

Aktivnost A18

Skritopis

Povzetek

Problem izmišljenih pisav je, da si jih človek težko zapomni. A ne za nas: spoznali bomo trik, s katerim si lahko izmišljamo nove pisave, ki si jih ni težko zapomniti.

Namen

Intuitivno spoznavanje *ekskluzivnega ali* (*xor*). Otroci vidijo tudi primer kriptografske metode, ki je na prvi pogled dobra, vendar se izkaže za zelo ranljivo.

Trajanje

1 ura

Potrebščine


Za učitelja

- list s skrivnim napisom

Za vsakega otroka


- učni listi

Skritopis

1. Otrokom pokaži list z napisom . Lahko uganejo, kaj piše na njem? V kateri državi uporabljajo to pisavo?
2. Odgovor: v nobeni. To je pisava, kakršno si lahko brez težav izmislimo sami. Na nek prav nič zapleten način jo sestavimo iz naših črk.
3. Razdeli učne liste.
4. Otrokom razloži, da se moramo najprej dogovoriti, kako bomo pisali običajne črke. Uporabljali bomo kvadratno mrežo in črke pisali natančno tako, kot je narisano na vrhu učnega lista.

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

Posebej jih opozori na B, ki je oglat; na I, ki je na sredi polja; ter na D in V, ki ju pišemo malo bolj "ošpičeno", da se razlikujeta od O in U. Strešic ne bomo pisali.

5. Zdaj pogledjmo, kako sestavimo svoje črke. Izberemo si skrivni znak. Ta mora biti sestavljen iz enakih črt, kot so sestavljene črke. Izberimo si znak .
6. Ta znak pišemo čez običajne črke, tako da uporabimo posebno "seštevanje":

$$A + \text{green arrow} = \text{A with green arrow} = \text{K with green arrow} = K$$

Črte skrivnega znaka naredijo tole: če znak, ki ga poskušamo skriti (A), na določenem mestu že ima črto, jo pobrišemo, če je nima, jo narišemo. Skrivni znak na podanih mestih "obrne", invertira, izgled znaka, ki ga skrivamo. (Na tabli ni potrebno napisati celega "računa", temveč lahko popravljamo kar prvo vsoto, znak, ki je v gornjem računu narisano z modro in zeleno.)

Otrokom pokaži še črko K. Skrivni znak ima črto zgoraj in desno; K teh črt nima, zato jih skrivni znak doda. Poleg tega ima skrivni znak diagonalno črto v zgornjem delu; tako črto ima tudi K, zato mu jo skrivni znak pobriše.

$$K + \text{green arrow} = \text{K with green arrow}$$

Poudari še drug pogled (to je namreč ozadje aktivnosti): vsota ima določeno črto samo, če jo ima eden ali drugi od seštevancev, ne pa oba.

7. Otroci naj še sami predelajo kakšno črko. Primerno lahki sta C in H. Zanimiva je tudi L.
8. Pokaži otrokom, kako zapišemo besedo MARKO. To imajo tudi na učnem listu.

9. Tako smo se naučili skriti besedilo: besedilo skrijemo tako, da k vsaki črki "prištejemo" skrivni znak. Kako pa takšna besedila beremo? Recimo, da nam je nekdo poslal besedo, ki so jo otroci videli na listu na začetku. Vemo, da je skrita s skrivnim znakom, s katerim smo se igrali zdajle. Kako iz skrivnih črk spet dobiti prave? Prepusti otrokom, da poskusijo sami odkriti pravilo.
10. Zelo preprosto je: spomnimo se, da skrivni znak naredi črte, kjer jih ni bilo, in jih briše, kjer so bile. Če hočemo priti do originalne črke, moramo to le ponoviti – kjer ima skrivni znak črte, jih spet pobrišemo, kjer jih nima, jih spet dodamo. Za primer jim lahko pokažeš prvi znak

$$\underline{5} + \uparrow = 5$$

11. Če presodiš, da bodo otroci razumeli, lahko pokažeš tudi nekoliko bolj matematično razlago. Skrivna črka $\underline{5}$ je nastala tako, da je nekdo seštel 5 in \uparrow , $5 + \uparrow = \underline{5}$. Če k $\underline{5}$ še enkrat prištejemo \uparrow , v bistvu računamo $5 + \uparrow + \uparrow$. Namesto, da bi seštevali z leve proti desni, najprej seštejmo zadnja člena.

$$5 + (\uparrow + \uparrow) = 5 + \square = 5$$

Če nekdo k običajni črki prišteje skrivni znak in ga nato prištejemo še enkrat, se bosta skrivna znaka med seboj uničila, zato spet dobimo prvotno črko.

Torej: recimo, da se z nekom dogovorimo za skrivni znak, ki ga bomo uporabljali. Ta bi nam rad poslal neko besedilo. Skrije ga tako, da mu prišteje dogovorjeni skriti znak. Če ga hočemo prebrati, moramo le ponovno prišteti skrivni znak, pa se spet pokaže originalno besedilo.

12. Otroci naj zdaj sami preberejo skriti napis.
13. Opozori otroke na nenavadno lastnost tega seštevanja: enega zraven drugega napiši naslednje tri račune.

$$\underline{5} + \uparrow = \underline{5} \qquad \underline{5} + \uparrow = 5 \qquad \underline{5} + 5 = \uparrow$$

Vrtimo jih lahko, kakor hočemo: ko seštejemo dva znaka, dobimo tretjega.

Prvi račun: ta, ki skriva besedilo, sešteje običajno črko in skrivni znak ter dobi skrivno črko.

Drugi račun: ta, ki bere skrito besedilo, sešteje skrivno črko in skrivni znak ter dobimo običajno črko.

Tretji račun? Če seštejemo skrivno črko običajno črko in običajno črko, dobimo skrivni znak. Kdo pa potrebuje tega? Bomo videli.

14. Povej, da je lepota tega skritopisa v tem, da nam omogoča, da si izmišljamo nove pisave tako, da si preprosto izmislimo nov znak. Kaj bi nastalo iz besede MARKO, če bi jo skrili z znakom ?

MARKO + □ = □ □ □ □ □ □ □ □

Saj to je videti skoraj kot korejska pisava!

15. Vsak otrok naj si izmisli svoj znak in z njim skrije eno besedo. Kot mrežo lahko uporabi učni list ali list karirastega papirja. Otroci naj si izmenjajo besede med seboj (pokažejo naj tudi skrivne znake!) in jih preberejo.

Dodatna vprašanja

1. Bi lahko namesto skrivnega znaka uporabljali kar kakšno črko? Kaj se zgodi, če k vsaki črki besede MARKO prištejemo S?
2. Kaj pa, če kot skrivni znak uporabimo črko M? Otroci naj seštejejo OSKAR in M. Pisava, ki jo dobimo s črko M, ima neko zanimivo značilnost.
3. Kaj pa dobimo, če seštejemo MARKO in M? Koliko je M+M?
4. Bi lahko uporabljali dva skrivna znaka (ali skrivni črki), ki bi ju izmenjevali? Kaj, če bi sešteli besedi BENJAMIN in SPSPSPSP? Se pravi

BENJAMIN
+ SPSPSPSP

Torej, k B-ju prištejemo S, k E-ju P, k N-ju S...

5. Kaj pa, če bi imeli kar skrivno besedo? Recimo, da je naša skrivna beseda EVA. Da skrijemo sporočilo, da BARBARA JE JOGURT, bi sešteli

BARBARA JE JOGURT
+ EVAEVAE VA EVAEVA

6. Si lahko izmisliš skrivni znak, ki bo iz vseh A-jev naredil E-je?

Ta skritopis ni preveč skriven

1. Otroke izzovi, naj preberejo naslednji napis (imajo ga tudi na učnih listih). Morda je skrit s katerim od skrivnih znakov, ki smo jih že uporabljali, morda pa s kakšnim novim, še neznanim znakom.



- Če jim ne gre, jih opozori, da je v besedilu vsaj ena izdajalska črka. Ena črka, ki ima neke črte, ki se pojavijo samo pri njej.
- Če še ne gre, pomagaj: četrta črka z desne je M. Če vedo, da je poznajo "pravo" črko, in vemo, da takrat, ko M-ju prištejemo skrivni znak, dobimo \mathbb{M} : bi znali izračunati skrivni znak? Otroci naj razmislijo.
- Rešitev smo videli, ko smo napisali tri vsote. Poznamo pravo črko in skrivno črko. Če ju seštejemo, bomo dobili skrivni znak. To je tretji račun!

$$\nabla + M = \nabla$$

5. Zdaj, ko poznajo skrivni znak, bi morali otroci brez težav prebrati skrivni napis.
6. V besedilu je še ena izdajalska črka: N, ki ima edina diagonalo. Uporabni sta še dve: črki T in I imata edini navpično črto po sredi. Čim v kakem znaku vidimo takšno črto, vemo, da gre za T ali I. Za katero, pa lahko hitro odkrijemo: predpostavimo, da gre za I, izračunamo skrivni znak in preberemo besedilo. Če ne deluje, pa gre za T; spet izračunamo skrivni znak (razlikoval se bo samo po zgornji črtici) in preberemo besedilo.
7. Otroci naj preberejo še zadnji napis z učnega lista. Skrit je z novim skrivnim znakom.



Z otroki se pogovori o tem, kako varen je ta skritopis. Če vemo, kako deluje, ni kaj pridati: vsak, ki prestreže sporočilo, ga lahko brez večjih težav prebere tudi, če ne ve kakšen je skrivni znak. Če ne vemo, kako deluje, pa je vse odvisno od tega, kako pameten je prisluškovalec. V resnici takšni sistemi, pri kateri le spremenimo pisavo, niso prav varni; čim je besedilo dovolj dolgo, ga lahko prisluškovalec prebere celo, če bi si izmislili povsem novo abecedo, ki niti ne bi bila izračunana iz običajne. Kako se to naredi, pa je za naše znanje žal (malenkost) prezapleteno.

Za kaj gre?

Skrite pisave so privlačna igra za vsakega otroka. V resnici pa je za to aktivnostjo nekaj povsem drugega: *ekskluzivni ali*, *xor*, ena od osnovnih operacij, ki jih uporabljamo v računalništvu.

Najprej si ga oglejmo kot logično operacijo. V šolah se navadno učimo o *in* in *ali*, *konjunkciji* in *disjunkciji*. Konjunkcija je izjava oblike "v ponedeljek bo dež *in* v torek bo sonce". Takšna napoved je pravilna, če drži oboje – dež v ponedeljek in sonce v torek. Disjunkcija je izjava oblike "v ponedeljek bo dež *ali* v torek bo sonce". To drži, čim drži eno ali drugo; če drži oboje, še toliko boljše.

Ekskluzivni ali je izjava oblike "*bodisi* bo v ponedeljek bo dež *bodisi* bo v torek sonce". Napoved je pravilna, če je res natančno eno od tega dvojega. Če ne drži nič (sonce v ponedeljek in poplava v torek), je izjava neresnična. Prav tako pa je neresnična, če drži oboje, namreč v ponedeljek dež in v torek sonce. Držati mora natančno eno.

Drug pogled na ekskluzivni ali je aritmetičen. Gre za seštevanje po modulu 2, torej seštevanje, pri katerem uporabljamo samo 0 in 1. Namesto z znakom + ga bomo označili s $+_2$, pravila seštevanja pa so takšna

$$0 +_2 0 = 0 \qquad 0 +_2 1 = 1 \qquad 1 +_2 0 = 0 \qquad 1 +_2 1 = 0$$

Za računalništvo je še posebej zanimivo seštevanje večmestnih števil v dvojiškem zapisu, kjer seštevamo po bitih, takole

$$\begin{array}{r} 1001101 \\ +_2 0100111 \\ \hline = 1101010 \end{array}$$

Za takšno vsoto veljajo nenavadna pravila, ki smo ju napisali za črke – vsak bit ustreza temu, kar je bila v skritopisu črta.

$$\begin{array}{r} 1001101 \\ +_2 0100111 \\ \hline = 1101010 \end{array}$$

$$\begin{array}{r} 1001101 \\ +_2 1101010 \\ \hline = 0100111 \end{array}$$

$$\begin{array}{r} 1101010 \\ +_2 0100111 \\ \hline = 1001101 \end{array}$$

In v tem je bistvo aktivnosti.