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

Доминантна дисциплина	Математика
Резиме	Ученици уопштавају Цезарев начин шифрирања на било које друго шифрирање моно-алфабетском супституцијом. Уче шифрирање поруке помоћу кључне речи или кључне фразе, рачунају број могућих алфабетских шифрирања.
Појмови	« Информације » • Шифрирање моно-аалфабетском супституцијом се састоји у замени сваког слова поруке другим словом • постоји велики број могућих алфабетских шифри • можемо креирати нашу алфабетску шифру помоћу кључне речи
Матријал	За сваког ученика: • Радни лист-B05

Полазна ситуација

Наставник подсећа на оно што је рађено претходног часа у вези Цезревог шифрирања које се састоји у померању слова у азбуци за, увек исти, одговарајући број места (« кључ »). Ово шифрирање се лако открива јер има свега 25 могућих кључева.
Предлаже рафинираниј приступ оваквом шифрирању тако шо би се сваком слову придружило неко друго слово, али без обавезе да то буде увек исти број померених места. Ово се у пракси своди на кореспонденцију 2 азбуке, једне која одговара реалној поруци (у одговарјућем редоследу слова) и друге « шифиране » (измешана слова).

Вежба (индивидуално)

Наставник расподељује Радни лист-B05 сваком ученику и предлаже да уради 2 прве вежбе.
Решење вежбе1 је:

- Реална порука: bonne chance pour casser ce code(*срећно разбијање шифре*, п.п.)
- Криптован порука: TCUUI KMJUKI HCYW KJVVIW KI KCJI

Решење вежбе 2 је:

- Криптована порука: D JB EBUB
- Реална порука : j ai fini (*завршио сам*)

Ученици уче да користе табелу кореспонденције у 2 смера (за шифрирање и дешифрирањье).

Колико има могућих кључева? (заједнички)

Пошто су урадили 2 прве вежбе са Радног листа-B05, наставник објашњава да је реч о шифрирању посредством моно-алфабетске супституције код које се свако слово азбуке супституише другим словом. Напомиње да је Цезарево шифрирање поједностављена верзија моно-алфабетског шифрирања.

Научна напомена
Цезарево шифрирање је специјалан случај моно-алфабетског шифрирања. Ово можемо разумети на два начина:

- Међу свим могућим моно-алфабетским шифрирањима налази се и Цезарево шифрирање које добијамо циркуларном пермутацијом слова у реалној поруци, што представља подскуп свих могућих мешавина.
- Други начин разматрања проблема се своди на Цезарево шифрирање као специјалан сучај моно-алфабетског шифрирања чији кључ је реч од једног слова. На пример, Цезарево шифрирање ранга 3 је моно-алфабетско шифрирање чији кључ је « D » (« A » је померено за 3 места). Појам кључа ће бити детаљније разматран у завршном делу овог часа.

Појављује се више питања у вези вођења ученика, заједничког, током прорачуна могућег броја кључева у моно-алфабетском шифрирању.

- Питање 1: колико могућности имамо за шифрирање слова « A » ? Одговор: 26.
- Питање 2: кад смо једном одабрали слово које одговара слову « A » (на пример, « K »), колико могућности остаје за шифрирање слова « B » ? Одговор: 25 (јер је « K » већ узето).
- Питање 3: кад смо једном одабрали одговарајућа слова за A и за B, колико могућности преостаје за слово C ? Одговор: 24
- Питање 4: колико корспонденција можемо направити између слова која су у реалној поруци и слова која су стигла у криптованој поруци? Одговор: 26x25x24x23…x2x1.

Педгошка напомена:
У сучају потшкоћа с рзумевањем мултипликације у питању 4, покушајте с представљањем на други начин.

Наиме, наставник објашњава да се тај број може написати и као « 26 ! » а каже се « факторијел од 26 ». Ученици рачунају (помоћу калкулатора):

- 1 ! = 1
- 2 ! = 1 x 2 = 2
- 3 ! = 1 x 2 x 3 = 6
- 4 ! = 1 x 2 x 3 x 4 = 24
- 5 ! = 1 x 2 x 3 x 4 x 5 = 120
- 6 ! = 720
- 7 ! = 5 040
- 8 ! = 40 320
- 9 ! = 362 880
- 10 ! = 3 628 800
- …
- 26 ! ≈ $4x10^{26}$, c'est-à-dire 400 000 000 000 000 000 000 000 000

Број могућих кључева није виш 26 (као што је то био случај код Цезаревг шифрирања), него 400 милиона милијарди милијарди!

Вежба (појединачно)

Наставник даје ученицима вежбу 3 с Радног листа-B05 , који омогућује да се ради и са степеном за основу 10.

Корекција:

- Вежба 3а: ако ставимо 5 x $4x10^{26}$ секунди, или $1,5x10^{21}$ година (или 100 милијарди пута старост универзума) тестирајте све кључеве.
- Вежба 3б: ако сарађују сва људска бића, уложиће се 8 милијарди пута мање времена, или још увек 12 пута старости универзума.
- Вежба 3в: најмоћнијим суперкомпјутерима је потрбно $4x10^{11}$ секунди, или 300 000 година, да би тестирали све могуће кључеве.

Одељење, пошто се направи корекција вежби 3, утврђује да је неизмерно велики број могућих кључев за овај метод шифрирања па је за разбијање овог типа шифрирања потребно више векова (ако се одстране размаци између речи, јер у противном се морамо послужти кратким речима да би открили које слово је у питању). Al-Kindi је, у деветом веку, направио анализу фреквенције појаве неког слова и тиме омогућио разбијање шифре код овог метода шифрирања. Овај метод ће бити приказан на следећем часу.

Шифрирање помоћу кључне речи или кључне реченице (заједнички)

Пошаљилац и прималац поруке би требало да се договоре коју азбуку ће користити, а то би могло да буде компликовано:

- Насумично мешање азбука би захтевало да их добро познајете, а то је доста тешко а могуће је лако направити грешке;

- Решење се налази у давању табеле одговарајуће азбуке (табела кореспонденције на Радном листу-B05) није задивиљавајућа, јер је довољно да неко непожељан дође до тог папира и тиме открије кључ шифрирања поруке.

Могуће решење се налази у не коришћењу неке азбуке, него у кључној речи, или кључној реченици. Наставник објашњав овај метод на неком примеру. Ако је кључ « JULES CESAR », попунићемо шифрирани део азбуке овим кључним словима, занемарујући размаке између речи… и **игноришући већ употребљена слова**! (ово је неопходно ако желимо да свако слово буде супституисано једним јединим могућим словом).
« JULES CESAR » тада постаје « JULESCAR »

Етапа 1: попуњавамо табелу са словима кључне реченице «без размака ».

Alphabet реалан	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet шифриран	J	U	L	E	S	C	A	R																		

Етапа 2: комплетирамо азбуку померајући и полазећи од места где се завршава кључна реченица, и изостављајући већ коришћена слова.

Alphabet реалан	a	b	c	d	e	f	g	h	i	j	k	l	m	n	o	p	q	r	s	t	u	v	w	x	y	z
Alphabet шифриран	J	U	L	E	S	C	A	R	T	V	W	X	Y	Z	B	D	F	G	H	I	K	M	N	O	P	Q

На овај начин лако реконструишемо шифрирану азбуку, и преостаје нам само једна реч или реченица, што је моног лакше него да тражимо насумично могућности са 26 слова!
С кључном реченицом « JULES CESAR », текст « VENI VIDI VICI » постаје MSZT MTET MTLT.

Педагошка напомена
Горе описани метод је углавном адаптиран у криптографији па ћемо га зато и уптребити у наставку. Потребно је ипак нагласити да је овај метод нека врста конвенције па је могуће креирати и неки други начин алфабетског шифрирања. На пример, на крају кључне речи, боље него да наставимо азбуку како је горе објашњено, могли би да почнемо из почетка (словом A, изузев ако већ није било у уотреби...). Наглашавамо да у том случачју крај азбуке бива непромењен што омогућује читљивост дела шифрираног текста... па самим тим и криптоанализа постаје знатно лакша.

Тренирање (у паровима)

Сваки пар користи вежбу 4 Радног листа –B05 с циљем да се увежба шифрирње моно-алфабетском супституцијом. Потребно је да се прво нађе кључ шифрирања а затим и генерише алфабетско шифрирање, а на крају и да се шифрира кратка порука. Та порука се шаље суседу који би требало да је дешифрује (пажња, потребно је послати шифрирану поруку, али и кључ!)

> **Научна напомена:**
> Употреба шифрираних порука моно-алфабетском супституцијом је коришћена и пре Јулија Цезара. На пример, у Кама сутри (написаној у 5-том веку пре нове ере). Међу бројним умећима неке конкубине био је и број 45 (*mlecchita-vikalpà*) који се састојао у тајном комуницирању с вољеним!

Закључак

Одељење заједнички дефинише кључне концепте поменуте на почетку овог часа: моно-алфабетско шифрирање, кључ, алафабетско шифрирање.
