Projekt byl podpořen z výzvy „NA UČITELÍCH ZÁLEŽÍ, ROZHODNUTÍ č. 20863/2021-2.“

Kódování

Mgr. Jan Konfršt

ZŠ Husova, Liberec

V této aktivitě již žáci umí zacházet s 3D editorem TinkerCad. Tématem hodiny je úvod do kódování a šifrování, který vychází z učebnice *Základy informatiky pro 1. stupeň ZŠ* (Mgr. Jan Berki, Ph.D.; Ing. Jindra Drábková, Ph.D.) volně dostupné zde: https://www.imysleni.cz/ucebnice/zaklady-informatiky-pro-1-stupen-zs.

Na začátek žáky návodnými otázkami dovedeme k odhalení toho, co je to kód a v jaké formě se s ním setkávají. Na tabuli jim pro úvod lze kreslit či promítat jednoduché symboly, například ukazatele WC, požárního východu, únikového schodiště a dalších podobných značek.

Obr. 1: Ukázka infotabulky jako příklad jednoduchého kódu v běžném životě.

Cílem je dovést žáky k tomu, že kódovaný jazyk používají dnes a denně, a to například za pomocí jednoduchých symbolů, jež jsou nezávislé na užitém jazyce. Takzvaný kódový přenos informace může zkrátka být velmi jednoduchý a univerzální.

Dalším příkladem mohou být pravěké jeskynní malby, to si mohou děti zkusit sami (mohou například nakreslit nájezdy lovců na mamuty). Další aktivitou může být cílený přenos informace za pomocí obrázků. Dětem lze například na tabuli napsat několik vět a jejich úkolem bude je zakódovat za pomocí obrázků, například:

Projekt byl podpořen z výzvy „NA UČITELÍCH ZÁLEŽÍ, ROZHODNUTÍ č. 20863/2021-2.“

Můj pes má hlad.
Včera jsem viděl svého nejlepšího kamaráda.
Kočka mi snědla můj domácí úkol.

Výsledky budou individuální a děti mohou pobavit nejrůznější variace v podání ostatních. Žáci zároveň zjistí, že ne všechna slova musí být nutně zakódovaná a důležité je obsáhnout slova nesoucí význam věty. Naopak výrazy vyjadřující gramatickou funkci je často možné zcela vynechat.

Na to navážeme aktivitou, ve které si děti už vymýšlejí sdělení a věty vlastní. Začít lze například jen frázemi či slovy (třeba *zavřená škola, elektromobil, rozbitá váza*) a poté se dostat ke komplexním souvětím. Žáci si své věty nejprve sami napíšou (pro urychlení aktivity je lepší využít skupinovou práci, či alespoň ve dvojicích), zakódují a poté na tabuli před ostatními prezentují. Ostatní skupiny následně hádají, co je smyslem jejich sdělení.

ŠIFROVÁNÍ

Od kódování se lehkým brainstormingem přesuneme k šifrování. Žáků se návodně doptáváme, jaký je asi rozdíl mezi tímto kódováním za pomocí obrázků a šifrováním. Pokud si nejsou jistí, použijeme příklady: symboly visící ze stropu v supermarketu a text:

XMA PGHJQ LDBAIE LASJC OSNA LSHA.

Cílem je, aby žáci ideálně sami přišli na to, že šifra má za cíl ukrýt zprávu.

Rychlým dotazováním zjistíme, zda žáci znají nějaké příklady šifer ze života okolo sebe. Lze třeba poukázat na mobilní zařízení a na chatovací aplikace a zde je možné rovnou jedním dechem varovat před důvěrou. Některé takové aplikace například proklamují šifrovaný přenos, jsou ale přitom schopné pro vlastní reklamní účely sledovat obsah konverzací a analyzovat jej.

Projekt byl podpořen z výzvy „NA UČITELÍCH ZÁLEŽÍ, ROZHODNUTÍ č. 20863/2021-2.“

Žáky postupně navedeme na téma Caesarovy šifry a promítneme následující tabulku na tabuli, žáky přitom upozorníme, že vycházet budeme z anglické abecedy:

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
L	m	n	o	p	q	r	s	t	u	v	w	x	y	z	a	b	c	d	e	f	g	h	i	j	K

– Vysvětlíme, že jde o Caesarovu šifru s posunem o 11 pozic, kde se písmeno *A* šifruje jako písmeno na 11. pozici v abecedě. Jako klíč se tedy v tomto případě udává písmeno *L*. 11. písmenko (*L*) se napíše na první pozici a poté následuje vypsání celé abecedy. Jakmile se dojde na konec, začne se zpět od *A*.

Žákům dle tabulky na tabuli zadáme několik slov k zašifrování a vysvětlíme, že šifrování probíhá „odshora dolů,“ kdy místo písmenka nahoře píšeme to, které je v tabulce pod ním.
Následuje několik příkladů na dešifrování, tentokrát „odzdola nahoru.“

Žákům (ideálně do dvojice) následně rozdáme nastříhané papíry s prázdnými tabulkami:

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

Obr. 2: Tabulka pro zápis šifry

Jako zadání dostanou klíč (písmenko, které přijde na první pozici a sami si vypíšou zbytek posunuté abecedy.

Možností, jak tuto aktivitu následně vést, je hned několik, jednou z nich je varianta, že všichni mají stejný klíč / posun, ale šifrují a dešifrují odlišné výrazy. Například na první řádek zadáme klíč *D*, čili pod písmenko *A* patří písmenko *D* a následují další písmenka z abecedy.

Projekt byl podpořen z výzvy „NA UČITELÍCH ZÁLEŽÍ, ROZHODNUTÍ č. 20863/2021-2.“

Žáci poté ve dvojicích šifrují unikátní výrazy (například světové metropole či jména celebrit) a poté svůj zašifrovaný text posouvají dvojici sedící po směru hodinových ručiček. Ti následně text dešifrují. Jakmile je hotové první kolo, zadáme dle nového klíče písmenka do druhého řádku a jedeme nanovo.

Propojení s dřívější aktivitou 3D modelování poté přichází ve formě jednoduchého šifrovacího nástroje.

Obr. 3: Šifrovací náramek vyrobený pomocí 3D tiskárny

Žákům lze předvést tento hotový model, ať už vytištěný, nebo jen ve formě 3D modelu v editoru a vysvětlit jim princip fungování: posun kruhů vůči sobě znamená definici šifrovacího klíče a onen posun. Šifrování a dešifrování následně probíhá za pomocí čtení propojených písmen.

Žákům lze tento model poskytnout k dalším úpravám, nebo je lze navést k tomu, aby si podobný zkusili vytvořit od základu sami, byť s řízenou pomocí v podobě demonstrace funkčního mechanismu.

Mechanismus kódování a princip fungování Caesarovy šifry si mohou žáci vyzkoušet v nové expozici na didaktické pomůcce Šifrování.