1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 12: Програмирање анализе фреквенције

Доминантна дисциплина	Математика
Резиме	Ученици, настојећи да олакшају начин криптоанализе, развијају нови програм који им омогућује да прорачунају фреквенцију сваког слова у поруци.
Појмови	« Алгоритми » • Неке петље, познате као "условне", се понављају док се не испун неки услов.
Материјал	За сваки пар ученика • Компјутер с везом на интернет (при коришћењу on-line верзије *Скрача*) или је *Scratch* претходно инсталиран • Радни лист B14 За одељење • Видеопројектор који се користи при заједничком представљању

Наставник предлаже ученицима да направе програм који ће им омогућити, у оквиру криптоанализе, да конструишу хистограм фреквенције неког текста. Рад се реализује у 2 дела:

- Кеирање табеле која садржи феквенцију сваког слова поруке. Ова етапа не представља неку потешкоћу и биће урађена на овом часу.
- Креирање графика омогућује визуелизацију ових фреквенција. Ова опциона етапа, која ће бити реализована током следећа 2 часа, је знатно тежа (али је зато изузетно интересантна, нарочито због могућности рада са функцијама и њиховом графичком репрезентацијом!).

Педагошка напомена

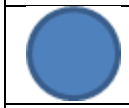
Коришћење термина « фреквенција » није најкоректнија, јер се овде рачуна број појављивања слова у поруци а не фреквенција како је дефинисана у физици. Ми ипак задржавамо овај термин с циљем да успоставимо везу с методом криптоанализе познатим под називом « анализа фреквенције ».

Етапа 1: дефинисање различитих етапа пројекта (15 минута)

Ученици, у првом делу, размишљају о алгоритму који омогућује бројање појаве неког слова (његова фреквенција) у датом тексту. Наставник, зависно од нивоа ученика, може да организује овај час у пару, групно (уз заједничко представљање резултата) или радећи са целим одељењем.

- Бројање појављивања слова « A », у неком тексту, се остварује следећим методом:
  - Прелази се текст од првог до последњег слова
  - Тестира се, за свако слово, да је у питању « A ». Ако јесте, додајемо « 1 » варијабли која броји појављивање овог слова.
- Та бројање фреквенције свих слова текста:
  - Довољно је да претходни метод уопштите увођењем петље која ће обухватити сва слова текста.
  - Вредности ће бити регистроване у табели од 30 места (прво место ће се односити на фреквенцију слова « A », друго на фреквенцију слова « B »…). Наставник објашњава да је у Скрачу ово могуће урадити помоћу варијабле познате под именом « листа ».

Приказујемо пример могуће поделе пројекта на различите етапе (графичка реализација ће бити разматрана на следећем часу):

Тежина	Име етапе	Природа задатка који је потребно решити
	1 – Дефинисање етапа пројекта	• Одељење управо то и ради.
	2 – Бројање фреквенције неког слова у датом тексту	• Писање програма који броји број појављивања слова « A » у датом тексту. • Уопштавање програма на било које слово азбуке и прављење функције • Писање програма за тестирање те функције.
	3 – Попуњавање табеле фреквенције	• Писање програма који преузима неки текст, а затим броји број појављивања сваког слова у том тексту, потом стокира вредности у варијабли типа « листа ».

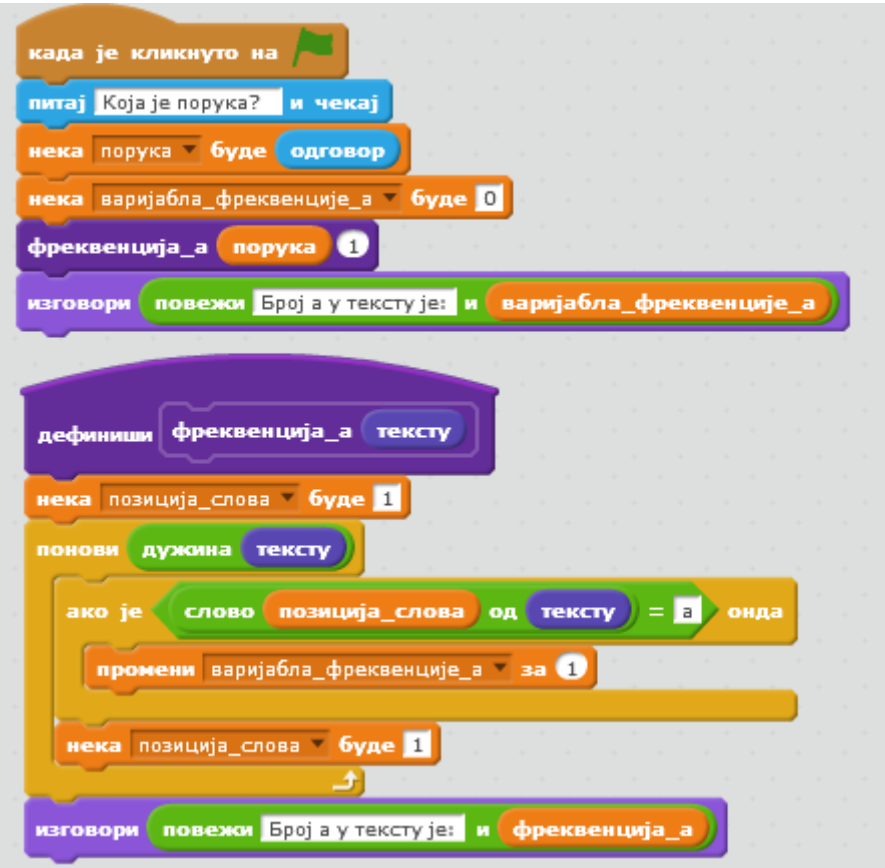
		• Прави се функција и тестира.
	4 – Третман слова с акцентима	• Модификовање програма да би се могли заменити акцентни карактери пре него што се приступи анализи фреквенције

Етапа: прорачун фреквенције неког слова у датом тексту (30 минута)

Ова етапа не представља потешкоћу јер се користе исти појмови као на претходна 4 часа програмирања Цезаревог шифрирања.
Програм који омогућује бројање појављивања слова « А » у датом тескту је следећи :

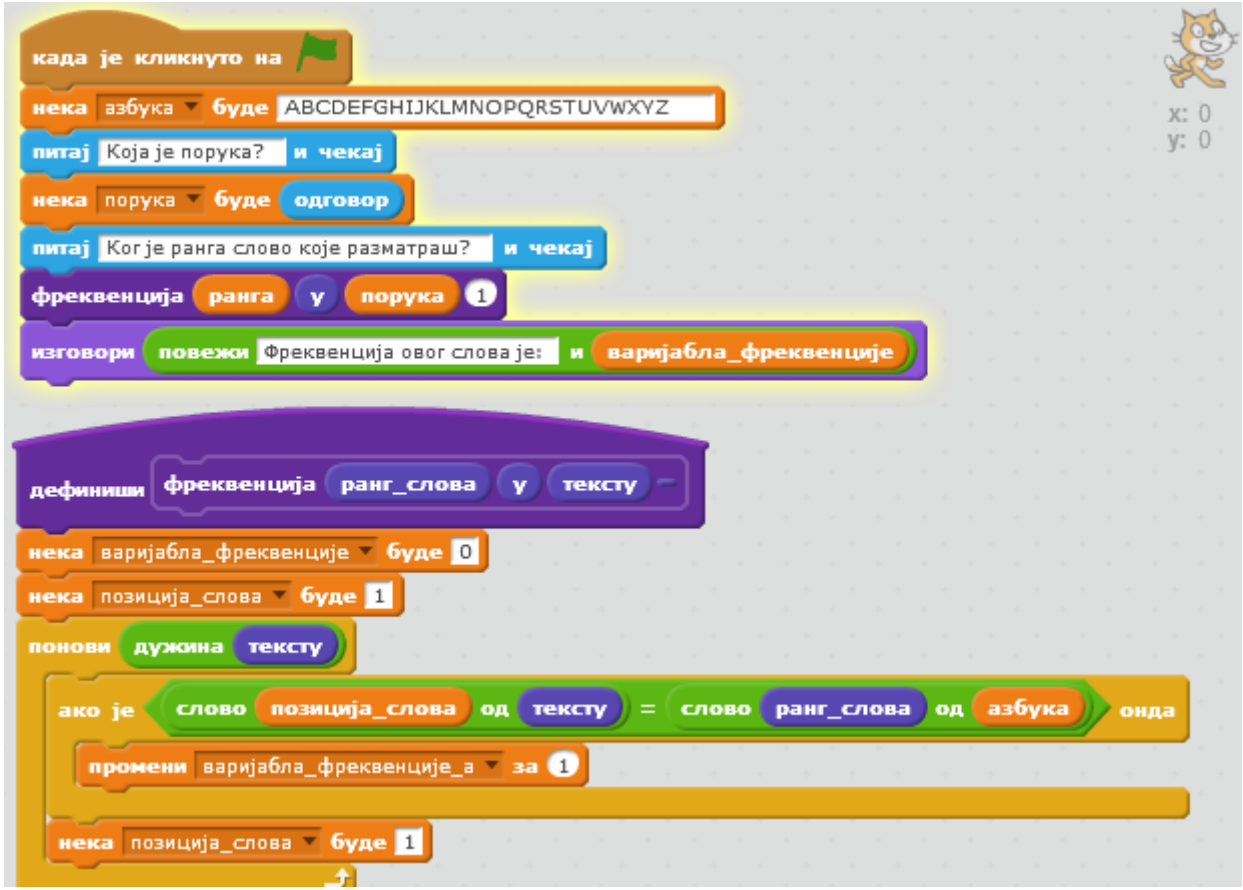
Научна напомена:
Подсећање: *Скрач* је неосетљив на класу слова. Слова « а » и « А » се сматрају идентичним у операцијама које се реализују с низовима карактера.

Програм,изражен помоћу неке функције, постаје:



Напомена :Употреба неке функције захтева промену имена наше варијабле « фреквенција_а » у « Варијабла_фреквенције_а », ако желимо да поштујемо усвојену конвенцију коју смо до сада примењивали.

Ако сад желимо да рачунамо фреквенцију, не смао слова « а », него и било ког слова азбуке, можемо да овај приступ уопштимо замењујући слово « а » с « елементом (ранг) у азбуци », где се под рангом подразумева број између 1 и 30 који представља азбуку од 30 слова према редоследу.



При модификацији својстава функције (преименовање у « фреквенцију » и додавање друге улазне варијабле), потребно је десним кликом на дефиницију те функције одабрати « уреди ». Напомињемо да је варјабла « Варијабла_фреквенције_а » такође преименована у « Варијабла_фреквенције ».

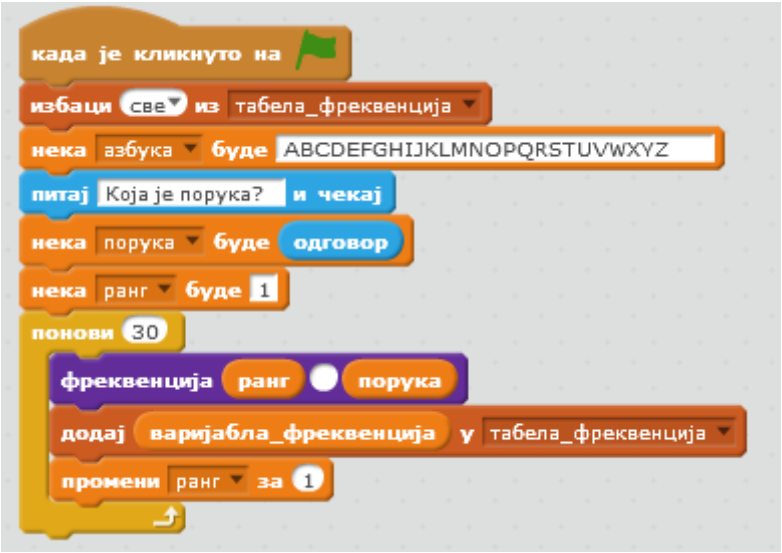
Етапа 3: попуњавање табеле фреквенција (30 минута)

Попуњавање табеле фреквенције за свако слово азбуке захтева варијаблу типа « листа ». Ако ученици нису до сада радили с листама у Скрачу, покажите им како то да ураде. Ово је садржано у Радном листу-B14, у ком је предложена и мала вежба. Предлажемо вам да урадите прву вежбу заједно, а затим и да се организује заједничко представљање за сваку етапу рада, јер само тако можете проверити колико су ученици успели да усвоје нови појам.

Одговори :

- Програм 1: овај програм захтева од корисника да укуца 3 текста, и да ове текстов стокира у варијабли типа « листа » (табела с једном колоном се појављује на екрану). Она је по дифолту празна, а њена дужина је 0.
- Програм 2: Инструкција « избаци… » додата на почетку програм омогућује да се листа буде поново празна.
- Програм 3: програм ће зауставити попуњавање листе само када корисник напише реч « OK ». Листа садржи све елементе које је помено корисник (а « OK » је последњи елемент).
- Програм 4: Овај програм избацује последњи елемент листе (то је, као што смо претходно видели « OK »), и приказује дужину (број елемената) ове листе (без « OK », које је елиминсано). Шаље поруку која ће покренути други програм (види ниже).
- Програм 5: Овај програм, покренут на крају претходног, рекапитулира листу (приказују се, један по један, елементи листе).

Ученици сад знају како креирати, дати полазну вредност и манипулисати листом (додавање елемената, њихово избацивање, приказивање целе листе...). Могу да преузму програм који је направљен на претходном часу, и да га искористе за рачунање фреквенције свих слова азбуке (ове фреквенције се стокирају у варијабли типа « листа »).



Модификација главног програма за рачунање фреквенције сваког слова азбуке.
Напомена: нема потребе да се модификује функција « фреквенца_ранга_у_поруци ».

Ученици верификују функционисање програма тестирајући га на кратким текстовима, у којим могу веома брзо да ручно израчунају фреквенције.

Педагошка напомена:
Поставите, без устручавања, проблем који би ученици требало да реше. На пример, да почну листу с нулама а затим да повећавају сваког пута када се појави слово у тексту (према другом алгоритму, у научној напомени која следи).

Научне напомене
За прављење табеле фреквенција могућа су 2 алгоритма:

- Први алгоритам (који је овде приказан)
  За слово А, прелазимо цео текст, тражимо то слово, и повећавамо број на бројачу кад год га нађемо. Петља садржи 30 слова
- Други алгоритам
  За прво слово текста, пређемо азбуку (да би видели који је његов ранг) повећавамо број на бројачу за овај ранг. Затим петљом обухваитмо сва слова текста. Овај метод је нешто ефикаснији, јер избегава да прегледамо цео текст за свако слово азбуке, укључујући и слова којих нема у тексту. Међутим, овај метод не омогућује коришћење функције коју смо увели у претходној етапи.

Етапа 4 (опционо): замените слова с акцентима (15 минута)

Ова етапа је веома слична оној коју смо реализовали за Цезарево шифрирање ; омогућује да ученици боље разумеју појмове које користе уз мање потешкоћа него што је то било када су радили први пут.
Следећа два опциона часа омогућују визуелизацију табеле фреквенција у форми графика.
