**Krüpteerimise teemaline õpituba**



**Teema:** Krüpteerimine

**Läbiviijad:** Carolin Tõntsu, Pirjo Jõelo, Kaspar Jesmin, Leonard Ladva , Daniel Kivi

**Sihtgrupp:**

* vanuserühm 12-15
* klassid, kellel on võimalus kasutada arvuteid
* klassid kellel on informaatika tunnid

**Eesmärk:** Osalejad saavad uusi teadmisi krüpteerimise, erinevate krüpteerimisviiside kohta ning lühida ülevaate krüpteerimise ajaloo kohta. Hiljem oskavad osalejad kasutada saadud teadmisi praktilises osas mängu läbimisel. Lisaks sellele saavad osalejad aru, kuidas toimib krüpteerimine ning kuidas ennast ja oma andmeid internetis liikudes paremini kaitsta.

**Töötuba:**

Koosneb kahest osast:

1) **Teooria** (45 min)

2) **Praktika** (45 min)

**Teooria**

Teooria osas räägitakse lahti, mis on krüpteerimine ning algoritmid üleüldiselt, käidakse lühidalt läbi kõige tähtsamad sündmused krüpteerimise ajaloos, räägitakse paarist krüpteerimise võttest ning binaarsüsteemi alustaladest. Lisaks sellele tuuakse esitluse lõpus välja, kus tänapäeval saadud teadmisi vaja läheb. Teooria osale on lisatud ka praktilised osad terve teooria vältel. Alguses saavad osalejad näidata oma juba olemasolevaid teadmisi Mentimeetris sõnapilve täites. Peale selle on osalejatel võimalus teha praktiliselt läbi ajaloo tutvustuse juures erinevaid krüpteerimise viise. Selleks läheb osalejatel vaja nutiseadet. Kogu teooria osa toetub PowerPoint esitlusele.

**Esitluses käsitletavad teemad:**

1. Mis on krüpteerimine?
2. Algoritmid
3. Krüpteerimise ajalugu (tähtsamad sündmused)
4. Krüpteerimise viisid
5. Binaarsüsteem
6. Kus kasutatakse krüpteerimist?

NB! Täpsem informatsioon esitluse kohta on failis “Esitluse käsikiri”.

**Praktika**

Töötoast osavõtjad saavad kinnistada oma uusi teadmisi pärast teooria osa omandamist praktilises osas, kus läbitakse sarnast protsessi käsitsi, mida läbivad programmid paroolide krüpteerimisel.

Ülesanne on jagatud kuueks erinevaks etapiks. Igal etapi teel saab osaleja kontrollida oma vahevastust. Etappe läbides peab osaleja kasutama teoorias tutvustatud krüpteerimise võtteid ning kasutama internetist leiduvat infot. Praktiline osa töötoast on lõimitud teooriaga ning aitab osalejatel saadud teadmisi kinnistada.

Ülesannetele on lisatud ka väike eellugu väljamõeldud isikust nimega Martin Kask. (Eellugu on välja toodud ülesande etappide all.)

**Läbiviimine:**

Ülesande läbimiseks jagatakse osavõtjad kahestesse gruppidesse (võib olla ka rohkem vajadusel) ja iga grupi peale on vaja üht arvutit (interneti ühendusega), paberit ja kirjutusvahendit. Osavõtjad jõuavad ülesandeni PowerPoint esitluse lõpus oleva lingi abil

(link: bit.ly/krupteerimine ). Ülesanded on mõeldud gruppidele iseseisvaks lahendamiseks, kuid küsimuste või probleemide korral võib pöörduda teemat valdava juhendaja poole.

**Eellugu:**

Martin Kask on alzheimeri tõvega mees. Selleks, et omada turvalisemat parooli on Martinil kodus peidetud algoritm, mille järgi ta mõtleb välja parooli. Jälgides algoritmi aita Martinil avaldada oma parool!

**Ülesande etapid:**

Ülesande link: <https://h5p.org/node/436445>

1. Mis vastuse saab Martin kui kasutab enda nime Caesari cipheris nihkega -3? (Kasutades eesti tähestiku, 23 tähte!)

Vastus: jänpek

2. Lisa eelmise ülesande vastuse lõppu Martin Kase haiguse 5. ja 7. täht.

Vastus: jänpekem

3. Liiguta eelmise ülesande vastuses igat täishäälikut 2 täishääliku võrra edasi tähestikus ja igat kaashäälikut 2 kaashääliku võrra edasi tähestikus.

Vastus: lürsomop

4. Lisa eelmise ülesande vastuse lõppu 01101011 01100001 01110011 01101011 (genereeri ümber Binaar koodist ASCII -sse).

Vastus: lürsomopkask

5. Liida eelmise ülesande arvuks tehtud vastuse esimese kuuele tähtedele viimased kuus tähte (esimesele liidad seitsmenda tähe ja teisele kaheksanda)

PS: A + B = D,

AB + DB = EE

Vastus: üpathõ

6. Räsi (hashi) eelmise ülesande vastus (MD5), kasuta väikeseid tähti!

Vastus: 3C7566A56239DD1A69B900CCF4C21A6C