Универзитет „Св.Кирил и Методиј“ – Скопје
Факултет за информатички науки и компјутерско инженерство

Домашна работа 1 по предметот
КРИПТОГРАФИЈА

Напад со фреквенција на букви

Стефан Андонов (151020)
stefan.andonov@students.finki.ukim.mk

Октомври, 2017
Скопје

1. Вовед

Во ова домашна задача ќе бидат прикажани следните работи:
- начин на шифрирање на аргумент со помош на субституциски шифрувач преку програма изработена во програмскиот јазик Јава
- начин на дешифрирање со помош на напад со фреквенција на букви преку програма изработена во програмскиот јазик Јава

Тектот којшто го дешифрирам го добив од колешката Ивана Срњакова (151073).

Тектот којшто го шифрирав е дел од натпис од новинарски портал достапен на следниот линк. Со цел да можеме да шифрираме и дешифрираме полесно, од тектот се остранети сите празни места и специјални карактери.

2. Шифрирање на текст

Најпрво се дефинира пермутација p:A->A на македонската азбука, која што ќе се користи во шифрирањето на текстот.

```
P:{'А','Б','В','Г','Д','Ѓ','Е','Ж','З','S','И','Ј','К','Л','Љ','М','Н','Њ','О','П','Р','С','Т',
'Ќ','У','Ф','Х','Ц','Ч','Џ','Ш'}                                                              ->
{'Ш','Р','С','У','Ќ','Х','Џ','А','В','Д','Ѓ','Б','Г','И','Е','З','S','К','Ј','Ц','Ч','Ф','Л','Љ
','Ж','Н','Њ','М','Т','О','П'}
```

Текстот којшто се шифрира е следниот:

Премиерот Зоран Заев е убеден дека нема да има потреба од политичка интервенција за Грција да ги екстрадира тајните агенти Горан Грујевски и Никола Бошковски. Посочи дека единствен проблем со јужниот сосед е името, додека на останат план двете држави функционираат нормално и оти нема пречки да се спроведе меѓународното право.
„Македонија има склучено со Грција, вакви договори, впрочем и во минатото и на претходната власт Македонија немаше проблем во сите други аспекти, освен проблемот со името. Навистина имаме соработка со Грција имаме од секој можен аспект, министерствата за внатрешни работи соработуваат еве министерствата за правда верувам дека ќе покажат на дело соработка, поради тоа што тие се надлежни и искрено не очекувам потреба од никаква политичка интервенција, зошто се работи за две соседни земји коишто се пријатели.“ – изјави Зоран Заев, премиер
На Горан Грујевски и Никола Бошковски утре во Солун ќе им се суди за поседување лажни бугарски пасоши. Рочиштето е закажно во 12 часот. Засега останува енигма дали за делото кое се товарат евентуално ќе добијат затворска казна во Грција. Грчката полиција неразделните Грујевски и Бошковски ги уапси на аеродромот во Солун, од каде требало да отпатуваат до Будимпешта. Тандемот од УБК станал сомнителен поради лошиот квалитет на пасошите. Горан Грујевски се прекрстил во Христо Атанасов додека Никола Бошковски во Нецби Хасан. Министерот за внатрешни работи Оливер Спасовски објасни дека двоецот од тајната полиција имале логистика во Македонија додека биле во бегство. Но, со помош на службите од регионот тие биле лоцирани и уапсени, откако Интерпол распиша потерница по нив.

По остранување на празните места и специјалните текстот, како и конверзија на сите букви во големи букви, ја добиваме следната низа од знаци:

ПРЕМИЕРОТЗОРАНЗАЕВЕУБЕДЕНДЕКАНЕМАДАИМАПОТРЕБАОДПОЛИТИЧКАИНТЕРВЕНЦИЈАЗАГРЦИЈАДАГИЕКСТРАДИРАТАЈНИТЕАГЕНТИГОРАНГРУЈЕВСКИ
ИНИКОЛАБОШКОВСКИПОСОЧИДЕКАЕДИНСТВЕНПРОБЛЕМСОЈУЖНИОТСОСЕДЕИМЕТОДОДЕКАНАОСТАНАТПЛАНДВЕТЕДРЖАВИФУНКЦИОНИРААТНОРМА
ЛНОИОТИНЕМАПРЕЧКИДАСЕСПРОВЕДЕМЕЃУНАРОДНОТОПРАВОМАКЕДОНИЈАИМАСКЛУЧЕНОСОГРЦИЈАВАКВИДОГОВОРИВПРОЧЕМИВОМИНАТОТОИНА
ПРЕТХОДНАТАВЛАСТМАКЕДОНИЈАНЕМАШЕПРОБЛЕМВОСИТЕДРУГИАСПЕКТИОСВЕНПРОБЛЕМОТСОИМЕТОНАВИСТИНАИМАМЕСОРАБОТКАСОГРЦИЈАИМ
АМЕОДСЕКОЈМОЖЕНАСПЕКТМИНИСТЕРСТВАТАЗАВНАТРЕШНИРАБОТИСОРАБОТУВААТЕВЕМИНИСТЕРСТВАТАЗАПРАВДАВЕРУВАМДЕКАЌЕПОКАЖАТНАДЕ
ЛОСОРАБОТКАПОРАДИТОАШТОТИЕСЕНАДЛЕЖНИИИСКРЕНОНЕОЧЕКУВАМПОТРЕБАОДНИКАКВАПОЛИТИЧКАИНТЕРВЕНЦИЈАЗОШТОСЕРАБОТИЗАДВЕСОС
ЕДНИЗЕМЈИКОИШТОСЕПРИЈАТЕЛИИЗЈАВИЗОРАНЗАЕВНАГОРАНГРУЈЕВСКИИНИКОЛАБОШКОВСКИУТРЕВОСОЛУНЌЕИМСЕСУДИЗАПОСЕДУВАЊЕЛАЖНИБУГ

АРСКИПАСОШИРОЧИШТЕТОЕЗАКАЖНОВОДВАНАЕСЕТЧАСОТЗАСЕГАОСТАНУВАЕНИГМАДАЛИЗАДЕЛОТОКОЕСЕТОВАРАТЕВЕНТУАЛНОЌЕДОБИЈАТЗАТВОРС
КАКАЗНАВОГРЦИЈАГРЧКАТАПОЛИЦИЈАНЕРАЗДЕЛНИТЕГРУЈЕВСКИИБОШКОВСКИГИУАПСИНААЕРОДРОМОТВОСОЛУНОДКАДЕТРЕБАЛОДАОТПАТУВААТДОБ
УДИМПЕШТАТАНДЕМОТОДУБКСТАНАЛСОМНИТЕЛЕНПОРАДИЛОШИОТКВАЛИТЕТНАПАСОШИТЕГОРАНГРУЈЕВСКИСЕПРЕКРСТИЛВОХРИСТОАТАНАСОВДОД
ЕКАНИКОЛАБОШКОВСКИВОНЕЏБИХАСАНМИНИСТЕРОТЗАВНАТРЕШНИРАБОТИОЛИВЕРСПАСОВСКИОБЈАСНИДЕКАДВОЕЦОТОДТАЈНАТАПОЛИЦИЈАИМАЛЕ
ЛОГИСТИКАВОМАКЕДОНИЈАДОДЕКАБИЛЕВОБЕГСТВОНОСОПОМОШНАСЛУЖБИТЕОДРЕГИОНОТТИЕБИЛЕЛОЦИРАНИИУАПСЕНИОТКАКОИНТЕРПОЛРАСПИ
ШАПОТЕРНИЦАПОНИВ

Откако ќе се примени пермутацијата на азбуката шифрираниот текст изгледа вака:

ЦЧЏЗЃЏЧЈЛВЈЧШЅВШЏСЏЖРЏЌЏЅЌЏГШЅЏЗШЌШЃЗШЦЏЛЧЏРШЈЌЏЈИЃЛЃТГШЃЅЛЏЧСЏЅМЃБШВШУЧМЃБШЌШУЃЏГФЛЧШЌЃЧШЛШБЅЃЛЏШУЏЅЛЃУЈЧШЅУЧЖ
БЏСФГЃЃЅЃГЈИШРЈПГЈСФГЃЏЧФЈТЃЌЏГШЏЌЃЅФЛСЏЅЦЧЧЈРИЏЗФЈБЖАЅЃЈЛФЈФЏЌЏЃЗЏЛЈЌЈЌЏГШЅШЈФЛШЅШЛЦИШЅЌСЏЛЏЌЧАШСЃНЖЅГМЃЈЅЃЧШШЛЅЈЧЗШИЅ
ЈЃЈЛЃЅЏЗШЦЧЏТГЃЌШФЏФЦЧЈСЏЌЏЗЏХЖЖЅШЧЈЌЅЈЛЏЦЧШСЈЗШГЏЌЈЅЃБШЃЗШФГИЖТЏЅЈФЈУЧМЃБШСШГСЃЌУЈСЈЧЃСЦЧЈТЏЗЃСЈЅЅШЛЛЈЛЃЅШЦЧЏЛЊЈЌЅШЛШ
СИШФЛЗШГЏЌЈЅЃБШЅЏЗШПЏЦЧЈРИЏЗСЈФЃЛЏЌЧЖУЃШФЦЏГЛЃЈФСЏЅЦЧЈРИЏЗЈЛФЈЃЗЏЛЈЅШСЃФЛЃЅШЃЗШЗЦФЈЧШРЈЛГШФЈУЧМЃБШЃЗШЗЦЈЌФЏГЈБЗЈАЏЅШ
ФЦЏГЛЗЃЅЃФЛЏЧФЛСШЛШВШСЅШЛЧЏПЅЃЧШРЈЛЃФЈЧШРЈЛЖСШШЛЏСЏЗЃЅЃФЛЏЧФЛСШЛШВШЦЧШСЌШСЏЧЖСШЗЌГШЛЊЏЦГШАШЛЅШЌЏИЈФЈЧШРЈЛГ
ШЦЧШЌЃЛШПЛЛЛЃЏФЏЅШЌИЏАЅЃЃЃФГЧЏЅЈЏТЏГЖСШЗЦЛЧЏРШЈЌЅЃГШСШЦИЃЛЃТГШЃЅЛЏЧСЏЅМЃБШВЈПЛЈФЏЧШРЈЛЃВШЌСЏФЈФЏЌЅЃВЏЗБЃГЈГЈПЛЈФ
ЏЦЧЃБШЛЦИЃЃВБШСЃВЈЧШЅВШЏСЅШУЈЧШЅУЧЖБЏСФГЃЃЅЃГЈИШРЈПГЈСФГЃЖЛЧЏСЈФЈИЖЅЛЊЏЃЗФЏФЖЖЌЃВШЦЏФЏЌЖСШКЏИШАЅЃРЖУШЧФГЃЏШФЈПЃЧТЃ
ПЛЏЛЏЏВШГШАЅЈСЈЌСШЅШЏФЏЛТШФЈЛВШФЏУШЈФЛШЅЖСШЏЅЃУЗШЌШИЃВШЌЏИЈЛЃГЏЏФЏЛЈСШЧШЛЏСЏЅЛЖШИЅЈЛЊЌЈРЃБШЛВШЛСЈЧФГШГШВЅШСЈУ
ЧМЃБШУЧТГШЛШЏИЃМЃБШЅЏЧШВЌЏИЅЃЛЏУЧЖБЏСФГЃЃРЈПГЈСФГЃУЃЖШЦФЃЅШШЏЧЈЌЧЈЗЛСЈФЈИЖЅЈЌГШЌЏЛЧЏРШИЈЌШЛЛЏШЛЖСШШЛЌЈРЖЌЃЗЏЏПЛ
ШЛШЅЌЏЗЛЛЌЖРГФЛШЅШИФЈЗЅЃЛЏИЏЅЏЧШЌЃИЈПЃЛГСШИЃЛЛЛЅШЏШФЈПЃЛЏУЧШЅУЧЖБЏСФГЃФЏЏЧЏГЧФЛЃИСЈЊЧЃФЛЈШЛЛЅШФЈСЌЈЌЏГШЅЃГЈИШР
ЈПГЈСФГЃСЈЅЏОРЃЊШФШЅЗЃЅЃФЛЏЧЛВШСЅШЛЧЏПЅЃЧШРЈЛЃЈИЃСЏЧФЏШФЈСФГЃЈРБШФЅЃЌЏГШЌСЏЏМЈЛЈЌЛШБЅШЛШЏИЃМЃБШЃЗШИЏИЈУЃФЛЃГШСЈЗШ
ГЏЌЈЅЃБШЌЈЌЏГШРЃИЏСЈРЏУФЛСЈЅЈФЏЗЈПЅШФИЖАРЃЛЏЈЌЧЏУЃЈЅЈЛЛЃЏРЃИЏИЈМЃЧШЅЃЃЖШЦФЏЅЃЛГШГЈЃЅЛЏЧЏИЧШФЦЃПШЏЛЏЧЅЃМШЏЅЃС

Кодот којшто го направив и користев за шифрирање во програмскиот јазик Java е достапен на Github.

2. Програма за броење на фреквенција на буквите и паровите букви

Се со цел да го изведеме нападот со фреквенција на букви мораме да ја пресметаме фреквенцијата на буквите и на паровите букви. Откако ќе го имаме тоа можеме да почниме да дешифрираме врз основа на фреквенцијата на буквите.

Кодот којшто го креирав е достапен на Github.

Објаснување на начинот како функционира кодот:
Се чуваат како податочни структури 2 типа на хеш мапи, едни кои ќе помогнат во броење на букви и се од тип <Character,Double> и други кои ќе помогнат во броење на паровите на букви во текстот и се од тип <String, Double>. Double користиме бидејќи подоцна ќе ни биде потребно да се пресмета фреквенцијата на буквите. Потоа со итерации низ текстот буква по буква и пар по пар и со манипулација со хеш мапите, се брои колку пати ни се јавува одреден карактер или одреден пар. Потоа тие броеви се делат со вкупниот број на карактери, односно вкупниот број на парови (карактери-1) со цел да ја добиеме фреквенцијата во децимален број.
Со помош на стимовите во Јава 8, ги сортираме хеш мапите по нивните вредности (фреквенцијата на буквите/паровите), со цел полесно да можеме да ги анализираме.
На крај, резултатите ги печатиме во .csv датотеки.

3. Дешифрирање на пораката

Пораката која што ја добив од колешката е следната:

БДГЦАДЖДФЦМЅАЦОФБЅХЅЗБИЊДЕДХЅЖДГБДТЅБЅЖАИЅНЬЅЖХИЊДЖКЅЌЦТЅНЬБЅХЅАНИЖБДЗЅАЕЅЖЖЦДЖУЦМФНЬГЦУЅНЬЖЦБИМНИФМИТЦПЦУДАЦФ
ИГЅТДАЦЈИГДЈБДНЬГДЕЈЕНЬЅДТБЦБИДТДНЬОФАИЅНЬЅЖЖЦДГЖДФБЗЦБДФИЏЦЈИЖИАИГЏАДЖДЅЖЅФИЖИАИЏДТЦАЅЧАДЖДЦНТИАЦЅАИГДЅОХЅНЬЖБОБ

ИИЖАИТЊSТОФЊЖДЖЦАЦФМИТЦДТТБИАИSЊЅЖТЗЃИБЦАИБДНЗИЊДЕДФЅЉОТSЊЅЖЦДЊОФАИSЊЅЖЏДТЏАЦЏОАЦДЗЦГИТЅЖЦЦЊМЦХАДГДЦЕДДЏ
MSTИАЦЖSЕЅЖАИSЊЅЖЦЏЗИАЦУЦМФДБЦДТДУЦЛЦЈИМАИЖИГДАГОЗSАЛЦЈИГИГДЦАИФАДЏОТЗОЏЦГЗИЖГЦЦТДГОФSАЖИЗАЦУЦМФДБЦХMSАДБЦЖS
АИЃЦЗЦЖДЏЦДТЌЗИИАИЈТДЌЗЦЖSБДЊSГДЈИГИЖSЏДЗЦЈИБSЏЅЗБИКSЌЦТИЖДЌЈИБSАЦЦГЦРИЖИАИАИЈТДЌЗЦЖSБДЊSГДЈИДТЕЗSТБЦТSАЦЖSГИЖSЏДЗ
ЦЦИКSЌЦТИЖЊДДЕЧЖSАЦЦЦГЦРИЖИАИАИЈТДЌЗЦЖSОХSЊАЦЛЦГДЦКSЏДЕЗSЖЊЖИБОБИИЖПЦУДАЦФИГSТДАЦЈИАИУSЊЖЦБИМДЖПЦУДАЦЅГЊЕЦЗ
ЦSАЊБДЦЖИМЦЈИЕSЖЖДЖДЦНТИАЦЕАИПЦУДАЦФИГSТДАЦЈИБГМОХОБИЧЅЦSТЦАИSЊЅЖЗИЌДЖЦМАЦЛЦНИУЦМФЖSИЖИЗГОНЦГИЖИАЛЦЕДБSКSЕЗ
ЦТЗОЃАЦИГЖЦБАДЊЖЦГДАЛЅЗЖЦЦТЗОЏДИЊЅДТБЦБИЧЅБДГЦАДЖSГИАИФИГSТДАЦЈИЦБДФМИТЦАЊГЦДЖГОМЖОЗSАЛSАЖИЗАИЊБSХSАДЖАНИЖБД
ЗИРSКSЌЦТИЖЕЗSЖЊЖИБSАЦТSМИЖИГДЦЏЦЊДНТИТДИАИЈФМИТЦЖSОХSЊАЦЛЦАИЗИЌДЖЦМАЦЛЏЖSТSМДТЊДНТИТSАЦЖSТSМИДТАИЈФМИТЦЖSО
ХSЊАЦЛЦКSЊЅЕ3ДТИБИИЖЕДЊЦФЌДМЦХАИЛSАИИЊДЌЗИАЦЖSЊЗ3STЊЖБИКSЊЅЕ3STИТИЖАИТДФДЖНИТSЛИЌSНЗДТЦЖSМЦSТЦАИSЊЅЖЖЦДГЖДФБ
ЗЦ

Пред да започнам со дешифрирање ќе дадам дефиниција на операција која што подоцна ќе биде извршувана во рамките на пермутацијата на азбуката, со цел да се стигне до точната пермутација:

def: Нека X, Y, Z се три карактери од македонската азбука и за нив важи дека $p(X) = Y$, односно X се пресликува во Y во пермутацијата на збуката p.
Тогаш, доколку се открие дека буквата Y треба да се пресликува во буквата Z, $p(x)$ ја добива вредноста Y $(p(X) = Y)$. Ќе запишуваме:

$$X \to Y + Y \to Z = X \to Z$$

Откако пораката помина низ програмата за пресметка на фреквенција, правиме споредба со фреквенциите кои што ни се познати:

од шифриран текст			познати	
буква	фрек	%	буква	%
Ц	0,11688	11,688	А	12,28
И	0,11596	11,596	О	10,98
S	0,1039	10,39	И	9,93
Д	0,09555	9,555	Е	9,52
Ж	0,07978	7,978	Т	7,27
А	0,07514	7,514	Н	7,00
Т	0,05473	5,473	Р	5,52
Њ	0,04174	4,174	С	4,98
Б	0,04174	4,174	К	4,13
Г	0,03711	3,711	В	3,68
З	0,03618	3,618	Д	3,56
Ф	0,02505	2,505	П	3,19
М	0,02412	2,412	М	2,94
О	0,02134	2,134	Л	2,59
Ј	0,01855	1,855	У	2,08
Е	0,01763	1,763	Ј	1,61
Џ	0,01577	1,577	З	1,60
Ќ	0,01299	1,299	Г	1,31
Х	0,01206	1,206	Б	1,23
Л	0,01113	1,113	Ч	1,03
Н	0,01113	1,113	Ц	0,89
У	0,0102	1,02	Ш	0,72
К	0,00742	0,742	Ж	0,57
П	0,00371	0,371	Ф	0,43
Ч	0,00371	0,371	Њ	0,33
Ѓ	0,00278	0,278	Ќ	0,33
Р	0,00278	0,278	Х	0,24
Љ	0,00093	0,093	Ѓ	0,05
В	0	0	S	0,01
С	0	0	Љ	0,00
Ш	0	0	Џ	0,00

Можеме да забележиме дека фрекфенциите на буквите Ц и И се највисоки, скоро 12%, па тие се сигурно некоја од самогласките А, О или И.

Најпрво со помош на програмата Decypher.java ќе пробаме да видиме каков текст ќе добиеме доколку во текстот ги замениме буквите според овој клуч (Ц = А, И = О, S = И, ...) и дали можеме нешто да воочиме таму.

Текстот којшто го добивме е следниот:
КЕВАНЕ**ТЕПАМ**ИНАЛПКИБИДКОСЕЈЕБИТЕВКЕРИК**ИТНО**И
СИТБОСЕТЖИГАРИСКИБИНЦОТКЕДИНЈИТТАЕТШАМПСВА
ШИСТАКОМЦОПМОРАФАШЕНАПОВИРЕНАУОВЕУКЕСВЕЈУ

ЈСИЕРКАКОЕРЕСЛПНОИСИТТАЕВТЕПКДАКЕПОЗАУОТОНО
ВЗНЕТЕИТИПОТОНОЗЕРАНИЊНЕТЕАЦРОНАИНОВЕИЛБИС
ТКЛКООТНОРСИРЛПСТЕТАНАПМОРАЕРРКОНОИСИТРДЌО
КАНОКЕЦДОСЕЈЕПИЃЛРИСИТАЕСЛПНОИСИТЗЕРЗНАУЛНА
ЕДАВОРИТААСМАБНЕВЕАЈЕЕЗМИРОНАТИЈИТНОИСИТАЗ
ДОНАШАМПЕКАЕРЕШАЧАУОМНОТОВЕНВЛДИНЧАУОВОВ
ЕАНОПНЕЗЛРДЛЗАВДОТВААРЕВЛПИНТОДНАШАМПЕКАБ
МИНЕКАТИНОЌАДАТЕЗАЕРГДООНОУРЕГДАТИКЕСИВЕУО
ВОТИЗЕДАУОКИЗИДКОЖИГАРОТЕГУОКИНААВАХОТОНОН
ОУРЕГДАТИКЕСИВЕУОЕРЈДИРКАРИНАТИВОТИЗЕДААОЖИ
ГАРОТСЕЕЈЊТИНАААВАХОТОНОНОУРЕГДАТИЛБИСНАЧАВ
ЕАЖИЗЕЈДИТСТОКЛКООТФАШЕНАПОВИРЕНАУОНОШИСТ
АКОМЕТФАШЕНАИВСЈАДАИНСКЕАТОМАУОЈИТТЕТЕАЦРО
НАЈНОФАШЕНАПОВИРЕНАУОКВМЛБЛКОЊИАИРАНОИСИ
ТДОГЕТАМНАЧАЦОШАМПТИОТОДВЛЦАВОТОНЧАЈЕКИЖ
ИЈДАРДЛЌНАОВТАКНЕСТАВЕНЧИДТААРДЛЗЕОСИЕРКАКО
ЊИКЕВАНЕТИВОНОПОВИРЕНАУОАКЕПМОРАНСВАЕТВЛМ
ТЛДИНЧИНТОДНОСКИБИНЕТНЦОТКЕДОХИЖИГАРОТЈДИ
ТСТОКИНАРИМОТОВЕАЗАСЕЦРОРЕОНОУПМОРАТИЛБИС
НАЧАНОДОГЕТАМНАЧЗТИРИМЕРСЕЦРОРИНАТИРИМОЕР
НОУПМОРАТИЛБИСНАЧАЖИСИЈДЕРОКООТЈЕСАПГЕМАБ
НОЧИНООСЕГДОНАТИСДИРСТКОЖИСИЈДИРОРОТНОРЕП
ЕТЦОРИЧОГИЦДЕРАТИМАИРАНОИСИТТАЕВТЕПКДА

Табелата за фреквенција на парови на букви е во прилог на ова домашна задача, но истата не ја искористив поради огромни разлики на проценти. Конретно парот АА се јавува најчесто со 12%, но во текстот којшто го добив од колешката пар којшто најчесто се појавува е со две различни букви и со фреквенција од 2%.

Очигледно е дека не можеме да добиеме точен резултат со ова смена па затоа ќе направиме неколку прилагодувања во замената кај буквите што имаат слични фреквенции меѓу буквите за кои што се сомневаме дека се самогласки:

- Ц = О и И = А

КЕВИНЕТЕПИМИНИЛПКИБИДКАСЕЈЕБИТЕВКЕРИКИТНАИСИТБАСЕТЖИГИРИСКИБИНЦАТКЕДИНЈИТТИЕТШИМПСВИШИСТИК
АМЦАПМАРИФИШЕНИПАВИРЕНИУАВЕУКЕСВЕЈУЈСИЕРКИКАЕРЕСЛПНАИСИТТИЕВТЕПКДИКЕПАЗИУАТАНАВЗНЕТЕИТИПАТАН
АЗЕРИНИЊНЕТЕИЦРАНИИНАВЕИЛБИСТКЛКААТНАРСИРЛПСТЕТИНИПМАРИЕРРКАНАИСИТРДЌАКИНАКЕЦДАСЕЈЕПИЃЛРИСИ
ТИЕСЛПНАИСИТЗЕРЗНИУЛНИЕДИВАРИТИИСМИБНЕВЕИЈЕЕЗМИРАНИТИЈИТНАИСИТИЗДАНИШИМПЕКИЕРЕШИЧИУАМНАТА
ВЕНВЛДИНЧИУАВАВЕИНАПНЕЗЛРДЛЗИВДАТВИИРЕВЛПИНТАДНИШИМПЕКИБМИНЕКИТИНАЌИДИТЕЗИЕРГДААНАУРЕГДИТ
ИКЕСИВЕУАВАТИЗЕДИУАКИЗИДКАЖИГИРАТЕГУАКИНИИВИХАТАНАНАУРЕГДИТИКЕСИВЕУАЕРЈДИРКИРИНИТИВАТИЗЕДИИА
ЖИГИРАТСЕЕЈЊТИНИИИВИХАТАНАНАУРЕГДИТИЛБИСНИЧИВЕИЖИЗЕЈДИТСТАКЛКААТФИШЕНИПАВИРЕНИУАНАШИСТИКА
МЕТФИШЕНИИВСЈИДИИНСКЕИТАМИУАЈИТТЕТЕИЦРАНИЈНАФИШЕНИПАВИРЕНИУАКВМЛБЛКАЊИИИРИНАИСИТДАГЕТИМН
ИЧИЦАШИМПТИАТАДВЛЦИВАТАНЧИЈЕКИЖИЈДИРДЛЌНИАВТИКНЕСТИВЕНЧИДТИИРДЛЗЕАСИЕРКИКАЊИКЕВИНЕТИВАНАП
АВИРЕНИУАИКЕПМАРИНСВИЕТВЛМТЛДИНЧИНТАДНАСКИБИНЕТНЦАТКЕДАХИЖИГИРАТЈДИТСТАКИНИРИМАТАВЕИЗИСЕЦР
АРЕАНАУПМАРИТИЛБИСНИЧИНАДАГЕТИМНИЧЗТИРИМЕРСЕЦРАРИНИТИРИМАЕРНАУПМАРИТИЛБИСНИЧИЖИСИЈДЕРАКАА
ТЈЕСИПГЕМИБНАЧИНААСЕГДАНИТИСДИРСТКАЖИСИЈДИРАРАТНАРЕПЕТЦАРИЧАГИЦДЕРИТИМИИРИНАИСИТТИЕВТЕПКДИ

И во овој случај не можеме да забележиме зборови од македонскиот јазик. Ќе пробаме нова пермутација на самогласките:
Ц = И, S=Е, Д = О, И = А,

КО**ВИНОТО**ПИМЕНИЛПКЕБЕДКАСОЈОБЕТОВКОРЕКЕ**ТНАЕСЕТ**БАСОТЖЕГИРЕСКЕБЕНЦАТКОДЕНЈЕТТИОТШИМПСВИШЕСТИКА
МЦАПМАРИФИШОНИПАВЕРОНИУАВОУКОСВОЈУЈСЕОРКИКАОРОСЛПНАЕСЕТТИОВТОПКДИКОПАЗИУАТАНАВЗНОТОЕТЕПАТА
НАЗОРИНЕЊНОТОИЦРАНИЕНАВОЕЛБЕСТКЛКААТНАРСЕРЛПСТОТИНИПМАРИОРРКАНАЕСЕТРДЌАКИНАКОЦДАСОЈОПЕЃЛРЕС
ЕТИОСЛПНАЕСЕТЗОРЗНИУЛНИОДИВАРЕТИИСМИБНОВОИЈООЗМЕРАНИТЕЈЕТНАЕСЕТИЗДАНИШИМПОКИОРОШИЧИУАМНА
ТАВОНВЛДЕНЧИУАВАВОИНАПНОЗЛРДЛЗИВДАТВИИРОВЛПЕНТАДНИШИМПОКИБМЕНОКИТЕНАЌИДИТОЗИОРГДААНАУРОГ
ДИТЕКОСЕВОУАВАТЕЗОДИУАКЕЗЕДКАЖЕГИРАТОГУАКЕН….

Во почетокот на текстот се јавува изразот КОВИНОТО, а понатаму се јавува изразот РЕКЕТНАЕСЕТ(БАСОТ). Доколку направиме рокада на буквите В и К, ќе ги добиеме изразите

ВОКИНОТО (Во киното) и РЕВЕТНАЕСЕТ(БАСОТ). Доколку претпоставиме дека „реветнаесет“ се однесува на некоја бројка имаме можност да станува збор за бројот деветнаесет, а пак зборот во заградите после него наместо „басот“ да биде „Часот“.

Ова значи дека треба да направиме промена во нашата последна пермутација. Самогласките кои што ги дефиниравме остануваат исти, а промената е следната:

$$Б \to К \ + \ \ К \to В = Б \to В$$
$$Г \to В + В \to К = Г \ \to К$$
$$Т \to Р + Р \to Д = Т \to Д$$
$$Х \to Б + Б \to Ч = Х \to Ч$$

Со првите две промени, само правиме замена на р(Б) и р(Г) со соодветните вредности, но со вторите две промени, доведуваме до случај р(Т)=р(З) = Д, како и р(Х)=р(Л)=Ч. Со цел ова да се реши примарно ќе поставиме р(З) = Р и р(Л)=Б. Ова е само претпоставка, не мора да биде точно.

Го дешифрираме текстот уште еднаш со промените во нашата примарна пермутација и го добиваме следниот текст:

ВО КИНОТО ПИМЕНИЛП ВЕЧЕРВА СО **ЈОЧЕТОК** ВО ДЕВЕТНАЕСЕТ ЧАСОТ ЖЕ ГИДЕ СВЕЧЕН **ЦАТВОРЕН ЈЕТТИОТ** ШИМПСКИШЕСТИВАМЦАПМАДИФ....

Наместо на буквата Ј треба да стои буквата П и ќе ги добиеме зборовите „почеток“ и „петтиот“. Фразата „ЖЕ ГИДЕ“ според типот на текстот (извештај, новинарска статија), јасно е дека треба да биде „ЌЕ БИДЕ“, па затоа буквата Ж ќе ја замениме со Ќ и буквата Г ќе ја замениме со Б. Дополнително, зборот „ЦАТВОРЕН“ треба да биде ЗАТВОРЕН, па затоа буквата Ц ќе ја замениме со З. Сите овие трансформации на пермутацијата на азбуката ќе изгледаат овака:

$$Е \to Ј + Ј \to П = Е \to П$$
$$К \to Ж + Ж \to Ќ = К \to Ќ$$
$$Ќ \to Г + Г \to Б = Ќ \to Б$$
$$Н \to Ц + Ц \to З = Н \to З$$

Исто како и претходно, имаме случај кога во пермутацијата две различни букви се пресликуваат во една. Буквите Е и Ф се пресликуваат во П. Ова ќе го решиме со тоа што Ф ќе се пресликува во Ј. Буквите К и Ѓ се пресликуваат во Ќ. Ова ќе го решиме со тоа што Ѓ ќе се пресликува во Ж. Буквите Ќ и Л се пресликуваат во Б. Ова ќе се реши со тоа што Л ќе се пресликува во Г. Буквите Н и Џ се пресликуваат во З. Ова ќе се реши со тоа што Џ ќе се пресликува во Ц. Како и претходно, ова е претпоставка со цел да немаме две букви кои што ќе се пресликуваат во една иста буква.

Со новодобиената пермутација на азбуката ќе го дешифрираме текстот уште еднаш и го добиваме следниот резултат:
ВО КИНОТО **ЈИМЕНИЛЈ** ВЕЧЕРВА СО ПОЧЕТОК ВО ДЕВЕТНАЕСЕТ ЧАСОТ ЌЕ БИДЕ СВЕЧЕН ЗАТВОРЕН ПЕТТИОТ ШИМЈСКИШЕСТИВАМЗАЈМАДИФИШОНИЈАКЕДОНИУАКОУ ВО **СКОПУЕ** СЕ ОДВИВА ОД **ОСЛЈНАЕСЕТТИ ОКТОЈВРИ** ВОЈАЦИУАТАНАКЦНОТОЕТЕЈАТАНАЦОДИНЕЊНОТО ИЗДАНИЕ НА КОЕ **ЛЧЕСТВЛВААТ** НАД **СЕДЛЈСТОТИНИ ЈМАДИ** ОД

ДВАНАЕСЕТ ДРЖАВИ НА ВОЗРАСО **ПОЈЕЌЛ** ДЕСЕТ И **ОСЛЈНАЕСЕТ** ЦОДЦНИ УЛНИОРИКАДЕТИИСМИЧНОКОИПООЦМЕДАНИТЕ ПЕТНАЕСЕТ ИЦРАНИШИМЈОВИОДОШИГИУАМНАТАКОНКЛРЕНГИУАКАКОИНАЈНОЦЛДРЛЦИКРАТКИИДОКЛЈЕНТАРНИШИМЈОВИЧМЕНО ВИТЕНАЖИРИТОЦИОДБРААНАУДОБРИТЕВОСЕКОУАКАТЕЦОРИУАВЕЦЕРВАЌЕБИДАТОБУАВЕНИИКИХАТАНАНАУДОБРИТЕВО СЕКОУАОДПРЕДВИДЕНИТЕКАТЕЦОРИИАЌЕБИДАТСООПЊТЕНИИИКИХАТАНАНАУДОБРИТЕЛЧЕСНИГИКОИЌЕЦОПРЕТСТАВЛВ ААТФИШОНИЈАКЕДОНИУАНАШЕСТИВАМОТФИШОНИЕКСПИРИЕНСВОИТАМИУАПЕТТОТОИЗДАНИПНАФИШОНИЈАКЕДОНИ УАВКМЛЧЛВАЊЕИЕДИНАЕСЕТРАБОТИМНИГИЗАШИМЈТЕАТАРКЛЗИКАТАНГИПОВЕЌЕПРИДРЛЖНИАКТИВНОСТИКОНГЕРТИИ ДРЛЦОАСЕОДВИВАЊЕВОКИНОТЕКАНАЈАКЕДОНИУАИВОЈМАДИНСКИОТКЛМТЛРЕНГЕНТАРНАСВЕЧЕНОТНЗАТВОРАХЕЌЕБИД АТПРЕТСТАВЕНИДЕМАТАКОИЦИСОЗДАДОАНАУЈМАДИТЕЛЧЕСНИГИНАРАБОТИМНИГЦТЕДЕМОДСОЗДАДЕНИТЕДЕМАОДНА УЈМАДИТЕЛЧЕСНИГИЌЕСЕПРОДАВААТПОСИЈБОМИЧНАГЕНАА СОБРАНИТЕ СРЕДСТВА ЌЕ СЕ ПРЕДАДАТ НА **ДОЈОТ** ЗА **ДЕГА** БЕЗ **РОДИТЕМИ** ЕДИНАЕСЕТТИ **ОКТОЈВРИ**

ЈИМЕНИЛЈ	МИЛЕНИУМ
СКОПУЕ	СКОПЈЕ
ОСЛЈНАЕСЕТТИ	ОСУМНАЕСЕТТИ
ОКТОЈВРИ	ОКТОМВРИ
ЛЧЕСТВЛААТ	УЧЕСТВУВААТ
СЕДЛЈСТОТИНИ	СЕДУМСТОТИНИ
ЈМАДИ	МЛАДИ
ДОЈОТ	ДОМОТ
ДЕГА	ДЕЦА
РОДИТЕМИ	РОДИТЕЛИ

Со цел, зборовите од левата страна на претходната табела да може да станат зборовите од десната страна на табелата потребно е да бидат направени следните трансформации во пермутацијата на азбуката:

$$Ф \to Ј + Ј \to М = Ф \to М$$
$$М \to М + М \to Л = М \to Л$$
$$О \to Л + Л \to У = О \to У$$
$$Ј \to У + У \to Ј = Ј \to Ј$$
$$Л \to Г + Г \to Ц = Л \to Ц$$

Како и претходно, се со цел да немаме две букви да покажуваат на една иста буква потребно ќе е да ја измениме рачно пермутацијата. Буквите Л и Џ покажуваат на Ц, но ова ќе се реши со тоа што Џ ќе покажува на Г.

Текстот го дешифираме уште еднаш со новата смена во пермутацијата и го добиваме следниот резултат:

ВО КИНОТО МИЛЕНИУМ ВЕЧЕРВА СО ПОЧЕТОК ВО ДЕВЕТНАЕСЕТ ЧАСОТ ЌЕ БИДЕ СВЕЧЕН ЗАТВОРЕН ПЕТТИОТ **ШИЛМСКИ ШЕСТИВАЛ** ЗА МЛАДИ **ФИШОНИ** МАКЕДОНИЈА КОЈ ВО СКОПЈЕ СЕ ОДВИВА ОД ОСУМНАЕСЕТТИ ОКТОМВРИ ВО МАГИЈАТА НА КИНОТО Е ТЕМАТА НА **ГОДИНЕЊНОТО** ИЗДАНИЕ НА КОЕ УЧЕСТВУВААТ НАД СЕДУМСТОТИНИ МЛАДИ ОД ДВАНАЕСЕТ ДРЖАВИ НА ВОЗРАСТ ПОМЕЃУ ДЕСЕТ И ОСУМНАЕСЕТ ГОДИНИ ЈУНИОРИ КАДЕТИ И СЛИЧНО КОИ ПОО ГЛЕДАНИТЕ ПЕТНАЕСЕТ ИГРАНИ **ШИЛМОВИ** ОД **ОШИЦИЈАЛНАТА** КОНКУРЕНЦИЈА КАКО И НА МНОГУ ДРУГИ КРАТКИ И ДОКУМЕНТАРНИ **ШИЛМОВИ** ЧЛЕНОВИТЕ НА ЖИРИТО ГИ ОДБРАА НАЈДОБРИТЕ ВО СЕКОЈА КАТЕГОРИЈА ВЕЧЕРВА ЌЕ БИДАТ ОБЈАВЕНИ ИМИХАТА НА НАЈДОБРИТЕ ВО СЕКОЈА ОД ПРЕДВИДЕНИТЕ КАТЕГОРИИ А ЌЕ БИДАТ СООПЊТЕНИ И ИМИХАТА НА НАЈДОБРИТЕ УЧЕСНИЦИ КОИ ЌЕ ГО ПРЕТСТАВУВААТ **ФИШОНИ** МАКЕДОНИЈА НА **ШЕСТИВАЛОТ** ФИШОНИ ЕКСПИРИЕНС

ВО ИТАЛИЈА ПЕТТОТО ИЗДАНИЕ НА ФИШОНИ МАКЕДОНИЈА **ВКЛУЧУВАЊЕ** И ЕДИНАЕСЕТ РАБОТИЛНИЦИ ЗА **ШИЛМ** ТЕАТАР МУЗИКА ТАНЦ И ПОВЕЌЕ ПРИДРУЖНИ АКТИВНОСТИ КОНЦЕРТИ И ДРУГО А СЕ **ОДВИВАЊЕ** ВО КИНОТЕКА НА МАКЕДОНИЈА И ВО МЛАДИНСКИОТ КУЛТУРЕН ЦЕНТАР НА СВЕЧЕНОТН **ЗАТВОРАХЕ** ЌЕ БИДАТ ПРЕТСТАВЕНИ ДЕЛАТА КОИ ГИ СОЗДАДОА НАЈМЛАДИТЕ УЧЕСНИЦИ НА РАБОТИЛНИЦИТЕ ДЕЛ ОД СОЗДАДЕНИТЕ ДЕЛА ОД НАЈМЛАДИТЕ УЧЕСНИЦИ ЌЕ СЕ ПРОДАВААТ ПО СИМБОЛИЧНА ЦЕНА А СОБРАНИТЕ СРЕДСТВА ЌЕ СЕ ПРЕДАДАТ НА ДОМОТ ЗА ДЕЦА БЕЗ РОДИТЕЛИ ЕДИНАЕСЕТТИ ОКТОМВРИ

Се појасно е дека сме на самиот крај на дешифрирањето, односно ни останаа уште многу малку зборови кои што се неточни:

ШИЛМСКИ	ФИЛМСКИ
ФИШОНИ	ЏИФОНИ
ГОДИНЕЊНОТО	ГОДИНЕШНОТО
ОШИЦИЈАЛНАТА	ОФИЦИЈАЛНАТА
ВКЛУЧУВАЊЕ	ВКЛУЧУВАЊЕ
ЗАТВОРАХЕ, ИМИХАТА	ЗАТВОРАЊЕ. ИМИЊАТА

За овие зборови да бидат точни потребно е да ги направиме следните промени во пермутацијата:

$$У \to Ш + Ш \to Ф = У \to Ф$$
$$Ч \to Њ + Њ \to Ш = Ч \to Ш$$
$$П \to Ф + Ф \to Џ = П \to Џ$$
$$Р \to Х + Х \to Њ = Р \to Њ$$

Во овој случај, буквите П и Ш покажуваат на буквата Џ, но тоа ќе го решиме со тоа што ќе ставиме буквата Ш да покажува на буквата Х, бидејќи само таа буква ја немаше во пермутацијата.

Конечно, текстот којшто го добив е дешифриран и изгледа овака:

ВО КИНОТО МИЛЕНИУМ ВЕЧЕРВА СО ПОЧЕТОК ВО ДЕВЕТНАЕСЕТ ЧАСОТ ЌЕ БИДЕ СВЕЧЕН ЗАТВОРЕН ПЕТТИОТ ФИЛМСКИ ФЕСТИВАЛ ЗА МЛАДИ ЏИФОНИ МАКЕДОНИЈА КОЈ ВО СКОПЈЕ СЕ ОДВИВА ОД ОСУМНАЕСЕТТИ ОКТОМВРИ ВО МАГИЈАТА НА КИНОТО Е ТЕМАТА НА ГОДИНЕШНОТО ИЗДАНИЕ НА КОЕ УЧЕСТВУВААТ НАД СЕДУМСТОТИНИ МЛАДИ ОД ДВАНАЕСЕТ ДРЖАВИ НА ВОЗРАСТ ПОМЕЃУ ДЕСЕТ И ОСУМНАЕСЕТ ГОДИНИ ЈУНИОРИ КАДЕТИ И СЛИЧНО КОИ ПОО ГЛЕДАНИТЕ ПЕТНАЕСЕТ ИГРАНИ ШИЛМОВИ ОД ОФИЦИЈАЛНАТА КОНКУРЕНЦИЈА КАКО И НА МНОГУ ДРУГИ КРАТКИ И ДОКУМЕНТАРНИ ШИЛМОВИ ЧЛЕНОВИТЕ НА ЖИРИТО ГИ ОДБРАА НАЈДОБРИТЕ ВО СЕКОЈА КАТЕГОРИЈА ВЕЧЕРВА ЌЕ БИДАТ ОБЈАВЕНИ ИМИХАТА НА НАЈДОБРИТЕ ВО СЕКОЈА ОД ПРЕДВИДЕНИТЕ КАТЕГОРИИ А ЌЕ БИДАТ СООПЊТЕНИ И ИМИХАТА НА НАЈДОБРИТЕ УЧЕСНИЦИ КОИ ЌЕ ГО ПРЕТСТАВУВААТ ЏИФОНИ МАКЕДОНИЈА НА ФЕСТИВАЛОТ ЏИФОНИ ЕКСПИРИЕНС ВО ИТАЛИЈА ПЕТТОТО ИЗДАНИЕ НА ЏИФОНИ МАКЕДОНИЈА ВКЛУЧУВАШЕ И ЕДИНАЕСЕТ РАБОТИЛНИЦИ ЗА ФИЛМ ТЕАТАР МУЗИКА ТАНЦ И ПОВЕЌЕ ПРИДРУЖНИ АКТИВНОСТИ КОНЦЕРТИ И ДРУГО А СЕ ОДВИВАШЕ ВО КИНОТЕКА НА МАКЕДОНИЈА И ВО МЛАДИНСКИОТ КУЛТУРЕН ЦЕНТАР НА СВЕЧЕНОТО ЗАТВОРАЊЕ ЌЕ БИДАТ ПРЕТСТАВЕНИ ДЕЛАТА КОИ ГИ СОЗДАДОА НАЈМЛАДИТЕ УЧЕСНИЦИ НА РАБОТИЛНИЦИТЕ ДЕЛ ОД СОЗДАДЕНИТЕ ДЕЛА ОД НАЈМЛАДИТЕ УЧЕСНИЦИ ЌЕ СЕ ПРОДАВААТ ПО СИМБОЛИЧНА ЦЕНА А СОБРАНИТЕ СРЕДСТВА ЌЕ СЕ ПРЕДАДАТ НА ДОМОТ ЗА ДЕЦА БЕЗ РОДИТЕЛИ ЕДИНАЕСЕТТИ ОКТОМВРИ

Исто така, ја добиваме и пермутацијата која што колешката ја користела при шифрирање на пораката:

А	Б	В	Г	Д	Ѓ	Е	Ж	З	S	И	Ј	К	Л	Љ	М	Н	Њ	О	П	Р	С	Т	Ќ	У	Ф	Х	Ц	Ч	Џ	Ш
И	Ќ	Б	Џ	Т	Љ	П	Ѓ	Н	В	Ц	Ј	Г	М	С	Ф	А	Р	Д	Е	З	Њ	Ж	К	О	У	Ш	Л	Х	П	Ч

За паровите на букви означени со црвена боја не можеме да бидиме сигурни (ова е случаен резултат од спроведувањето на трансформациите погоре), бидејќи тие букви се немаат ниту еднаш појавено во оригиналниот и во шифрираниот текст којшто го добив од колешката. Доколку при идни текстови шифрирани со ова пермутација на азбуката, се сретнат овие букви, ќе биде многу лесно да се открие која буква што означува, бидејќи познати ни се значењата на другите 28 букви од македонската азбука користени во ова пермутација.