Pracovní list

Caesarova šifra 2/2

Jméno a příjmení _____

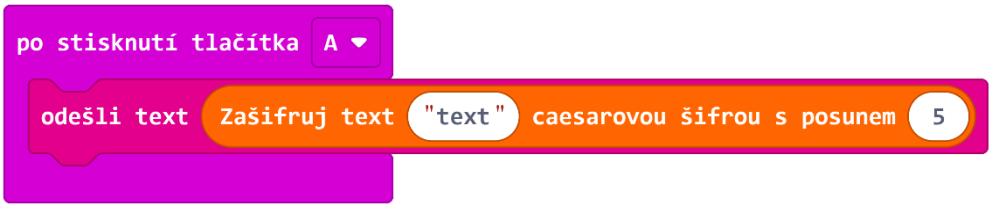
Datum _____

Třída _____

1. **V této úloze zúročíme vědomosti, které jsme posbírali v minulé části úlohy na Caesarovu šifru. Už byste měli vědět, jak na micro:bitu zašifrovat zprávu a poté ji zase rozšifrovat do původního znění. V této hodině si zkusíme posílat šifrované zprávy z jednoho micro:bitu na druhý.**

2. **Rozdělte se podle počtu micro:bitů ve třídě tak, aby v každé skupině či dvojici byly k dispozici dva micro:bity – jeden bude šifrovat a posílat, druhý přijímat a dešifrovat.**

3. **První část skupiny použije blok „Zašifruj text“ a poté ho pošle na druhý micro:bit.**



!!Opět myslíme na to, že součástí zprávy mohou být pouze tyto znaky!!

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

4. **Po naprogramování si první část skupiny (první z dvojice) vymyslí zprávu a číslo posunu při šifrování. Zprávu poté bez toho, aniž by svůj klíč prozradil spolužákům u druhého micro:bitu pošle.**

5. **Druhý z dvojice nebo druhá část ze skupiny musí být připravena a ještě, než první micro:bit vyšle zašifrovanou zprávu, musí nastavit klíč, který si myslí, že první skupina použila. Vyzkoušejte, jak dlouho vám bude trvat, než metodou pokus-omyl zjistíme správný klíč a podaří se vám zprávu rozšifrovat.**

Odkaz na GitHub rozšíření: https://github.com/microbit-cz/pxt-caesar-cipher-extension

6. **Nyní to zkuste ještě jednou. Tentokrát ale první skupina prozradí té druhé svůj klíč. Druhá skupina ho tedy nastaví a přijme zprávu, která by se okamžitě měla správně rozšifrovat.**

7. **Co si myslíte, že je hlavní důvod šifrování? Znáte nějaké další šifry? Kde by se šifrování dalo použít?**

Odkaz na GitHub rozšíření: https://github.com/microbit-cz/pxt-caesar-cipher-extension