

<b>Název úlohy</b>	<b>Caesarova šifra 1/2</b>
<b>Třída</b>	4. třída
<b>Úloha splňuje RVP rámce</b>	<ul style="list-style-type: none"> <li>• DATA, INFORMACE A MODELOVÁNÍ – kódování a přenos dat</li> <li>• ALGORITMIZACE A PROGRAMOVÁNÍ – řešení problému krokováním, programování, kontrola řešení</li> </ul>
<b>Propojení s RVP výstupy</b>	<ul style="list-style-type: none"> <li>• <b>I-5-1-02</b> - Žákyně/žák popíše konkrétní situaci, určí, co k ní již ví, a znázorní ji</li> </ul>
<b>Propojení s ŠVP výstupy</b>	<ul style="list-style-type: none"> <li>• Žákyně/žák zakóduje/zašifruje a dekoduje/dešifruje text</li> </ul>
<b>Časová náročnost</b>	45 minut (jedna vyučovací hodina)
<b>Stručný popis úlohy</b>	Žáci se seznámí s šifrováním a pomocí předpřipravených bloků v MakeCode si zkusí zašifrovat jejich vlastní zprávu.
<b>Odkaz na rozšíření</b>	<a href="https://github.com/microbit-cz/pxt-caesar-cipher-extension">https://github.com/microbit-cz/pxt-caesar-cipher-extension</a>

# Caesarova šifra 1/2

## Co budete potřebovat

- PC s přístupem k [MakeCode](#)
- Propojovací USB kabel s micro USB koncovkou
- Micro:bit

## Co je Caesarova šifra?

Caesarova šifra je postavena na principu posunu podle předem zvoleného „klíče“ (tj. číslo). Všechny znaky ve zprávě jsou v tomto procesu zaměněny právě za ty, které se v dané řadě (např. ASCII tabulka) vyskytují na místě hodnoty klíče přičtené k pozici původního znaku.

## Práce s pracovním listem

Vysvětlíte žákům základní princip Caesarovy šifry. Zmiňte možnost zvolení záporného čísla jako klíč. Ukažte příklad na náhodném slově (např. Vaše jméno).

Nechte studenty vypracovat cvičení 1 a 2 v pracovním listu.

## Vyzkoušení s Micro:bitem

V této úloze budeme pro zjednodušení používat pouze znaky níže uvedené:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---	---

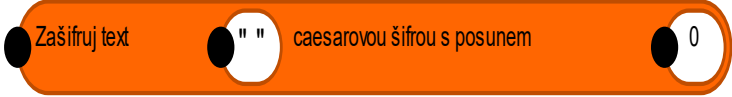
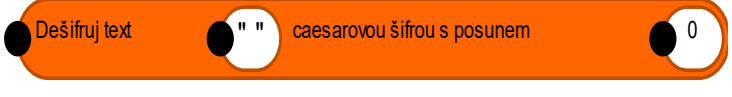
*Pokud student ve své zprávě zvolí jakýkoliv jiný znak, nezašifruje se (např. mezera zůstává mezerou.)*

*V případě diakritiky samotný micro:bit sice nevyhodí chybu, ale jelikož ji neumí zobrazovat, ukáže se na displeji místo jiného písmena pouze prázdný znak. Proto znovu žáky upozorněte, aby používali pouze písmena, která mají napsaná na pracovním listě ve **cvičení 3**.*

*Je jedno, jestli žáci používají velká nebo malá písmena. Celý text se vždy převede na malá písmena a až potom se zašifruje.*

## Rozšíření

## Popis rozšíření

<b>Zašifruj</b> 	<ul style="list-style-type: none"> <li>• Zašifruje zadaný text zadaným klíčem</li> <li>• Parametry: <ul style="list-style-type: none"> <li>○ text k zašifrování (text)</li> <li>○ klíč (posun) - může být kladný i záporný (číslo)</li> </ul> </li> <li>• Návrátová hodnota: zašifrovaný text (text)</li> </ul>
<b>Dešifruj</b> 	<ul style="list-style-type: none"> <li>• Dešifruje zadaný text zadaným klíčem</li> <li>• Parametry: <ul style="list-style-type: none"> <li>○ text k dešifrování (text)</li> <li>○ klíč (posun) - může být kladný i záporný (číslo)</li> </ul> </li> <li>• Návrátová hodnota: dešifrovaný text (text)</li> </ul>

## Možný postup v úloze

1. V této úloze stačí k zprovoznění pouze jeden jednoduchý krok. Do „při startu“ přidáme dva bloky „zobraz text“. Do každého z nich pak dáme jedno z našich rozšíření. Žáci si již poté jenom dopíší do vstupních parametrů obou rozšíření jejich zprávu a posun.

