1, 2, 3, кодирај ! - Активности циклуса 4 - Пројект « Криптографија » - Час 1: Како комуницирати тајно?

Доминатна дисциплина	Математика
Резиме	Ученици траже методе које им омогућују да криптују поруку, дискутују поузданост тих метода.
Појмови	« Информација » • Криптографија се бави заштитом комуникација на следеће начине: Трансформишући поруку тако да је она неразумљива (изузев за оног коме је намењена), тај поступак се назива шифрирање; Прикривајући поруку, поступак познат као стеганографија • Криптоанализа је наука која се бави "откривањем" шифри « Алгоритам » • Алгоритам је метод који омогућује решавање проблема.
Материјал	За сваког ученика: • Радни лист-B01 • (факултативно), Радни лист-B02 • (факултативно) огледало

Полазна ситуација

Наставник подсећа на актуелну друштвену дебату у вези поверљивости размене информација (телефонско прислушкивање, надзирање интернета…) и усмерава дебату у знатно шири историјски контекст. Наиме, људи су одувек желели да заштите своје комнуикације (при слању љубавних писама, војних наредби, или дипломатских информација…) иако су истовремено желели да открију тајне својих суседа и/или непријатеља.
Наставник предлаже ученицима да током наредних 5 минута напишу на шта их асоцира реч « криптографија ». Предлоге ученика пише на табли. Неколико примера најчешћих одговора ученика циклуса 4 (виши разреди основне и почетни средње школе, п.п.): криптограм, информатика, алгоритам, криптирање, декриптирање, кодирање, декодирање, пиратерија, робот, сигурност, заштита података, прост број…

Предлаже ученицима **једноставан проблем: како написати поруку, на пример SMS, неком пријатељу а да она буде неразумљива другим лицима** (посебно, родитељима, професорима, итд.).
Закључак заједничке дискусије је да се пошаљилац и прималац поруке морају договорити у вези неког « кода » (речник ће бит касније прецизиран).

Истраживање (по групама)

Ученици, подељени у мале групе (на пример, 4 ученика), би требло да размисле о неком коду који ће им омогућити да тајно комуницирају.Потребно је да јасно објасне свој метод и то илуструју на неком примеру уз једно питање и одговор.
Напомена: због поједностављења проблема није потребно правити разлику између великих и малих слова, уз занемаривање знакова за акценте.

Заједничко представљање

Наставник организује заједничко представљње резултата током ког различите групе представљају своје предлоге, затим следи заједничка дисикусија. Потребно је истражити да ли « код » :

- омогућује комуникацију (да ли се 2 учесника разумеју? да ли има неодређености?) ;
- је врло лак за учење и употребу;
- се тешко « разбија » од стране неког ко са њим није упознат.

Примери ученичких предлога:

- Измешати ред слова у поруци: написати је с десна налево, писање у « огледалу » (ред и облик слова су инверзни). Ако се прихвати овај прдлог потребно је да ученицима дате огледала како би то могли и да ураде.
- Скривање поруке у оквиру неке друге поруке
- Елиминисање неких карактера (на пример самогласника).
- Замењивање слова у пруци бројевима (A →01, B → 02…). Пажња, ако замените A са « 1 », шифрирање је лако, али зато дешифрирање постаје неодређено: да ли « 13 » значи « 1 » затим « 3 », тј., A затим C, или тринаесто слово, тј., M? Управо због елиминасања неодређености је потребно користити 2 цифре за свако слово.
- Замењивање слова симболима а не шифрама, као код Морзеовог кода (цртице, тачке, празни простори …)
- Употреба мало познатог страног језика (на пример, навахо).
- Употреба језика који је намењен само за нашу комуникцију. Овде није у питању замена цифрама или неким другим симболима, него су речи замењене другим речима.
- Говорити својим језком, уз елиминсање размака, акцената и интерпункције.

Ако неке предлоге нису направили ученици немојте их сад уводити, то ће бити урађено касније током часа.

Педагошка напомена
Током ове дискусије појавило се неколико речи које је потребно прецизније дефинисати:

- « **Криптирати** » неку поруку, значи да је она тако формулисана да је њен садржај разумљив само оном ком је намењена. Порука, дакле, није скривена али је неразумљива другима. Ова активност се назива криптографија (користе се глаголи « криптирати » и « декриптирати »). **Криптоанализа** се бави налажењем метода који нам омогућује да се декриптује нека порука од стране оних којима није намењена.
    - Када су речи замењене другим речима или исказима (пример: « Јупитер » означава професора математике), онда се то криптирање назива « код ». Употребљавамо глаголе **« кодирати » и « декодирати »**.
    - Када су пак слова замењена (али не и речи), било другим словима, било другим знацима, онда говоримо да « шифрирамо ». Користимо глаголе **« шифрирати » и « дешифрирати »**.
- Могуће је и скривање поруке, а не њено формулисање у неразумљивом облику. Порука се у том случају шаље таква каква јесте али подлога на којој се шаље има скривену поруку (на пример, папир уролан у пенкалу …). Ова активност је позната као **стенографија**. Коришћена је у старо време а може бити и предмет неког часа продубљивања.
- Неки предлози ученика (попут Морзеовог кода) не сврставају се ни у криптографију ни у стенографију. Није упитању ни скривена или поверљива порука, него једноставно налажење практичне подршке. Код Морзеа се словима придружују краћи или дужи електронски импулси и то је коришћено код слања телеграма. Морзе може представљати добро средство за изучавање кодиране информације, али није криптографија.

Вежбе

Наставник расподељује ученицима Радни лист-B01 који садржи више порука криптованих (шифрираних или кодираних) различитим методама. Ученици би требало да нађу праву поруку.

Радни лист-B02 садржи табелу кореспонденције која омогућује да се лако ураде 3 вежбе. Наставник их дели зависно од спремонсти ученика да реализују овакаве задатке.

Корекција урађених вежби се реализује заједнички.

- Вежба 1: у питању је текст написан помоћу огледала (с десна на лево)
  Криптована порука: SERTTEL SEL RESREVNI D TIFFUS LI
  Декриптована порука: IL SUFFIT D INVERSER LES LETTRES
- Вежба 2: ист текст али без размака између речи што га чини тежим за декриптовање
  Криптована порука: RUDSULPTSECSECAPSESELSNAS
  Декриптована порука без размак : SANSLESESPACESCESTPLUSDUR
  Декриптована порука са размацима: SANS LES ESPACES C EST PLUS DUR
- Вежба 3:у питању је једноставна кореспонденција између слова и њиховог места у азбуци (A →01, B → 02…)
  Криптована порука: 15112021031514140109191201121608010205 20
  Декриптована порука: OKTUCONNAISLALPHABET
  Декриптована порука са размацима: OK TU CONNAIS L ALPHABET

Вежба 3 омогућује да се види да шифрирање слова помоћу 2 броја омогућује шифрирање и других карактера (мала слова, акцентни карактери …) јер је употребљено само 26 бројева од 100 могућих (од 00 до 99).

Закључак

Наставник наглашава заједничку карактеристику свих метода криптовања (кодирања или шифрирања) који су овде разматрани. Прелаз од реалног текста на криптовани текст захтева исту операцију као и прелаз од криптованог тескта на реални текст. Може да прецизира да то није увек случај (видећете на Часу 5). Одељење заједнички дефинише кључне концепте поменуте на почетку овог часа: криптографија, криптоанализа, шифрирање, стенографија и алгоритам.

Продубљивање применом *Практичног интердисциплинарног подучавања*

- У Српском језику: изучавање улоге интерпункције у разумевању неког текста.
- У математици: кодирање (Морзеово кодирање, ASCII, бинарно кодирање…)
  Одељење може да изучава како информација моможе бити кодирана тако да се лако стокира и преноси. Морзеово кодирање је добар историјски пример, док су ASCII и бинарно кодирање више у складу с данашњом информатиком.
- Стенографија је добар пример за физику, хемију и математику.
  Наш пројект третира на продубљен начин проблематику шифрирања. Одељење може да реализује додатне часове математике и/или физике и хемије за изучавање стенографије.
  - Прављењем, на часовима *физике и хемије*, « симпатичног » мастила (с млеком и лимуновим соком) које омогућује да се њиме написан текст појави тек на повишеној температури
  - Инфромација, на часовима *математике*, је скривена унутар неке слике (формат pbm). Овај поступак захтева 3 до 4 часа, јер ученици морају прво да се упознају с репрезентацијом слике (кодирање пиксела) као и кодирање текста у ASCII и бинарном коду. Када су ученици у стању да кодирају проуку пикселима у оквиру нивоа сиве слике, на пример (довољно је 256 нивоа сиве боје). Голим оком није могуће било шта приметити, дока се при отварању слике у текст едитору може наћи скривена информација (после бинарног декодирања → ASCII).