Nagy Sándor

2/3 tevékenység

A kommunikáló ember – titkosírás

A tevékenység rövid leírása: Az emberi kommunikáció összetettsége mindenképpen kiemel bennünket az állatvilág soraiból. Az elvont kommunikáció magasiskolája a titkosírás (kriptográfia), amelynek számos változatát a diákok is könnyen megérthetik, elsajátíthatják és gyakorolhatják. Sőt, saját maguk is kitalálhatnak technikákat, amelyeknek csak a kreativitásuk szab határt. A foglalkozás során elkészítenek egy kódoló/dekódoló korongot (Caesar-rejtjel), amellyel titkosított üzeneteket küldhetnek és fogadhatnak.
Cél: A tanulók kapjanak általános tájékozottságot a kriptográfia témájában. Legyenek képesek elemi szintű vagy akár bonyolultabb kódolási, esetleg dekódolási feladatok megoldására.
Tantervi kapcsolódás: az emberi szervezet felépítése, működése, a testi-lelki egészség
Tantárgyi kapcsolódás: magyar nyelv és kommunikáció, technika és tervezés, történelem, digitális kultúra
Megismerési módszer: megfigyelés, leírás, mérés, modellezés
Anyag, eszköz: páronként 2 db eltérő színű A/4-es méretű színes kartonpapír, körző, szögmérő, ceruza filctoll, 1 db miltonkapocs, olló, okoseszköz internetelléréssel
Időigény: 35 perc *(az osztály összetételétől és érdeklődésétől függően tetszőlegesen hosszabbítható)*

A TEVÉKENYSÉG MENETE

Párokban dolgozzunk!

1. *(10 perc)*: **Tájékozódás kriptográfia témában**

- Minden pár nyissa meg az **1. melléklet**ben található linket. Tanulmányozzuk a **„behelyettesítéses módszereket”** és válasszunk ki csoportonként egyet, amit megértünk, érdekesnek találunk, és amit néhány mondattal és példával illusztrálva be tudunk mutatni a többi csoportnak.

2. *(10 perc)*: **A Caesar-rejtjel kódoló/dekódoló korongok elkészítése**

- Az egyik színes kartonpapírra rajzoljunk körzővel egy 10 cm-es sugarú kört, majd a szögmérő segítségével osszuk 36 egyenlő körcikkre *(10 fokonként berajzolva a kör sugarait).*
- A másik színes kartonpapírra rajzoljunk körzővel egy 8 cm-es sugarú kört, majd ismételjük meg a 36 egyforma körcikkre osztását az előzőekben leírt módszert használva.
- Ollóval vágjuk körbe mindkét körlapot!
- Mindkét korongra filctollal írjuk fel a karakterkészletet (1 körcikkbe 1 karaktert írva): az angol ABC 26 betűjét valamint 0-tól 9-ig a számjegyeket **(2. Melléklet 1. ábra)!**
- Közös középpontban rögzítsük a két korongot a **(2. Melléklet 2. ábra)** alapján a miltonkapoccsal!

3. A Caesar-rejtjel kódoló/dekódoló korongok használata

Kiindulási állapotként a nagyobb és a kisebb korong karakterkészlete szinkronban van.
A tanulópárok egyezzenek meg, hogy **melyik irányba és hány karakterrel fordítják el a belső korongot.**

Kódolásnál: az eredeti üzenet karaktereit a külső tárcsán keressük és a belsőről leolvasva írjuk le a „titkosított üzenet” karaktereit.
Dekódolásnál: a „titkosított üzenet” karaktereit a belső tárcsán keressük és a külsőről leolvasva írjuk le az eredeti üzenet karaktereit.
Példa: a belső tárcsát az óramutató járásával megegyezően forgatjuk el 3 karakter távolságba

- eredeti üzenet: VARLAK 5KOR A MEGBESZELT HELYEN
- kódolva: S7OI7H 2HLO 7 JBD8BPWBIQ EBIVBK

4. Lezárás, értékelés

Sikeres a foglalkozás, ha:

- a munkacsoportok elkészítik a működőképes eszközüket
- sikeres üzenetkódolásokat és -dekódolásokat hajtanak végre
- motiváltan és kreatívan dolgoznak akár saját kódkulcsok elkészítésével is.

VÁLTOZAT

- a belső, kisebb (kódtárcsára) véletlenszerűen is felírhatják a karaktereket – a lényeg, hogy az üzenőpárok kódtárcsái azonosak legyenek
- a kódtárcsára tetszőleges grafikus karaktereket is választhatnak
- tárcsáik segítségével igyekezzenek megfejteni más munkacsoportok üzeneteit, anélkül hogy tudnák az elforgatás mértékét – *ez már egy nehezebb feladat; nagyon motivált és jó képességű tanulókkal valósítható meg!*
- egy harmadik, még kisebb átmérőjű tárcsa beiktatásával (a megfelelő beállítások mellett) megvalósítható a kétszintű kódolás – még inkább megfejthetetlenné téve az üzenetet az „illetéktelenek” számára.

HÁTTÉR

Biztassuk a tanulókat, hogy engedjék el a fantáziájukat és a korábban megadott linkről inspirálódva próbáljanak ki más kódrendszereket vagy adott esetben alkossák meg a saját kódkulcsukat.
A kriptográfia rendkívül szerteágazó téma – ezt hangsúlyozhatjuk pusztán csak azzal, hogy nem szabunk határt a tanulók kreativitásának a „kódkulcs” megalkotásakor.
Hangsúlyozzuk, hogy csakis akkor működik a kódolás/dekódolás folyamata, ha mindkét félnél azonos módon állítják be a tárcsát/tárcsákat.

1. melléklet: A kriptográfia története (link)
2. melléklet: Fotók a korong elkészítéséről