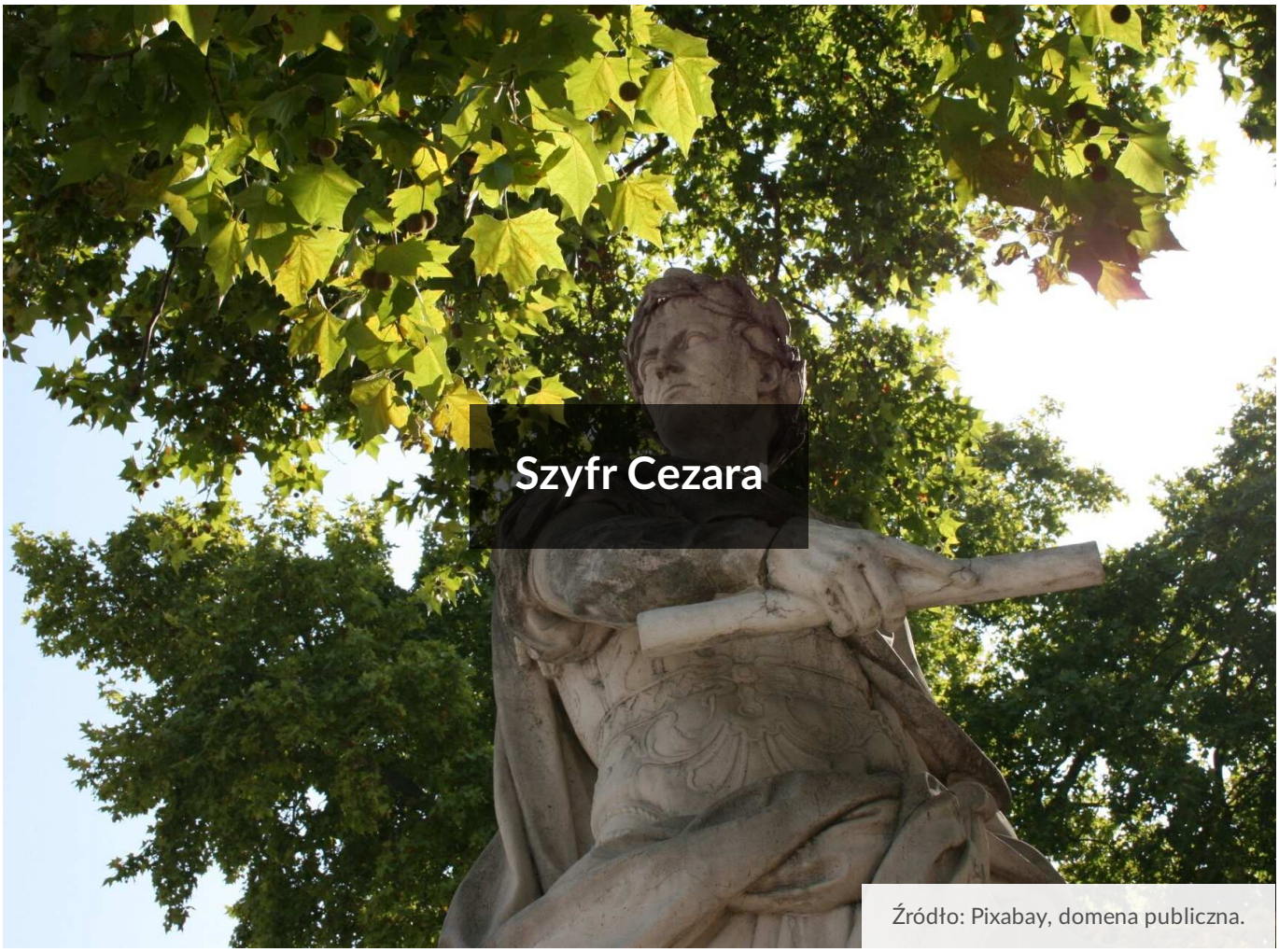
Szyfr Cezara



Źródło: Pixabay, domena publiczna.

Wyobraź sobie, że chcesz komunikować się ze znajomymi za pomocą prostego szyfru, jednak przetwarzanie słów ręcznie zajmuje zbyt dużo czasu. Jak wykonać prosty program, który zaszyfruje i rozszyfruje tekst przy użyciu algorytmu stosowanego od wieków?

W tym e-materiale dowiesz się, czym jest i jak działa szyfr Cezara.

Implementacje omawianego zagadnienia w poszczególnych językach programowania znajdziesz w e-materiałach:

- Implementacja szyfru Cezara w języku C++,
- Implementacja szyfru Cezara w języku Java,
- Szyfr Cezara w języku Python.

Więcej zadań? Sięgnij do Szyfr Cezara – zadania maturalne.

> **Twoje cele**
>
> - Prześledzisz, czym jest i jak działa szyfr Cezara.
> - Zaszyfrujesz przykładową wiadomość.
> - Przeanalizujesz algorytm, sprawdzając, czy szyfr Cezara łatwo jest złamać.

Przeczytaj

Imprerium Rzymskie, I w. p.n.e. Państwem włada Juliusz Cezar. Przypuszcza się, że do komunikowania się ze swoimi przyjaciółmi używał szyfru, który później zyskał miano szyfru Cezara. W jaki sposób szyfrowano informacje w starożytności?

Szyfr przesuwający

Pod pojęciem „szyfr Cezara" kryje się szyfr przesuwający. To niezwykle prosta technika, będąca szczególnym przypadkiem szyfru podstawieniowego, w której każdy znak szyfrowanej wiadomości jest zastępowany innym, oddalonym od niego w alfabecie o określoną odległość. W przypadku tego algorytmu ignoruje się wielkość liter.

Posłużymy się przykładem, aby sprawdzić, jak działa taka technika. Załóżmy, że chcemy zorganizować niespodziewane przyjęcie urodzinowe dla naszego kolegi. Musimy wysłać wiadomość do jego znajomych, kiedy wyjdzie z domu, ale nie chcemy, by przypadkiem ją odczytał. Umówiliśmy się, że zakodujemy wiadomość jak Juliusz Cezar, który stosował przesunięcie o trzy pozycje do przodu. W przypadku tego algorytmu jest to **klucz** szyfru.

Przygotujemy sobie wiadomość do zaszyfrowania, czyli **tekst jawny**:

```
Tekst jawny: MIESZKANIE OTWARTE WRACAMY ZA GODZINĘ
```

Polski alfabet liczy 32 litery, zatem przesuwając cały **alfabet** o trzy pozycje, otrzymamy następujący **szyfr**:

```
Alfabet:    AĄBC ĆDEĘ FGHI JKLŁ MNŃO ÓPRS ŚTUW YZŹŻ
Szyfr:      CĆDE ĘFGH IJKL ŁMNŃ OÓPR SŚTU WYZŹ ŻAĄB
```

Podmieniając każdą literę tekstu jawnego jej zaszyfrowanym odpowiednikiem, otrzymamy następujący wynik, czyli **tekst zaszyfrowany**:

```
Tekst jawny:
    MIESZKANIE OTWARTE WRACAMY ZA GODZINĘ

Tekst zaszyfrowany:
    OLGUAMCÓLG RYŹCTYG ŹTCECOŻ AC JRFALÓH
```

Tak zaszyfrowany tekst wygląda jak przypadkowa wiadomość, ale może zawierać istotne informacje – w tym wypadku czas, jaki pozostał do powrotu kolegi do domu. Niestety, ze względu na swoją prostotę szyfr Cezara znajduje zastosowanie jedynie tam, gdzie nie zależy nam na gwarancji bezpieczeństwa komunikacji. Czasem bywa również fragmentem bardziej złożonych algorytmów szyfrujących.

Odszyfrowanie wiadomości to operacja odwrotna do wykonanej na początku. Zatem jeśli wiadomość zaszyfrowano, przesuwając alfabet o trzy pozycje do przodu, to rozszyfrowanie sprowadza się do przesunięcia go o trzy pozycje do tyłu.

Kryptoanaliza

Istnieją dwie techniki łamania szyfru Cezara, zależne od tego, czy jesteśmy pewni, że to właśnie on został użyty. Przyjrzyjmy się najpierw przypadkowi, w którym wiemy, że użyto szyfru Cezara.

Liczbę możliwych przesunięć możemy wyrazić wzorem:

$$L = n - 1$$

gdzie n jest liczbą znaków w alfabecie; w przypadku języka polskiego mamy do dyspozycji 32 litery.

W przypadku alfabetu łacińskiego mowa już tylko o 26 znakach. Jedno przesunięcie możemy pominąć, ponieważ wiadomość znajduje się już w stanie początkowym. Oczywiście moglibyśmy użyć znacznie bardziej skomplikowanego alfabetu i utrudniłoby to ręczne odszyfrowanie wiadomości. Programistycznie jednak przypadek ten sprowadza się do metody siłowej, gdzie w prosty sposób jesteśmy w stanie uzyskać wszystkie możliwe przesunięcia, a wśród nich będzie również to prawidłowe. Podchodząc do problemu matematycznie, moglibyśmy przyjąć, że każda litera alfabetu oznaczona jest liczbą, na przykład A→0, Ą→1, B→2. Szyfrowanie moglibyśmy zatem zapisać w postaci następującego równania:

$$S_i = (x_i + t) \bmod n$$

gdzie:
S_i – numer litery po zaszyfrowaniu,
x_i – przyporządkowany numer litery,
t – przesunięcie,
mod – operator reszty z dzielenia (modulo),
n – liczba znaków w alfabecie.

Używając tego równania, moglibyśmy skonstruować następujący pseudokod:

```
dla t = 0, 1, 2 ... n - 1 wykonuj:
    przesuń każdy znak o t pozycji
```

A co zrobić, jeśli słowo było wielokrotnie szyfrowane? Przesunięcia się sumują, zatem przesunięcie o 10 do przodu, 3 do tyłu i 5 do przodu w rzeczywistości sprowadza się do jednego przesunięcia o 12 do przodu. Jedynym przypadkiem, w którym rozszyfrowanie może nie być skuteczne, są bardzo krótkie wiadomości. Dla nich może istnieć więcej niż jedno rozwiązanie.

Drugą techniką łamania szyfru jest sytuacja, w której nie mamy pewności, czy użyto szyfru Cezara. Stosuje się wtedy te same metody, co w przypadku innych szyfrów podstawieniowych, np. wykorzystuje się statystykę. Litery w różnych językach pojawiają się z pewnym prawdopodobieństwem. W języku polskim najczęściej występują litery A, I, O oraz E. Zatem w zaszyfrowanej wiadomości można czasem odnaleźć pewną zależność i wywnioskować, że użyto właśnie szyfru Cezara.

Słownik

> **Juliusz Cezar**
>
> (100 p.n.e. – 44 p.n.e.), rzymski polityk, wódz, dyktator i pisarz
> **szyfr podstawieniowy**
>
> szyfr, w którym każdy znak tekstu jawnego zastępowany jest innym znakiem szyfrogramu

Schemat interaktywny

Polecenie 1

W poniższym schemacie przygotuj algorytm analogiczny do szyfru Cezara, uwzględniający zamianę (kodowanie) cyfr na litery z przesunięciem o 4 znaki.

Sprawdź się

Pokaż ćwiczenia:

Ćwiczenie 1

Ćwiczenie 2

Ćwiczenie 3

Ćwiczenie 4

Ćwiczenie 5

Ćwiczenie 6

Ćwiczenie 7

Co oznacza zdanie: Yhql, ylgl, ylfl? Odczytaj je, posługując się szyfrem Cezara. W szyfrze użyto alfabetu łacińskiego i nie uwzględniono znaków interpunkcyjnych.

Ćwiczenie 8

Tekst zaszyfrowano kluczem z przesunięciem o 5 do przodu: Jy yz, Gwzyj, htsywf rj? Rozszyfruj, co powiedział Cezar. W szyfrze użyto alfabetu łacińskiego i nie uwzględniono znaków interpunkcyjnych.

Dla nauczyciela

Autor: Zespół Gromar.eu

Przedmiot: informatyka

Temat: Szyfr Cezara.

Grupa docelowa: III etap edukacyjny, liceum, technikum

Podstawa programowa:

Zakres podstawowy

I. Rozumienie, analizowanie i rozwiązywanie problemów. Uczeń:

2) stosuje przy rozwiązywaniu problemów z różnych dziedzin algorytmy poznane w szkole podstawowej oraz algorytmy:

b) na tekstach: porównywania tekstów, wyszukiwania wzorca w tekście metodą naiwną, szyfrowania tekstu metodą Cezara i przestawieniową.

Kompetencje kluczowe:

- kompetencje w zakresie rozumienia i tworzenia informacji,
- kompetencje w zakresie wielojęzyczności,
- kompetencje matematyczne oraz kompetencje w zakresie nauk przyrodniczych, technologii i inżynierii,
- kompetencje cyfrowe,
- kompetencje osobiste, społeczne i w zakresie umiejętności uczenia się.

Cele operacyjne:

Uczeń:

- dowiaduje się, czym jest i jak działa szyfr Cezara,
- szyfruje przykładową wiadomość,
- analizuje algorytm, sprawdzając, czy szyfr Cezara jest łatwo złamać.

Strategie nauczania:

- konstruktywizm.

Metody i techniki nauczania:

- burza mózgów;

- rozmowa kierowana;
- dyskusja.

Formy pracy:

- praca indywidualna;
- praca w parach;
- praca w grupach;
- praca całego zespołu klasowego.

Środki dydaktyczne:

- komputery z głośnikami i dostępem do internetu, słuchawki;
- zasoby multimedialne zawarte w e-materiale;
- tablica interaktywna/tablica, pisak/kreda.

Przebieg zajęć:

Faza wstępna

1. Przed zajęciami chętni uczniowie przygotowują krótkie prezentacje dotyczące szyfru Cezara i innych historycznych metod szyfrowania (np. ROT13, ADFGVX, One Time Pad). Inna czteroosobowa grupa przygotowuje osiem zaszyfrowanych wiadomości szyfrem Cezara.
2. Przedstawienie tematu i celów zajęć oraz wspólne z uczniami ustalenie kryteriów sukcesu.
3. Burza mózgów na temat szyfrów i szyfrowania. Pytania do uczniów:

- Jakie szyfry znacie?
- W jakim celu stosuje się szyfry?
  Moderator zapisuje propozycje na tablicy. Po fazie twórczej następuje weryfikacja pomysłów i podsumowanie zadania.

Faza realizacyjna

1. Prezentacja materiałów dotyczacych szyfrów przygotowanych przez uczniów przed zajęciami. Dyskusja.
2. Nauczyciel wspólnie z uczniami omawia metody kryptoanalizy stosowane do odczytywania szyfru Cezara.
3. Podział klasy na cztery grupy. Każda otrzymuje dwie wiadomości zaszyfrowane przez kolegów (o jednej wiadomo, że użyto szyfru Cezara, o drugiej – nie wiadomo). W każdej grupie powinien znaleźć się szyfrant, który w razie potrzeby będzie naprowadzał kolegów na rozwiązanie. Uczniowie samodzielnie rozszyfrowują wiadomości. Wspólna analiza rozwiazań.

4. Praca z multimedium bazowym. Uczniowie przygotowują algorytm analogiczny do szyfru Cezara, uwzględniający zamianę (kodowanie) cyfr na litery z przesunięciem o 4 znaki. Następnie prezentują go kolegom i koleżankom. Wspólnie omawiają rezultaty swojej pracy i oceniają się wzajemnie. Praca w grupach lub w parach.
5. Uczniowie rozwiązują ćwiczenia interaktywne wskazane przez nauczyciela. Wspólne omówienie odpowiedzi.

Faza podsumowująca

1. Na koniec zajęć nauczyciel prosi uczniów o rozwinięcie zdań:

- Dziś nauczyłem się…
- Zrozumiałem, że…
- Zaskoczyło mnie…
- Dowiedziałem się…
- Łatwe było dla mnie…
- Trudne było dla mnie…

Dwa ostatnie zdania oceniają trudność omawianego zagadnienia; dzięki nim uczeń dokonuje samooceny swoich wiadomości i umiejętności.

Materiały pomocnicze:

1. Materiały na temat innych historycznych szyfrów ROT13, ADFGVX, One Time Pad, np. Dirk Rijmenants, *Secure Communications with the One Time Pad Cipher*

Wskazówki metodyczne opisujące różne zastosowania multimedium:

Multimedium można również wykorzystać do pracy domowej – uczniowie przygotowują samodzielnie algorytmy, np. z przesunięciem do tyłu o 6 znaków.