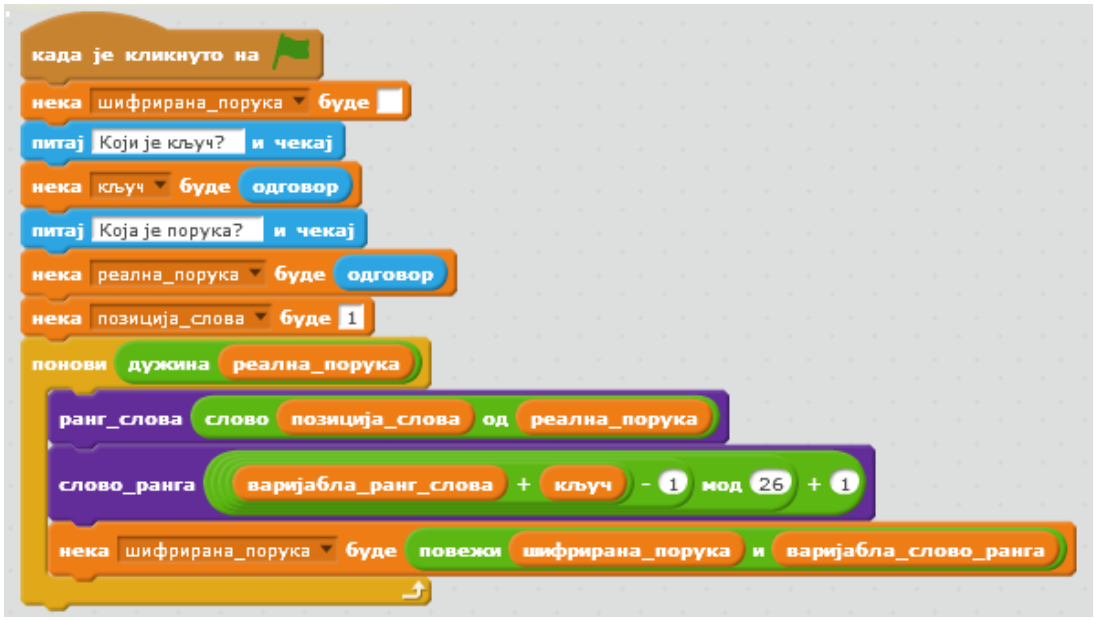
1, 2, 3, кодирај ! - Активност циклуса 4 - Пројект « Криптографија » - Час 11: Програмирање Цезаревог шифрирање(4/4)

Доминантна дисциплина	Математика
Резиме	Ученици завршавају свој програм Цезаревог шифрирања којим су сад у стању да потпуно дешифрују целу поруку, узимајући при том у обзир и размак, интерпункцију и акценте. У стању су да на читљив и разумљив начин коментаришу неки програм. Предложено је и продубљење које се односи на коришћење логичких оператора.
Појмови	« Алгоритми » • За прављење неког логичког исказа користимо логичке операторе попут И, ИЛИ, НЕ. « Машине » • Кмпујтер је, за већину задатака из области шифрирања и криптоанализе, знатно ефикаснији од човека. « Добре праксе програмирања » Постављање коментара у програм олакшава његово читање и размену.
Материјал	За сваки пар ученика • Компјутер с везом на интернет (при коришћењу on-line верзије *Скрача*) или је *Scratch* претходно инсталиран • (факултативно) фотокопија Радног листа B11 За одељење • Видеопројектор који се користи при заједничком представљању За сваког ученика : фотокопија Радног листа B13

Етапа 7: шифрирање целе поруке (20 минута)

Ова етапа не представља већу потешкоћу. Потпуно исто као и у етапи 3, потребно је увести петљу јер не шифрирамо само једно слово, него сва слова поруке.
Програм уводи две нове варијабле: « реална_порука » (представља поруку коју желимо да шифрирамо), и « позиција_слова », која означава које слове поруке тренутно шифрирамо.
Шифрирана порука је добијена груписањем шифрираних слова у свакој етапи петље.
Могући програм је:



Етапа 8: искористите већ направљени програм! (10 минута)

Практикујте да сачувате написане програме јер ће вам затребати! Ученици могу током десетак минута да се играју с програмима и утврде да програм који је коришћен за шифрирање може бити употребљен и за дешифрирање поруке. Уствари, за дешифрирање поруке која је шифрирана с кључм 3, могуће је користити

исти програм, али са кључем који је једнак 30-3 =3 (слова се померају за исти број места,али у другом смеру … што нас доводи до оригиналне поруке) .
Пажња: тренутно, ваш програм није у могућности да разматра интерпункцију (укључујући и размаке) и акценте! То ће се радити опционо после следеће 2 етапе …

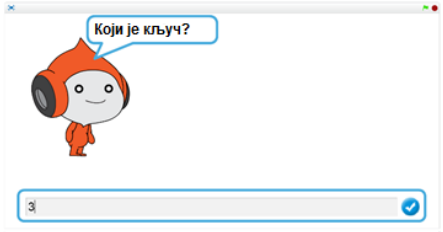
Одељење закључује да је Цезарево шифрирање « симетрично », јер се познавањем кључа коришћеног при шифрирању може реализовати и дешифрирање.

Научна напомена:

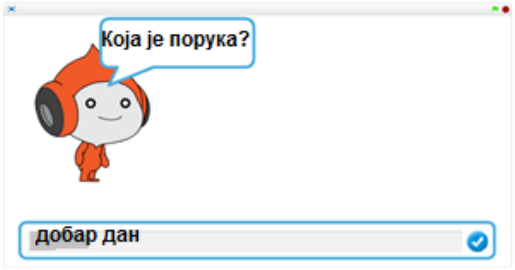
- Симетрично шифрирање, и поред своје комплексности, има врло слабе тачке. На пример, потребно је послати кључ свом саговорнику који ће он искористити за дешифрирање поруке. Евентуалном пресретачу те поруке биће познат садржај послате поруке..
- Постоје и « асиметричне » методе шифрирања, које користе различите кључеве за шифрирање и дешифрирање поруке. Комлексност ових алгоритама (као на пример RSA- Rivest–Shamir–Adleman је један од првих јавних кључева криптосистема) знанто превазилази оно што се очекује од ученика виших разреда основне школе. Ипак, интересантно је да се позабавимо питањем размене кључева. Такви алгоритми се позивају на јавне и приватне кључеве. Можемо шифрирати поруку коју упућујемо саговорнику чију јавни кључ познајемо, и још да му пошаљемо поруку која ће само њему користити да је дешифрује помоћу приватног кључа.

Приказ програма:

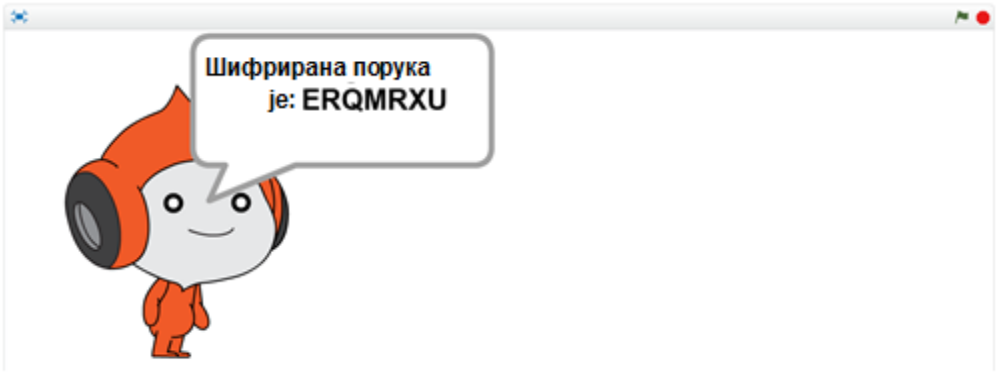
1: Корисник даје кључ с којим жели да шифрира своју поруку



2: Корисник на тастатури куца поруку која се шифрира



3 : Програм приказује шифрирану поруку



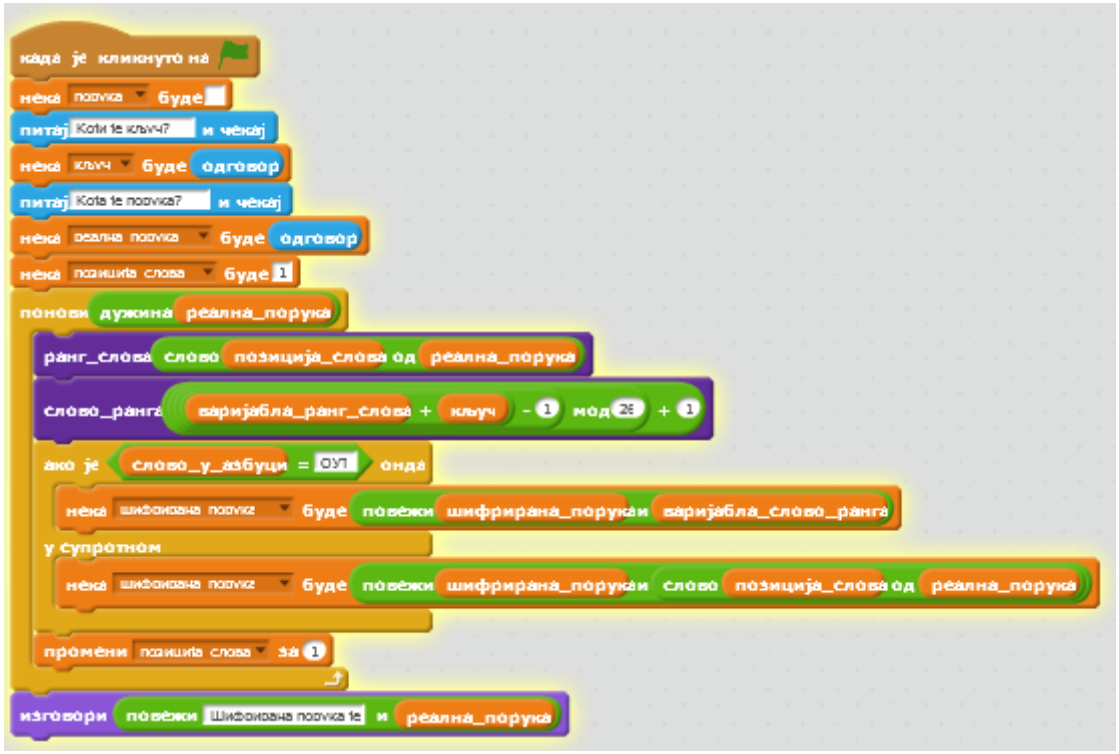
Вероватно је одређен број ученика више напредовао у односу на друге па наставник даје листу нових задатака који ће омогућити побољшање програма:

Тежина	Назив етапе	Природа реализованих задатака
	Етапа 9 – узимање у обзир размака и интерпункције	• Модификовање програма тако да не шифрира размаке и интерпункцију, а који се копира такав какв јесте.
	Етапа 10 – вођење акцентних карактера	• Креирање функције која замењује акцентне карактере реалне поруке с еквивалентном поруком без акцената. • Модификација главног програма тако да шифрира поруку без акцената.
	Етапа 11 – коментарисање свог програма	• Додајте коментаре и тако побољшајте читљивост програма

Напомињемо да, ако су етапе 9 и 10 опционе, онда би етапу 11 морали да реализују сви ученици.

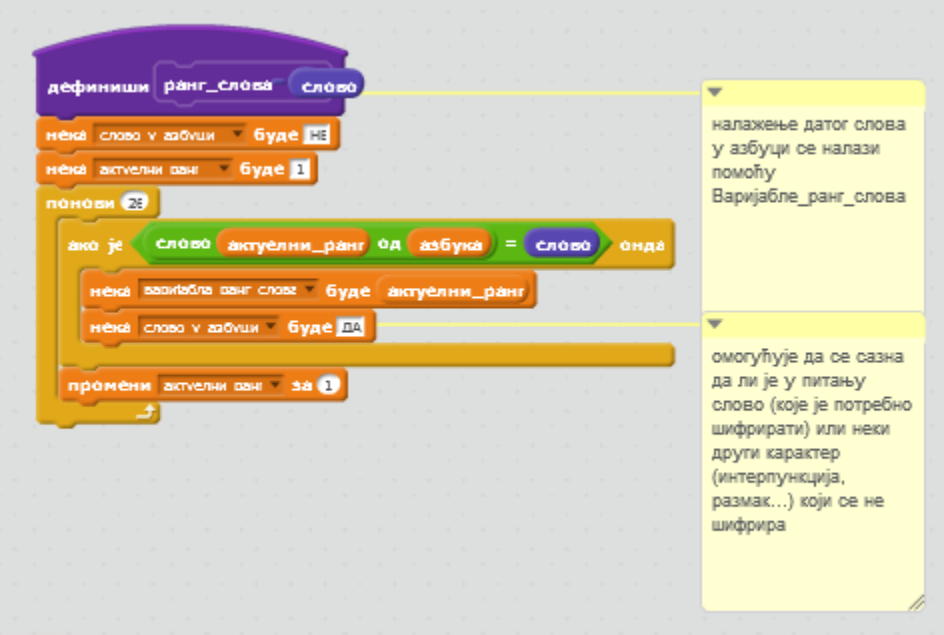
Етапа 9: узимање у обзир размака и интерпункције (20 минута)

Наш програм, у овом стадијуму, не функционише ако реална порука садржи осим специфичних слова и друге ствари (размаци, интерпункција …).
Решење овог проблема се реализује тако што програм не шифрира карактере који нису део азбуке. Уводимо варијаблу (називамо је, на пример, « слово_у_азбуци »). Ако варијабла узме вредност « да »,програм функционише нормално (шифрира се слово). Ако варијабла узме вреднсот « не », програм копира карактере који нису шифрирани.



Програм помера свако слово за вредност кључа, а да се притом не третирају карактери који нису у азбуци.

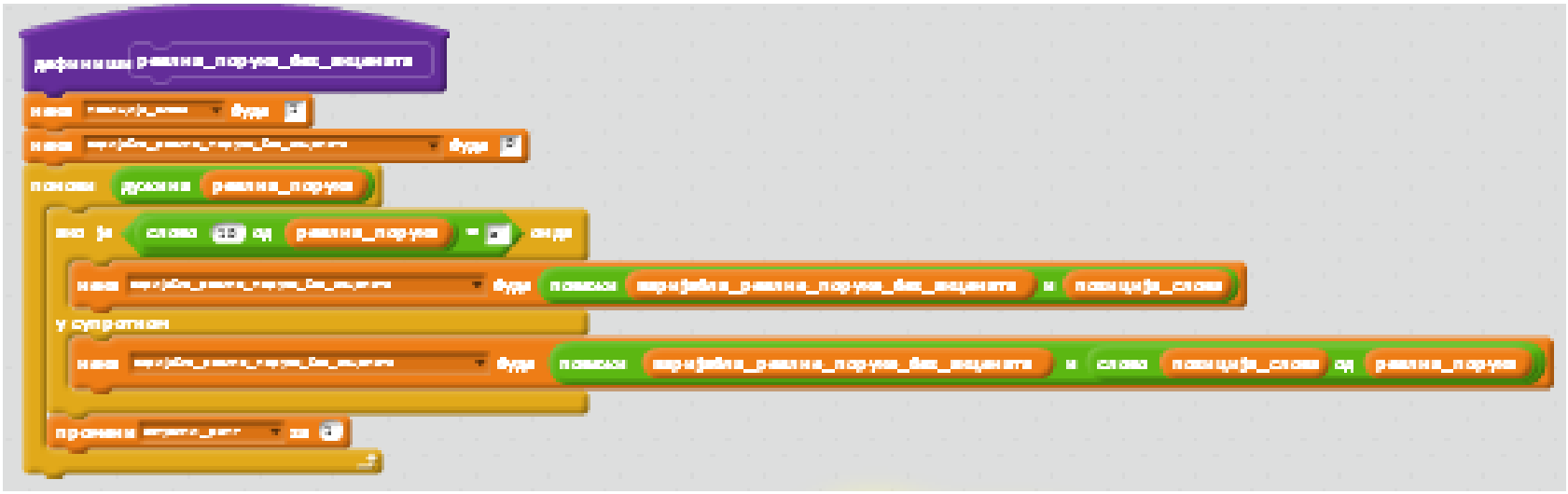
Потребно је верификовати функцијом « ранг_слова » да ли је слово нађено или не. Дакле, функција постаје:



Ова верзија, модификације функције « ранг_слова »
омогућује детекцију да ли је тај каратер присутан у азбуци или не.
NB: додвање коментара је разматрано у доњој етапи 11.

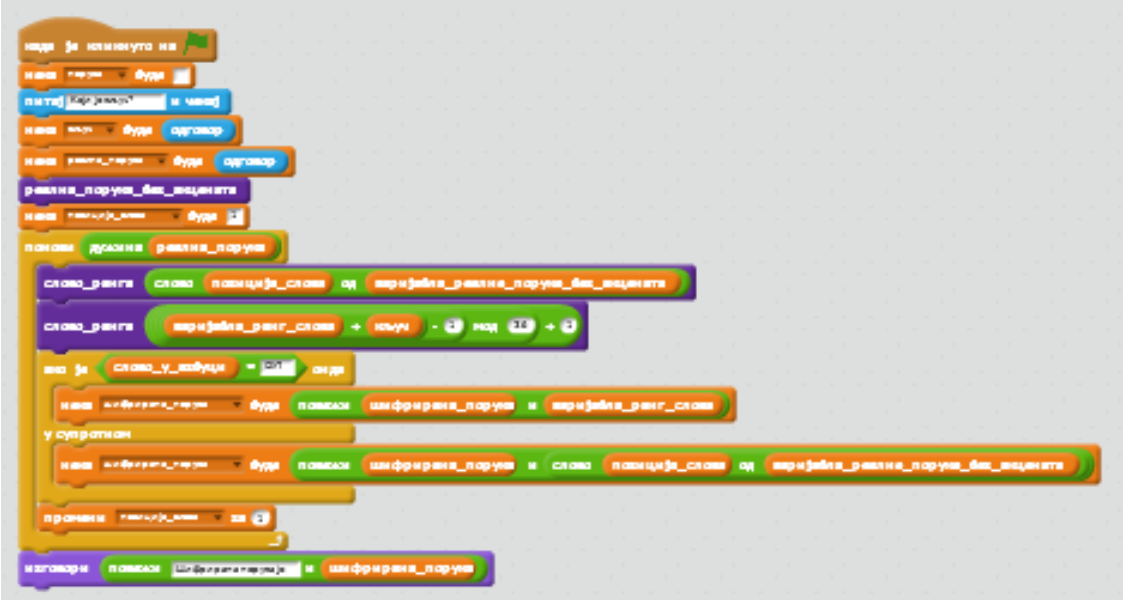
Етапа 10: третман слова с акцентом (20 минута)

Програм, у актуелној ситуацији, не узима у обзир карактере с акцентима. Одељење може, иако то није неопходно, да посвети 20 додатних минута за разговор о овом недостатку. Можемо, на пример, словом « а », заменити свако слово а с акцентом, итд.
Овај рад захтева укључивање више тестова, један у оквиру другог, што за ученике не би требало да представља неку потешкоћу да то реше индивидуално. Ово раде помоћу нове функције назване « реална_порука_без_акцената ». Ова функција копира све карактере без акцената такве какви јесу, а оне с акцентима замењује њиховим еквивалентом без акцента.



Овде смо приказали, због боље видљивости, само једну некомплетну верзију те функције (она само третира « à » и « â »). Потребно је убацити и друге петље АКО…ОНДА…АКОНЕ да би се третирали и други акценти.

Подразумева се да је потребно заменити, у главном програму, варијаблу « реална_поука » са « варијабла_реална_порукаr_без_акцената » па се добија:



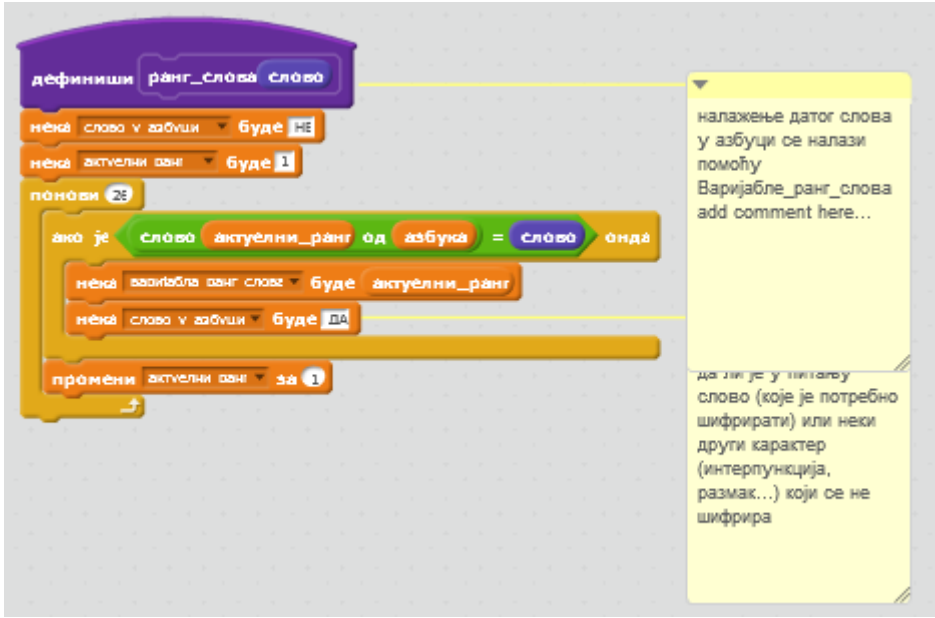
Педагошка напомена:
Уместо убацивања АКО… ОНДА у функцију « реална_порука_без_акцената », пожељније је груписање неких тестова помоћу логичког оператора ИЛИ. На пример, АКО слово=« à » ИЛИ слово=« â » ОНДА заменити са « a ». Зато вам предлажемо да искористите Радни лист-B13 сциљем да се ученици увежбају при коришћењу логичких оператора.

Етапа 11: коментарисање свог програма (10 минута)

Програм коректно функционише, али врло брзо постаје комплексан. Тешко је разумљив другим корисницима. Наставник објашњава како коментрисати свој програм и организвати га на логичан начин.

Педагошка напомена
Требало је да овај начин рада уведемо раније, и да већ од самог почетка имамо јаснији програм, али изгедало нам је да је много боље да се ученици сами суоче с оваквим потешкоћама.

Доле је коментарисана функција « ранг_слова »:



Продубљивање (20 минута)

Ученици могу да реализују активност, манипулације неколико логичких оператора, без компјутера. Вежбе у оквиру Радног листа 13 могу да послуже као помоћ при овим активностима. Пожељније је да ученици прво одговоре на постављена питања а затим да реализују програм који ће им омогућити да верификују своје одговоре.
Одговори на постављена питања су:

Вежба 1:

- метро
- пешке
- пешке
- бицикл (запажамо да су 2 последња програма еквивалентна иако су им форме различите. Резултати нису исти јер је једна од варијабли променила вредност)

Вежба 2:

- 12 (једница није прецизирана… претпоставимо да је у питању еуро)
- 7 + 12 - 3 = 16
- 7 + 12 + 6 - 3 = 22
- 7 + 6 = 13 (у овом случају нема редукције!)

Продубљивање (опционо-2 часа)

Реализовани програм омогућује да се једноставно декларишу слова неког ранга у некој поруци (Цезарево шифрирање). Ученици могу да покушају да програмирају и шифрирање моно-алфабетском супституцијом. Један такав програм:

- захтева кључну_реч за шифрирање;
- трансформише кључну-реч pangrammique (избачени су размаци, doublons…);
- генерише шифрирану азбуку;
- захтева коришћење текста који је потребно шифрирати;
- шифрира текст моно-алфабетском супституцијом.

Наставник може, ако су ученици довољно напредовали у програмирању коришћењем *Скрача*, да им предложи пројект у ком ће масивно користити тестове, логичке операторе, петље унете једна у другу...
Анализа фреквенције, коју предлажемо за часове који следе, је знатно лакша (осим графичког представљања).

Наставницима дајемо комплетан программ с коментарима шифрирања моно-алфабетском супституцијом што ће им омогућити:

- лако креирање вежби (и њихову корекцију) с циљем да се увежба овај метод шифрирања
- да овај пројект реализују, ако желе, с ученицима. Моћиће да програмирају *in extenso*, или пак да програмирају само неке делове, као и да анализирају најтеже делове програма. Јер, анализирање начина рада постојећег програма доприноси његовом бољем разумевању што им је сигурно интересантно.
