Název úlohy	**Caesarova šifra 2/2**
Třída	6. třída
Úloha splňuje rámce	• DATA, INFORMACE A MODELOVÁNÍ – kódování a přenos dat • ALGORITMIZACE A PROGRAMOVÁNÍ – řešení problému krokováním, programování, kontrola řešení
Propojení s RVP výstupy	• ***I-9-2-05*** - Žákyně/žák v blokově orientovaném programovacím jazyce vytvoří přehledný program s ohledem na jeho možné důsledky a svou odpovědnost za ně; program vyzkouší a opraví v něm případné chyby; používá opakování, větvení programu, proměnné • ***I-9-1-02*** - Žákyně/žák navrhuje a porovnává různé způsoby kódování dat s cílem jejich uložení a přenosu
Propojení s ŠVP výstupy	• Žákyně/žák v blokově orientovaném programovacím jazyce sestaví program, dbá na jeho čitelnost a přehlednost
Časová náročnost	25 minut
Stručný popis úlohy	Žáci si vyzkouší přenos zašifrovaných zpráv mezi dvěma micro:bity.
Odkaz na rozšíření	https://github.com/microbit-cz/pxt-caesar-cipher-extension

Caesarova šifra 2/2

Co budete potřebovat

- PC s nainstalovaným editorem Microsoft MakeCode, případně webová verze
- Propojovací USB kabel s micro USB koncovkou
- Micro:bit (min. 2)

Začátek

Na této úloze si žáci vyzkouší, jak v praxi funguje Caesarova šifra, se kterou se měli seznámit minule. Žáci se nejdříve rozdělí do skupin nebo dvojicí (podle počtu micro:bitů ve třídě) a následně si pomocí lehce upraveného kódu z minulé hodiny budou vzájemně posílat zašifrované zprávy. Druhý z dvojice nebo druhá část skupiny pak na druhém micro:bitu vyzkouší zprávu rozšifrovat.

Rozšíření Popis rozšíření

Zašifruj	• Zašifruje zadaný text zadaným klíčem
	• Parametry:
	  ○ znak k zašifrování (znak)
	  ○ klíč (posun) - může být kladný i záporný (číslo)
	• Návratová hodnota: zašifrovaný znak (znak)

Dešifruj	• Dešifruje zadaný text zadaným klíčem
	• Parametry:
	  ○ znak k dešifrování (znak)
	  ○ klíč (posun) - může být kladný i záporný (číslo)
	• Návratová hodnota: dešifrovaný znak (znak)

Vyzkoušení s Micro:bitem

V této úloze budeme opět 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

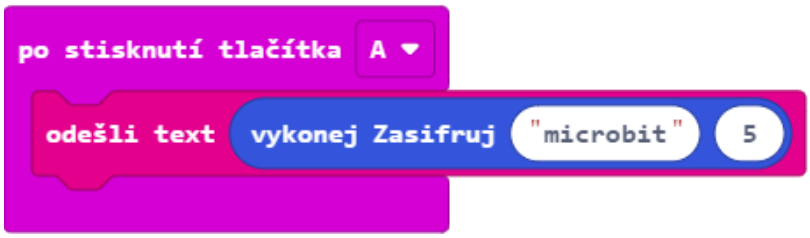
Pokud student ve své zprávě zvolí jakýkoliv jiný znak, nezašifruje se (např. mezera zůstává mezerou.)

*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.

1. Jako první si v bloku „při startu“ zvolíme skupinu rádia. Můžeme volit hodnoty od 0 do 255. Každá skupina žáků bude mít své vlastní číslo, které do tohoto bloku vloží, aby nedocházelo k tomu, že budou přicházet na jeden microbit zprávy od všech ostatních.

2. K odesílání adresy využijeme funkci, kterou jsme vytvořili v první části.



3. V moment, kdy na náš microbit naopak někdo pošle text, přichází na řadu funkce k dešifrování.

POZOR: *V bloku zašifrování je úmyslně dán posun 5 a do dešifrování posun 31. Takto se text samozřejmě dešifruje ŠPATNĚ a vznikne nesmysl. Pro správné dešifrování musí být klíče totožné.*

Žáci si je tedy musí říct někde „mimo“ (symetrické šifrování). Ideální počet žáků ve skupině jsou tedy 3 (jeden posílá text, jeden ví správný posun a tím pádem se mu podaří dešifrovat text a druhý ho neví a jen to zkouší s náhodnými čísly).