

Název úlohy	Caesarova šifra 2/2
Třída	4. třída
Úloha splňuje rámce	<ul style="list-style-type: none"> • DATA, INFORMACE A MODELOVÁNÍ – kódování a přenos dat • ALGORITMIZACE A PROGRAMOVÁNÍ – řešení problému krokováním, programování, kontrola řešení
Propojení s RVP výstupy	<ul style="list-style-type: none"> • I-5-1-02 - Žákyně/žák popíše konkrétní situaci, určí, co k ní již ví, a znázorní ji • I-5-4-01 - Žákyně/žák najde a spustí aplikaci, pracuje s daty různého typu
Propojení s ŠVP výstupy	<ul style="list-style-type: none"> • Žákyně/žák zakóduje/zašifruje a dekoduje/dešifruje text • Žákyně/žák předá informaci zakódovanou pomocí textu či čísel
Časová náročnost	45 minut (jedna vyučovací hodina)
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
Odkaz na řešení	https://github.com/microbit-cz/pxt-caesar-cipher2-demo-easy

Caesarova šifra 2/2

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 dvojic (podle počtu micro:bitů ve třídě) a následně si pomocí lehce upraveného kódu z minulé hodiny budou vzájemně posílat zašifrované zprávy.

První z dvojice či první část skupiny si vymyslí klíč, poté jím zašifruje libovolnou zprávu a pošle jí. Druhý z dvojice nebo druhá část skupiny pak na druhém micro:bitu zprávu odchytí a vyzkouší ji rozšifrovat.

Žák/Žákyně se v této úloze naučí/procvičí


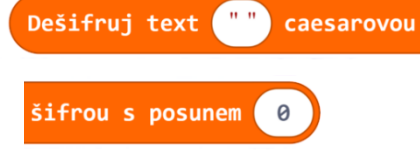
- Využití a smysl šifrování
- Zobrazování textu na microbitu
- Komunikace dvou microbitů mezi sebou

Co budete potřebovat

- PC s přístupem k [MakeCode](#)
- Propojovací USB kabel s micro USB koncovkou
- Micro:bit (min. 2)

Rozšíření

Popis rozšíření

<p>Zašifruj text</p> 	<ul style="list-style-type: none"> • zašifruje zadaný text zadaným klíčem • parametry: <ul style="list-style-type: none"> ○ text k zašifrování (text) ○ klíč (posun) - může být kladný i záporný (číslo) • návratová hodnota: zašifrovaný text (text)
<p>Dešifruj text</p> 	<ul style="list-style-type: none"> • dešifruje zadaný text zadaným klíčem • parametry: <ul style="list-style-type: none"> ○ text k dešifrování (text) ○ klíč (posun) - může být kladný i záporný (číslo) • návratová hodnota: dešifrovaný text (text)

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.)

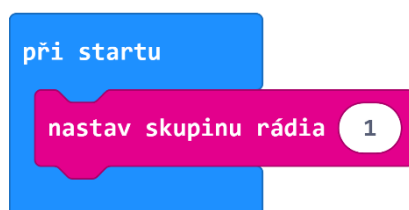
*V případě diakritiky samotný micro:bit sice nevyhodí chybu, ale jelikož ji neumí zobrazovat, ukáže se na displeji místo jiného písmena pouze prázdný znak. Proto znovu žáky upozorněte, aby používali pouze písmena, která mají napsaná na pracovním listě ve **cvičení 3**.*

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

Možný postup v úloze

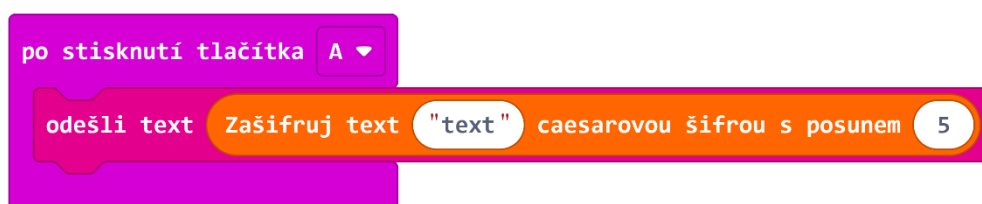
1. Nastavení komunikace přes rádio (Bluetooth)

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.



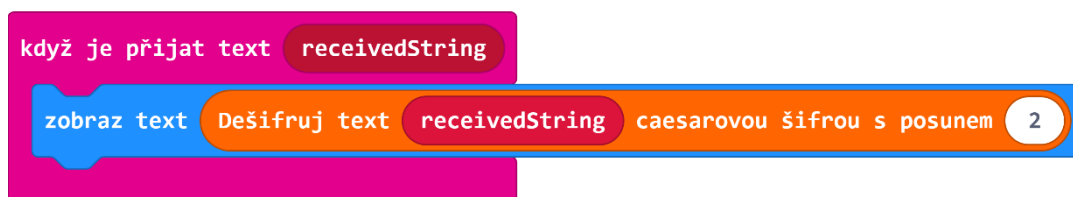
2. Odesílání textu z prvního microbitu

Dále si nastavíme odesílání textu. V tomto příkladu se odešle po stisknutí tlačítka A. V bloku odešli text budeme posílat blok Zašifruj text. Text v něm i posun může být samozřejmě libovolný.



3. Přijetí a dešifrování zprávy na druhém microbitu

Jako poslední si na druhém microbitu naprogramujeme přijímání zprávy. Budeme zobrazovat text, který získáme pomocí bloku *Dešifruj text*.



V bloku zašifrování je úmyslně dán posun 5 a do dešifrování posun 2. Takto se text samozřejmě dešifruje ŠPATNĚ a vznikne nesmysl. Pro správné dešifrování musí být klíče totožné.

Žáci si je tedy musí říct někde „mimo“. 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).