1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 2: Цезарево шифрирање

Доминантна дисциплина	Математика
Резиме	Ученици се упознају с основама криптоанализе, декриптују поруку за коју не знају како је криптована. Упознају Цезарев начин шифрирања који се заснива на замени места слова у азбуци, моно-алфабетска супституција.
Појмови	« Информације » • Цезарево шифрирање се састоји у померању места слова у азбуци • Врло се лако открива шифра
Матријал	За сваког ученика: • Радни лист-B03 • Радни лист-B04

Полазна ситуација

Наставник подсећа на неопходост тајног комуницирања, пре свега у преносу војних наредби (ако непријатљ дозна о маневрима које врши наша војска онда неће бити ефекта изненађења).
Представља криптовану поруку на табли и тражи од ученика да је дешифрују:

QLBKP, H TPKP, KLZ YLUMVYAZ CPLUULUA WHY SH TLY

Научна напомена

- Подесћање на речник :
  Када знамо метод криптирања (то је случај са примаоцем поруке коме је намењена), порналажење реалног послатог текста се назива « декодирање » или « дешифрирање » (зависно од типа коришћеног криптирања) или, општије, « декриптирање » поруке.

Ако прималац поруке није легитиман (и ако *a priori* игнорише како је порука криптована), његови покушаји откривања правог текста се називају « криптоанализа » поруке.

- Конвенција: уобичајено је, у криптографији, да се текстови порука пишу малим словима а шифрирани тесктови великим словима. Од сада ћемо користити ову конвенцију. Поједностљење криптоанализе реализујемо тако што користимо интерпункцију и размаке између речи а игноришемо акценте).

Истраживање (по паровима)

Ученици се расподељују у парове, покушавају да направе криптоанализу поруке на табли. Вероватно ће помислити на метод коришћен на претходном часу у вези коришћења писања помоћу огледала.
Мало је вероватно да ће успети у првом покушају, изузев ако већ нису упознати с Цезаревим шифрирањем.

Заједничко представљање

Одељење, после низа насумичних покушаја покушава да заједнички нађе како да се реализује криптоанализа поруке.
Наставник може да води ученике у настојању да нађу које слово се најчешће појављује у француском језику(« e »), (*погледајте на часу српског језика које слово се најчешће појављује у српском језику, п.п.*), а које слово је најчешће у овом тексту (« L »). Шта се дешава ако најчешће појављивано слово у поруци « L » заменимо с најчешће појављиваним словом у француском језику, « e »? Добијамо:

Q**e**BKP, H TPKP, K**e**Z Y**e**UMVYAZ CP**e**UU**e**UA WHY SH T**e**Y
због боље читљивости написано је мало слово « e » у болду.

Запажамо да су слово E и L померени за 7 места у азбуци. Шта се дешава ако је порука криптована тако да су слова померена за 7 места? Покушавамо прво с кратким речима да би видели да ли ова хипотеза функционише. Заменимо сад « L » са « e », значи померамо за 7 места. Истим методом,

- Друга реч поруке « H » постаје « a ». Што је кохерентно јер је « a » реч од једног слов акоје се често појављује у француском језику
- 4-та реч поруке, « K**e**Z », ае трансформише у « des » (што је такође често појављивна реч);
- последња реч поруке, « T**e**Y », се трансформише у « mer » (и тако даље).

Ова етапа нам потврђује да смо на добром путу па даље настављамо декриптовање целе поруке на овај начин. Добијамо:

jeudi, a midi, des renforts viennent par la mer (*четвртак, у подне, појачања стижу морем, п.п.)*
(подсећање: нисмо узели у обзир акценте, а стварни текст смо написали малим словима)

Одељење закључује да је успешно урађен пример криптоанализе поруке тражењем најчешће појављиваног слова и уз помоћ кратких речи. Наставник обајшњава да је у питању Цезарев начин шифрирања који је Јулије Цезар често користио када је слао тајне поруке (дипломатске или војне). Наставник напомиње да није обавезно померање слова за 7 места, нега се може употребити било које померање. Коришћење померања се назива « **кључ** ». Познавање вредности кључа омогућује лако декриптовање поруке.

Педагошка напомена
Јулије Цезар је користио више различитих кључева у дипломатској и војној кореспонденцији. Најпознатија је била она са померањем слова за 3 места у азбуци, познато као « Цезарево шифрирање ». Овде смо одабрали померање за 7 места, а не за 3, да би избегли ситуацију да, деца која већ знају за Цезарево шифрирање, не нађу истог тренутка решење.

Вежба (у паровима)

Ученици, подељени у парове, увежбавају Цезарево шифрирање:

- Сваки ученик бира кључ и шифрира поруку од десетак слова (што је довољно за вежбу!) ;
- Шаљу шифрирану поруку и њен кључ свом суседу, који затим помера слова у инверзном смеру од оног коришћеног при шифрирању поруке.

Концепција машине за шифрирање/дешифрирање (заједнички)

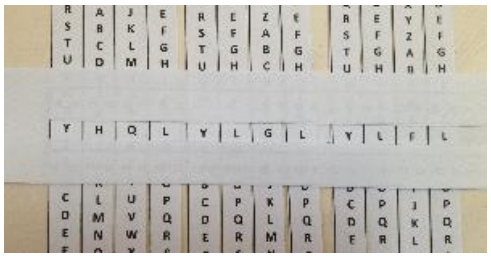
Ако не познајемо вредност кључа, можемо да покушамо да је нађемо (као што смо радили на примеру најчешће појављиваног слова), или пак можемо да тестирамо све могуће кључеве. Наставник пита ученике колико кључева је могуће наћи при Цезаревом шифрирању. Одговор је 25 (у случају француске азбуке), јер можемо да померамо слова азбуке за 1 место (кључ = +1), за 2 места… до 29 места (кључ= +30, А постаје Ш, у случају ћириличног писма!).
Ако се порука криптује према Цезаревом шифрирању у случају француске азбуке биће 25 кључева за тестирње, што није тако дуго! Наставник тражи од ученика да размисле о систему који би омогућио да се одједном прочита 25 могућих порука, и да се тако нађе она права.

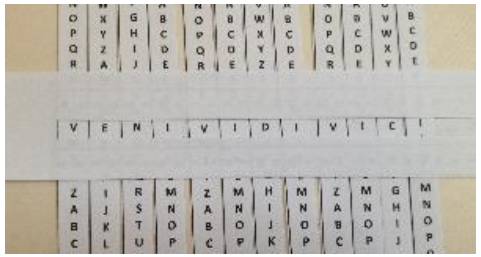
Први тип уређаја је цилиндар за шифрирање.

На доњој слици су представљена одштампана сва слова од A до Z на језичцима од 138x5mm који су затим постављени на картонски цилиндар Језичци су прилепљени на својим крајевима, а затим навучени на картонски цилиндар, тако да могу да се покрећу око своје осе. Померајући их можемо врло брзо да шифрирамо и дешифрирамо поруку. Овде , « LE CODE DE CESAR » (читљив на централној линији постаје « MF DPEF EF DFTBS » с кључем +1 (линија испод), итд..
Језичци се штампају коришћењем Радног листа –B03.

Други тип оруђа је систем од две равни постављене једна поред друге.

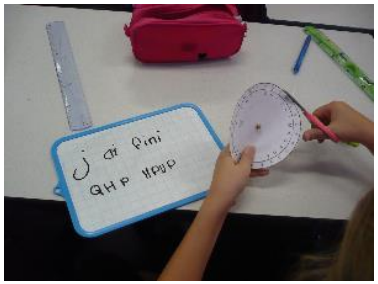
Сваки језичак садржи две азбуке (тако да се A надовеже на слово Z јер овде, супротно од цилиндра, језичци нису самоповезани). Користећи лењир тржимо да се појави порука. Затим, језичци остају фиксирани, а ми померамо вертикално у једном или у другом смеру лењир да би прочитали шифрирану поруку. Напомена: « VENI VIDI VICI » је славна изрека Јулиј Цезара (Дођох, видех, победих).





Трећи тип оруђа је диск за шифрирање.

Састоји се из 2 концентрична повезана диска.
На ивицма дискова су слова азбуке. Померајући диск један у односу на други лако шифрирамо и дешифрирамо било које слово. Дискове можете добити помоћу Радног листа –B04.



Употреба машине за шифрирање/дешифрирање (појединачно)

Сваки ученик прави своју машну за шифрирање, према једном од 3 претходно описана начина (или на основу неке друге идеје која се појави у одељењу!).

Продубљивање

На математици или технологији могуће је направити друга оруђа критографије. На пример, *scytale* (реч је о шифрирању премештањем, код кога су слова помешана, па није у питању шифрирње супституцијом, код кога се слово замењује другим словом …).
