

Algorytmy szyfrowania

<https://www.algorytm.edu.pl/algorytmy-maturalne/szyfr-cezara.html>

Co musisz wiedzieć?

- kod ASCII
- czym jest typ char w C++
- tablica

Szyfr Cezara

Zacznijmy od wyjaśnienia idei szyfru Cezara. Jest to jeden z najprostszych szyfrów przesuwających. Polega ona na przesunięciu każdej litery o pewną stałą wartość zwaną kluczem. Prześledźmy przykład:

Zaszyfrujmy słowo Marcin kluczem o wartości równej -2. A więc każdą literę przesuwamy w lewą stronę o dwie wartości:

Przed szyfrowaniem	Po szyfrowaniu
M	K
a	y
r	p
c	a
i	g
n	l

Oczywiście szyfrowanie odbywa się w zakresie liter alfabetu łacińskiego. Aby zaszyfrować literę **a** należy się cofnąć do końca alfabetu i będzie to litera **y**:

Słowo "**Marcin**" po zaszyfrowaniu wygląda następująco: "**Kypagl**".

Aby **zdeszyfrować** dane słowo należy przesunąć każdy znak o $-klucz$, czyli w tym przypadku o $-(-2)=2$