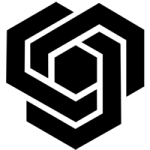
****

**ТЕХНИЧЕСКИ УНИВЕРСИТЕТ – СОФИЯ**

НАПРАВЛЕНИЕ „Компютърно и софтуерно инженерство”

Курсов проект по Криптографски методи за защита на информацията

Тема: „Честотен анализ на шифрирано съобщение на кирилица 2”

*Изработил/a:*

Ясна Владимиров, фак.номер: 123219010, група: 31

*Одобрил/а:*

доц. Антония Ташева

**Съдържание:**

1. Задание.......................................................................................................3
2. Прост заместващ шифър..........................................................................6
3. Метод – честотен анализ..........................................................................9
4. Резултати..................................................................................................14
5. Литература...............................................................................................36
6. **Задание:**

* Да се направи честотен анализ на шифрирано съобщение на кирилица
* Да се извърши декриптиране на текста с просто заместване.

**Шифрираното съобщение:**

***“****ЙАЧРПМ ВЯ ШЧЛЕЯ ЛЦВМ ЦЙГЦЙЛ. ЕМ УАПМ ГФВМ А СЯУМЕПАЧМ А ФВМТМ МУАНЯПМ ЦЯ ФЯЖШЕМСА СЯДВА ВЛОЯ. ЦЛВ ШПЛЦ ЦЛВ АДХГЪГЧЯПМ ЧЛЩЕМСААЕЛ, ХМАЕМ ЩМСЯЕЯ ЕСГЪЯПА ЪМ ЪСЯКВАЕЛ ША ЕЯЧЯВА, Я ЪМШПЛ ТА ЪМЪСЯЧРПМ А ТА ЪСМЦЯЧЯПМ ФВМТМ ЪМ-ШХЗЪМ. ЕЯХЯ ША АДХЯСЧЯПМ ЪСЛЩСЯВЯЕЯ.*

*ЦЙГЦЙЛЕМ ША АФЯПМ ФЯПХЯ ХЯСГНХЯ, Ш ХМРЕМ ЪСЛЧМДЧЯПМ ЧШАНХАЕЛ ША ЧЛОА. ЕЛТПЛПМ Р ШЯФ-ШЯФАНХМ! ЪМВРХМТЯ ШЛ МЪАЕЧЯПМ ЦЯ ВЯЕМЧЯСА Ч ВЛР А ФВМТМ ЕЛЙХА ЪСЛЦФЛЕА, ВМ ВЯПА УАПМ ЦСЛУВМ — ВЛ ФГ ШЕАТЯПА ШАПАЕЛ ЦЯ Р ЪМФСЗЦВЛ.*

*ЧЛЦВЗЙ ЕМ ШЛ ДЯФАШПАПМ ХЯХЧМ ЦЯ ВЯЪСЯЧА, ДЯ ЦЯ ФМЙЛ ЦЯ ЪСЛЧМДЧЯ А ЪМ-ЛЦСА ВЛОЯ. ФАШПАПМ, ФАШПАПМ… А ША АДФЯЖШЕМСАПМ ЪЯСВЯ ХМПЯ!*

*ЧЛНЛСЕЯ СЯУМЕПАЧМЕМ ЦЙГЦЙЛ ЪМХЯВАПМ ТМШЕА, ДЯ ЦЯ МЕЪСЯДВГЧЯ СЯЦМШЕВМЕМ ШЗУАЕАЛ, Я ВЯ ЦСГТАР ЦЛВ ЪМЦХЯСЯПМ ВМЧЯЕЯ ША ХМПЯ А ЪМЕЛТПАПМ ВЯ ЦЗПЗТ ЪЗЕ.*

*ЪСАШЕАТВЯПМ Ч ЛЦАВ ТМПРФ ТСЯЦ А ВЯХГЪАПМ УЛДУСМЖ ЧЛЩЕМСАА. ВЯЕМЧЯСАПМ ТА Ч ХМПЯЕЯ А ЪМЛПМ МУСЯЕВМ. ВМ ЕМТЯЧЯ ДЯЪМНВЯПА ЕСГЦВМШЕАЕЛ.*

*ШЪГШВЯП ШЛ ФСЯХ, ДЯЧЯПРП ШАПЛВ ЪМСМЖ… ЪМ ЛЦВМ ЧСЛФЛ ЦЙГЦЙЛЕМ СЯДУСЯПМ, НЛ Л ДЯТГУАПМ ЪЗЕР! ХМПХМЕМ ЪМЧЛНЛ ЧСЛФЛ ФАВЯЧЯПМ, ЕМПХМЧЯ ЪМ-ШЕСЯКВМ ШЕЯЧЯПМ.*

*АДЧЛЦВЗЙ ХМПЯЕЯ ЮМЪВЯПЯ Ч ЛЦВМ УПЯЕМ А ДЯЕЗВЯПЯ!*

*ФЗНАПМ ШЛ ЦЙГЦЙЛЕМ ЦЯ Р АДЕЛТПА, ФЗНАПМ ШЛ, ВМ ХМПЛПЯЕЯ Ж ВЛ ЪМФСЗЦЧЯПА! МЕНЯРП ШЛ ФЯПХАРЕ ЪЗЕЛКЛШЕЧЛВАХ. ЮРПЯ ВМО ШЛЦРП Ч ЕЗФВМЕМ А НЯХЯП ЦЯ ФАВЛ ВРХМЖ ЦМУЗС НМЧЛХ, ХМЖЕМ ЦЯ ФГ ШЛ ЪСАЕЛНЛ ВЯ ЪМФМО.*

*ВМ ВАХМЖ ВЛ АЦЧЯП.*

*Я ВЯ ШГЕСАВЕЯ ВЯЦ УПЯЕМЕМ ЪЯЦВЯПЯ ТЗШЕЯ ФЗТПЯ А МЕ ЧШАНХА ШЕСЯВА ШЛ СЯДВЛШПМ МТПГКАЕЛПВМ ХЧЯХЯВЛ. ХМТЯЕМ ФЗТПЯЕЯ ШЛ СЯДЪСЗШВЯПЯ, ЦЙГЦЙЛЕМ ЧАЦРПМ, НЛ Л ДЯМУАХМПЛВМ МЕ ЮРПЯ ЯСФАР ЙЯУА!*

*ШХМСМ ШЛ ЪМРЧАП УПЯЕВАРЕ ЮЯС.*

*— ЕА ХЯХЧМ ЕЗСШАК Ч ФМЛЕМ ЮЯСШЕЧМ? — ЪМЪАЕЯП ЕМЖ.*

*— ДЯТГУАЩ ШЛ Ч ЕЗФВМЕМ — ЪСМФЗПЧАПМ ЦЙГЦЙЛЕМ.*

*— ХЯХ ШФЛЛК! — СЯДТВЛЧАП ШЛ ЙЯУМХЗЕ. — ВАХМЖ ВРФЯ ЪСЯЧМ ЦЯ ШЕЗЪЧЯ Ч ФМЛЕМ УПЯЕМ УЛД СЯДСЛКЛВАЛ!*

*— ВМ ЯД ВЛ ДВЯЛЩ ХЗЦЛ ШЗФ, ЮЯСБ НЛШЕАЕА! — ЧЗДСЯДАПМ ГЪПЯКЛВМЕМ ЦЙГЦЙЛ.*

*— ЕМЧЯ ВЛ ЕЛ МЪСЯЧЦЯЧЯ! — МЕШРХЗП ЮЯСРЕ, ХМЖЕМ ВЯШХМСМ ША УАП ЪМШЕСМАП НАШЕМ ВМЧ ЕСЗШЕАХМЧ ЦЧМСЛЮ А ШЛТЯ ШЛ НГЦЛП Ш ХЯХЧМ ТМ МУДЯЧЛЦЛ. — Р ЦЯ ЧАЦР ХЯХЧМ АФЯК Ч ХМПЯЕЯ!*

*— ВАОМ ЮЛВВМ — МЕЧЗСВЯПМ ТМСХМЕМ ЦЙГЦЙЛ. — ШЯФМ ВРХМПХМ ВЛЪМЕСЛУВА ВЛОЯ.*

*ЙЯУМХЗЕ МТПЛЦЯП ПБУМЪАЕВМ ЕМЧЯСЯ А ХЯДЯП:*

*— Л, ЦМУСЛ. ОЛ ЕА ЪМФМТВЯ ЦЯ ША АДЕЛТПАК ХМПЯЕЯ МЕ УПЯЕМЕМ, ВМ Ч ДЯФРВЯ ЕА ОЛ ФА ЦЯЦЛК ЧШАНХА ЕЛДА ВЛОЯ.*

*ЦЙГЦЙЛЕМ СЯДУСЯПМ, НЛ ОЛ ДЯТГУА ЮРПМЕМ ША УМТЯЕШЕЧМ, А ЛЦЧЯ ВЛ ДЯЪПЯХЯПМ. ВМ ВРФЯПМ ОМ ЦЯ ШЕМСА — ШХПМВАПМ.*

*— УАЧЯ, ЮЯСБ — ХЯДЯПМ ЕМ. — ШЯФМ НЛ ФА ЪМДЧМПА ЦЯ ДЯЪЯДР ДЯ ШЛУЛ ША МВМЧЯ, ХМЛЕМ ФМЙЛ ЦЯ ШЛ ЪМУЛСЛ Ч ФЯПХМЕМ ФА НЛСЧЛВМ КЯПНЛ.*

*ЮЯСРЕ ЪМФАШПАП ФЯПХМ А ШЛ ШЗТПЯШАП. ЪМШПЛ ЪМЧАХЯП ЙЯУЛКХАР ТЛВЛСЯП А ФГ ДЯЪМЧРЦЯП ЦЯ ЦМЧЛЦЛ ВЯЖ-ЦМУСАР МЕСРЦ МЕ ЮЯСШХЯЕЯ ТЧЯСЦАР. НЛ ХЯЕМ ДЯЪСААЙЦЯПА ЛЦВА ФА ЕА ЙЯУМЮА… ЧШАНХА ЦСГЙВМ ШЛ ЩЧЯВЯПА ДЯ СЯУМЕЯ! ЦЗСЪЯПА, ЦЗСЪЯПА, ВМ ВЛ ГШЪЛПА ЦЯ АДЧЯЦРЕ ХМПЯЕЯ МЕ УПЯЕМЕМ.*

*ВЯПМЙАПМ ШЛ ЦЯ ЪМЧАХЯЕ ВЯ ЪМФМО УМУЗСЯ А ЦЧЯ ЧМЦВА ЪПЗЩЯ.*

*Ч ЕМЧЯ ЧСЛФЛ ГФВМЕМ ЦЙГЦЙЛ ШЛ ЪМХЯЕЛСАПМ ВЯ ЧЗСЩЯ ВЯ ХГЪНАВЯЕЯ ЧЛЩЕМСАА А ДЯЪМНВЯПМ УЗСДМ-УЗСДМ ЦЯ СЯДЪПАЕЯ ФЯПХМЕМ ША НЛСЧЛВМ КЯПНЛ. АДЕЛТПАПМ ЛЦВЯ ЦЗПТЯ ЧЗПВЛВЯ ВАКХЯ А Р ВЯФМЕЯПМ ВРХМПХМ ЪЗЕА МХМПМ ЕМЧЯСЯ!*

*ХМТЯЕМ ХМПЯЕЯ ВЯЖ-ЪМШПЛ ШЛ МДМЧЯПЯ ВЯ ШГКЯЕЯ, ЮЯСРЕ ЦМЧЕЯШЯП ЦЯ ЧДЛФЛ ХЯХЧМЕМ ФГ ШЛ ЪМПЯТЯ.*

*ЦЙГЦЙЛЕМ ТМ ЪМШСЛОВЯПМ Ш ЦГФАЕЛ:*

*— ЮЯСБ НЛШЕАЕА, СЯДУСЯЩФЛ ШЛ ЦЯ ДЯЪЯДР ДЯ ШЛУЛ ША МВМЧЯ, ХМЛЕМ ФМЙЛ ЦЯ ШЛ ЪМУЛСЛ Ч ФЯПХМЕМ ФА НЛСЧЛВМ КЯПНЛ. ШЗЙЯПРЧЯФ, ВМ ДЯ ЕЛУЛ ВАОАНХМ ВЛ МШЕЯВЯ!*

*ЕМТЯЧЯ УПЯЕВАРЕ ЮЯС СЯДУСЯП, НЛ ЦСЛУМШЗХЗЕ ТМ Л ВЯЦЩАЕСАП, ЯПЯ ВРФЯПМ ОМ ЦЯ ШЕМСА — ЮЯСШХЯ ЦГФЯ ВЯ ЦЧЛ ВЛ ШЕЯЧЯ!*

*ЦМЧМПВМ А ОЯШЕПАЧМ, ГФВМЕМ ЦЙГЦЙЛ ШЛ ЪСАУСЯПМ Г ЦМФЯ ША А ГШЕСМАПМ ТМПРФМ ЪАСКЛШЕЧМ, ВЯ ХМЛЕМ ЪМХЯВАПМ А ВМЧАЕЛ ША ЪСАРЕЛПА ЙЯУАЕЛ. ВЯТМШЕАПМ ТА УМТЯЕМ. ВЯХСЯР СЯДЕМЧЯСАПМ ЪЯСВЯЕЯ ХМПЯ А СЯДЦЯПМ ЪМЦЯСЗЮА ВЯ ЧШАНХА.*

*— Я ЪЗХ ЧАЛ, ЯХМ ЙЛПЯЛЕЛ, ФМЙЛЕЛ ЦЯ ФА ЪМЦЯСАЕЛ ЛЦАВ ВМЧ НЛСЧЛВ КЯП — ЪМКЛТГЧЯПМ ШЛ ЕМ.*

1. **Прост заместващ шифър:**

В криптографията заместващият шифър е метод на криптиране, чрез който единиците от отворен текст се заменят с шифроване съгласно обикновена система; "единиците" могат да бъдат единични букви (най-често срещаните), двойки букви, тройки букви, смеси от горните и т.н. Получателят дешифрира текста, като извършва обратно заместване.

Шифърите за заместване могат да бъдат сравнени с транспозиционните шифри. При транспозиционен шифър единиците на открития текст се пренареждат в различен и обикновено доста сложен ред, но самите единици се оставят непроменени. За разлика от това, при заместващ шифър, единиците на отворения текст се запазват в същата последователност в шифротекста, но самите единици се променят.

Има редица различни видове заместващи шифъри. Ако шифърът работи с единични букви, той се нарича прост заместващ шифър; шифър, който оперира с по-големи групи от букви, се нарича полиграфски. Едноазбучен шифър използва фиксирано заместване върху цялото съобщение, докато полиазбучен шифър използва редица замествания в различни моменти в съобщението, където единица от отворения текст се съпоставя с една от няколкото възможности в шифротекста и обратно.

Прост заместващ шифър (наричан още моноалфабетен шифър) замества всеки знак в открития текст с друг предварително определен знак, за да образува шифротекста. Формално, нека **A** е буквен символ на обикновен текст с размер **n**, където **A** ∈ {a0, a1, ..., an−1} и **C** е буквен знак за шифрован текст с размер **n**, **C** ∈ {f(a0), f( a1), ..., f(an−1)}. Всеки символ на A има едно към едно съпоставяне със съответния символ на C, f: A → C.

За азбука с **n** знака има **n!** възможни пермутации; например за английската азбука от 26 букви има 26! възможни пермутации или 4.03e+26. Ако някой можеше да проверява 1 000 000 пермутации в секунда, все пак ще отнеме над 12 трилиона години, за да провери всички възможни ключове, така че криптоанализът при този метод с груба сила е неосъществим. Този тип криптосистема е лесна за внедряване и използване. Въпреки това, не е трудно да се разбие, тъй като не прави нищо, за да прикрие статистическите свойства на езика. Следователно, той не осигурява много сигурност и може лесно да бъде разбит чрез анализ на *честотното разпределение*. Ръчното дешифриране на заместващи шифри обикновено започва с честотен анализ, при условие че шифротекстът е достатъчно дълъг, последван от различни евристики.

Чрез използване на честотен анализ на отделни букви, криптоаналитикът може лесно да дешифрира ръчно шифрован текст, който използва тази криптосистема. Това все пак ще се случи, дори ако честотите на знаците на шифрования текст са различни от тези на нормалния текст. С няколко опита и след като изпробва някои от възможностите, криптоаналитикът ще може да намери правилната замяна.

Основният въпрос, когато разчитате на честотен анализ е „доколко това декриптиране прилича на езика в който декритптираме (английски или български или др.)?“ Формален процес на честотен анализ ни позволява да определим колко точно даден текст изглежда като езика, на който е написан откритият текст.

Разпределенията на диаграми, триграми, най-често използвани думи в даден език предоставят по-полезна информация, която също може да бъде достъпна от криптоаналитика. Обикновено различните езици имат различна честота на буквите. Така че е възможно да се определи езикът на отворения текст, преди да започне да се декриптира шифротекста, ако е даден достатъчно дълъг шифров текст.

Въпреки факта, че обикновените заместващи шифри не се използват обикновено в реалните кодиращи системи в днешно време, много ефективни и сигурни съвременни шифри използват заместващи шифри в комбинация с други шифри, например транспозиционни шифри, модулна аритметика, булева алгебра и т.н. Тази мощна комбинация е важна иновация, тъй като води до метод, който е по-силен от оригиналните му компоненти. Въпреки че едноазбучните шифри не се считат за сигурни, те често се използват като градивни елементи в по-големи криптографски системи от най-съвременно състояние.

Следователно е толкова важно да се разбере уязвимостта на тези прости системи за шифроване, за да се помогне при изграждането на по-сложни шифри.

Класическите шифри обикновено попадат в две основни категории: заместващи шифри и транспониращи шифри. Съвременните системи за криптиране вече са изместили класическите системи; обаче, най-популярното криптологично приложение и реализация за изследване на метаевристично търсене е криптоанализът на класическите шифри. Основните концепции за заместващи шифри и транспозиционни шифри все още се използват широко в наши дни в Advanced Encryption Standard (AES) и Международния алгоритъм за криптиране на данни (IDEA).

Докато операциите и концепциите на класическите шифроващи системи са основните градивни елементи на по-сигурните съвременни шифри, тогава класическите шифри обикновено са първите шифри, които се разглеждат в случай на разследване и изследване на нови атаки.

MonoAlphabetic Substitution Cipher картографира отделни букви на отворен текст към отделни букви на шифротекст на уникална основа 1 към 1. Тоест, всеки екземпляр на дадена буква винаги се съпоставя с една и съща буква от шифрован текст.

Най-старият известен такъв шифър е шифърът на Цезар, където картографирането включва проста промяна в азбуката.

През 9-ти век арабският ерудит Абу Юсуф Якуб ибн Исхак ал-Саббах Ал-Кинди в „Ръкопис за дешифриране на криптографски съобщения“ описва честотния анализ като метод за унищожаване на едноазбучния заместващ шифър.

Този метод използва характеристиките на всеки даден участък от писмения език, където определени букви или комбинации от букви се срещат с различна честота.

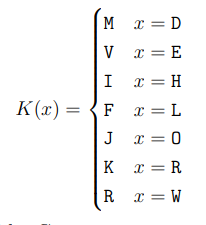
Всички форми на симетрично криптиране приемат ключ, споделен между малка група хора, и кодират данни с помощта на този ключ, така че само тези с ключа да могат да го декриптират. Алгоритмите за криптиране са склонни да разчитат на проблеми, които са изчислително неразрешими за сигурност, но дори по-общо тези алгоритми разчитат на основното предположение: че броят на потенциалните ключове е толкова голям, че не може да се търси чрез груба сила за правилния ключ в разумно количество време.

Някои шифри – като шифрите с едноалфавитно заместване – имат изключително големи ключови пространства, като привидно избягват тази слабост. Тези шифри обаче проявяват определено свойство, което всъщност прави възможно ефективно търсене в тези невероятно големи ключови пространства, което ги прави уязвими за криптоанализ чрез рандомизирани алгоритми за търсене.

Една конкретна форма на шифър за заместване е моноалфавитният заместващ шифър, често наричан „прост шифър за заместване“. Моноалфавитните заместващи шифри разчитат на една функция за преобразуване на ключ **K**, която последователно замества конкретен знак **α** със знак от преобразуването **K(α)**. За **функция за криптиране** **E** и **функция за декриптиране D** с **отворен текст P** и **шифрован текст C**, *|P| = |C|* и

∀i, 0 < i ≤ |P|, Ci = E(Pi) = K(Pi), Pi = D(Ci). Преобразуването е едно към едно, така че за всички знаци α, β в открития текст, α = β ⇒ K(α) = K(β) и α ≠ β ⇒ K(α) ≠ K(β ).

Като пример, ако вземем обикновения текст P = HELLO WORLD и използваме:



Полученият шифротекст би бил C = IFVVJ FJKFM.

Методът е елегантен и лесен за използване, изисква само познаване на ключ, чиято дължина не е по-дълга от размера на азбуката.

Моноалфавитните заместващи шифри са различни от много други шифри, тъй като частичните ключове са полезни, което ги прави уязвими за оптимизирана атака. Най-простият и най-малко ефективен от тези алгоритми, простият Evolutionary Strategy алгоритъм, може да извърши автоматизиран криптоанализ на достатъчно дълги шифротекстове за няколко минути на скромен компютър, бързо намирайки почти оптимален ключ въпреки ключовото пространство в септилионите.

Моноалфавитният заместващ шифър, тъй като има количествено измерим размер на решението и оптимално решение, което не може да бъде известно предварително, е чудесен еталон за нови метаевристики. Наистина, много изследвания показват, че това е така, като по-модерните метаевристики бързо намират ключове за шифроване. Това също е разширено до полиалфабетни заместващи шифри и е логично, че ще работи за всеки шифър, който показва свойството полезност на частичните решения. Въпреки че класическите схеми за криптиране като тези заместващи шифри вече не се използват широко днес, заслужава да се отбележи, че те са толкова слаби, че съвременните компютри могат да извършват автоматизирани криптоанализни атаки срещу тях невероятно лесно въпреки огромните ключови пространства, подчертавайки важността на използването на съвременни шифри за криптиране на дълги съобщения.

1. Метод - Честотен анализ:

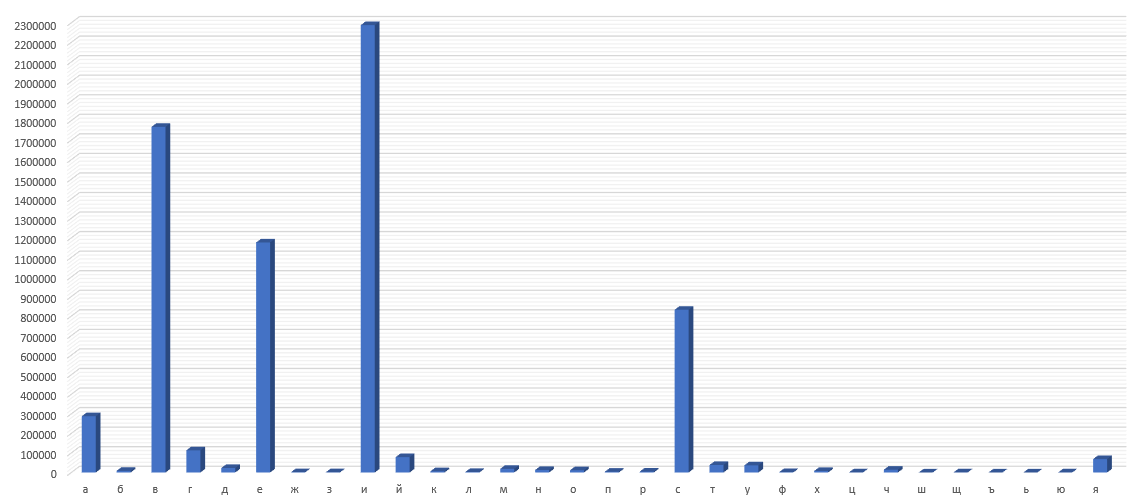
За честотите на буквите от българската азбука, използвах се от метода – честотен анализ, в криптографията честотният анализ е изследване на честотата на буквите или групите от букви в шифров текст. Методът се използва като помощно средство за разбиване на заместващи шифри (напр. едноазбучен шифър за заместване, шифър за смяна на Цезар, и др.).

За тази цел, използвах се от изследванията на българска организация под название BullTreeBank Group, която работи по проекти, свързани с компютърната лингвистика и семантичен уеб и предоставят езикови ресурси и инструменти за българския език. По точно, тeхния статистически анализ който дава сведения за честотите на най-срещаните 100 000 думи в българския език ()

*Коя буква колко пъти се среща?*

В таблицата по-долу се намира списъка с 30 букви от българската азбука, заедно с броя на срещанията им, и също техните съотношения представени графично:

|  |  |
| --- | --- |
| ***А-Я :*** | ***Честота на срещания:*** |
| а | 287965 |
| б | 8885 |
| в | 1767775 |
| г | 113746 |
| д | 23157 |
| е | 1176445 |
| ж | 1885 |
| з | 1683 |
| и | 2288298 |
| й | 78702 |
| к | 6806 |
| л | 3088 |
| м | 19022 |
| н | 12952 |
| о | 11761 |
| п | 4261 |
| р | 4917 |
| с | 832328 |
| т | 38348 |
| у | 36799 |
| ф | 2422 |
| х | 7733 |
| ц | 881 |
| ч | 14579 |
| ш | 285 |
| щ | 956 |
| ъ | 198 |
| ь | 123 |
| ю | 849 |
| я | 68823 |



Следващата стъпка е да се направи честотен анализ и на шифрирания текст, за да разберем коя буква колко пъти се среща и следователно започнем със заместването. За тази цел съм написала програма на С#, която минава през целия текст и като резултат изписва коя буква колко пъти се появява.

namespace CountLetters

{

class Program

{

public static void Main()

{

var letters = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЬЮЯ".ToArray();

Dictionary<char, int> lettersCount = new Dictionary<char, int>();

using (var f = new StreamReader("EncryptedMessage2.txt"))

{

while (!f.EndOfStream)

{

char c = (char)f.Read();

if (letters.Contains(c))

{

if (lettersCount.ContainsKey(c))

{

lettersCount[c]++;

}

else

{

lettersCount.Add(c, 1);

}

}

}

}

foreach (var letter in lettersCount)

{

Console.WriteLine($"{letter.Key} - {letter.Value}");

}

}

}

}

*Получения резултат:*

Й - 45

А - 219

Ч - 119

Р - 49

П - 173

М - 350

В - 150

Я - 353

Ш - 117

Л - 214

Е - 188

Ц - 118

Г - 45

У - 54

Ф - 75

С - 128

Т - 49

Н - 37

Ж - 13

Д - 61

О - 17

Х - 99

Ъ - 88

Щ - 12

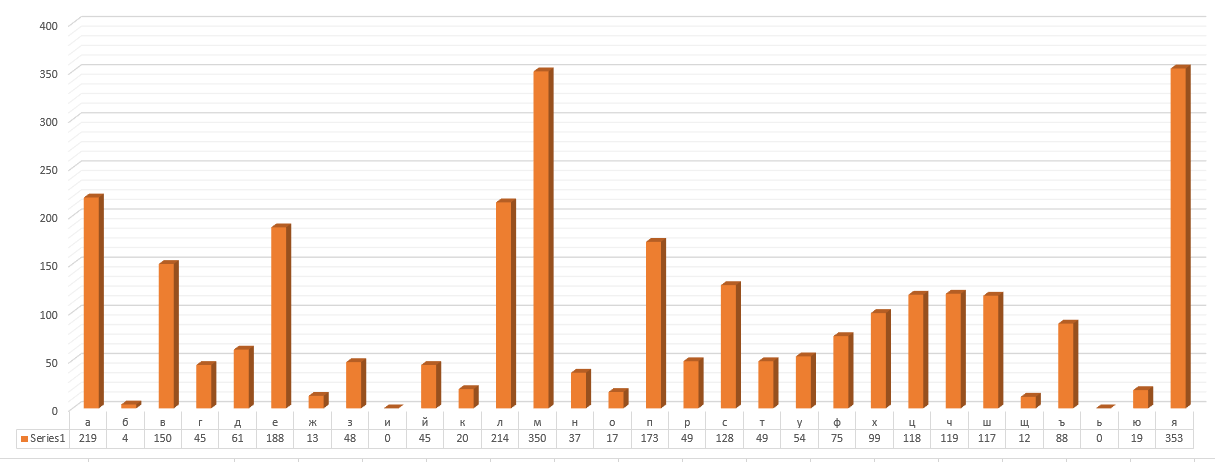
К - 20

З - 48

Ю - 19

Б - 4

За по-добро разбиране, резултата съм представила и графично:



След като имаме честотите и на шифрирания текст, можем да започнем с декриптирането, но понеже процесът на честотния анализ използва различни фини свойства на езика, не е достатъчно да се напише програма в която компютърът да върши цялата работа, неизбежно е човешкия принос в този процес, за да се вземат обосновани решения кои букви да се заменят. За да се спести време и труд, изготвя се програма която замества буквите в шифрирания текст с дадена буква която потребителя задава, като на всяка итерация главните букви от шифрирания текст се заместват с малки букви зададени от потребителя. По този начин се допуска контрола на декриптирането на потребителя, тъй както вече беше споменато, компютърската програма не може сама да декриптира текста.

namespace CountLetters

{

class Program

{

public static void Main()

{

const string path = "EncryptedMessage2.txt";

char[] letters = "АБВГДЕЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЬЮЯ".ToArray();

Dictionary<char, int> lettersCount = new Dictionary<char, int>();

using (var f = new StreamReader(path))

{

while (!f.EndOfStream)

{

char c = (char)f.Read();

if (letters.Contains(c))

{

if (lettersCount.ContainsKey(c))

{

lettersCount[c]++;

}

else

{

lettersCount.Add(c, 1);

}

}

}

}

lettersCount = lettersCount

.OrderByDescending(x => x.Value)

.ToDictionary(x => x.Key, x => x.Value);

foreach (var letter in lettersCount)

{

Console.WriteLine($"{letter.Key}: {letter.Value}");

}

string text = File.ReadAllText(path);

while(true)

{

Console.WriteLine(Environment.NewLine + text + Environment.NewLine);

Console.Write("Заместване на: ");

string letter = Console.ReadLine();

Console.Write("Нова буква: ");

string replaceWith = Console.ReadLine();

text = text.Replace(letter, replaceWith);

}

}

}

}

1. **Резултати**

Резултите от декриптирането на шифрирания текст са представени в 10 стъпки.

1. Я 🡪 а ⇒ В 🡪 н ⇒ Ж 🡪 й

ЙАЧРПМ на ШЧЛЕа ЛЦнМ ЦЙГЦЙЛ. ЕМ УАПМ ГФнМ А СаУМЕПАЧМ А ФнМТМ МУАНаПМ Ца ФайШЕМСА СаДнА нЛОа. ЦЛн ШПЛЦ ЦЛн АДХГЪГЧаПМ ЧЛЩЕМСААЕЛ, ХМАЕМ ЩМСаЕа ЕСГЪаПА ЪМ ЪСаКнАЕЛ ША ЕаЧанА, а ЪМШПЛ ТА ЪМЪСаЧРПМ А ТА ЪСМЦаЧаПМ ФнМТМ ЪМ-ШХЗЪМ. ЕаХа ША АДХаСЧаПМ ЪСЛЩСанаЕа.

ЦЙГЦЙЛЕМ ША АФаПМ ФаПХа ХаСГНХа, Ш ХМРЕМ ЪСЛЧМДЧаПМ ЧШАНХАЕЛ ША ЧЛОА. ЕЛТПЛПМ Р ШаФ-ШаФАНХМ! ЪМнРХМТа ШЛ МЪАЕЧаПМ Ца наЕМЧаСА Ч нЛР А ФнМТМ ЕЛЙХА ЪСЛЦФЛЕА, нМ наПА УАПМ ЦСЛУнМ - нЛ ФГ ШЕАТаПА ШАПАЕЛ Ца Р ЪМФСЗЦнЛ.

ЧЛЦнЗЙ ЕМ ШЛ ДаФАШПАПМ ХаХЧМ Ца наЪСаЧА, Да Ца ФМЙЛ Ца ЪСЛЧМДЧа А ЪМ-ЛЦСА нЛОа. ФАШПАПМ, ФАШПАПМ: А ША АДФайШЕМСАПМ ЪаСна ХМПа!

ЧЛНЛСЕа СаУМЕПАЧМЕМ ЦЙГЦЙЛ ЪМХанАПМ ТМШЕА, Да Ца МЕЪСаДнГЧа СаЦМШЕнМЕМ ШЗУАЕАЛ, а на ЦСГТАР ЦЛн ЪМЦХаСаПМ нМЧаЕа ША ХМПа А ЪМЕЛТПАПМ на ЦЗПЗТ ЪЗЕ.

ЪСАШЕАТнаПМ Ч ЛЦАн ТМПРФ ТСаЦ А наХГЪАПМ УЛДУСМй ЧЛЩЕМСАА. наЕМЧаСАПМ ТА Ч ХМПаЕа А ЪМЛПМ МУСаЕнМ. нМ ЕМТаЧа ДаЪМНнаПА ЕСГЦнМШЕАЕЛ.

ШЪГШнаП ШЛ ФСаХ, ДаЧаПРП ШАПЛн ЪМСМй: ЪМ ЛЦнМ ЧСЛФЛ ЦЙГЦЙЛЕМ СаДУСаПМ, НЛ Л ДаТГУАПМ ЪЗЕР! ХМПХМЕМ ЪМЧЛНЛ ЧСЛФЛ ФАнаЧаПМ, ЕМПХМЧа ЪМ-ШЕСаКнМ ШЕаЧаПМ.

АДЧЛЦнЗЙ ХМПаЕа ЮМЪнаПа Ч ЛЦнМ УПаЕМ А ДаЕЗнаПа!

ФЗНАПМ ШЛ ЦЙГЦЙЛЕМ Ца Р АДЕЛТПА, ФЗНАПМ ШЛ, нМ ХМПЛПаЕа й нЛ ЪМФСЗЦЧаПА! МЕНаРП ШЛ ФаПХАРЕ ЪЗЕЛКЛШЕЧЛнАХ. ЮРПа нМО ШЛЦРП Ч ЕЗФнМЕМ А НаХаП Ца ФАнЛ нРХМй ЦМУЗС НМЧЛХ, ХМйЕМ Ца ФГ ШЛ ЪСАЕЛНЛ на ЪМФМО.

нМ нАХМй нЛ АЦЧаП.

а на ШГЕСАнЕа наЦ УПаЕМЕМ ЪаЦнаПа ТЗШЕа ФЗТПа А МЕ ЧШАНХА ШЕСанА ШЛ СаДнЛШПМ МТПГКАЕЛПнМ ХЧаХанЛ. ХМТаЕМ ФЗТПаЕа ШЛ СаДЪСЗШнаПа, ЦЙГЦЙЛЕМ ЧАЦРПМ, НЛ Л ДаМУАХМПЛнМ МЕ ЮРПа аСФАР ЙаУА!

ШХМСМ ШЛ ЪМРЧАП УПаЕнАРЕ ЮаС.

- ЕА ХаХЧМ ЕЗСШАК Ч ФМЛЕМ ЮаСШЕЧМ? - ЪМЪАЕаП ЕМй.

- ДаТГУАЩ ШЛ Ч ЕЗФнМЕМ - ЪСМФЗПЧАПМ ЦЙГЦЙЛЕМ.

- ХаХ ШФЛЛК! - СаДТнЛЧАП ШЛ ЙаУМХЗЕ. - нАХМй нРФа ЪСаЧМ Ца ШЕЗЪЧа Ч ФМЛЕМ УПаЕМ УЛД СаДСЛКЛнАЛ!

- нМ аД нЛ ДнаЛЩ ХЗЦЛ ШЗФ, ЮаСБ НЛШЕАЕА! - ЧЗДСаДАПМ ГЪПаКЛнМЕМ ЦЙГЦЙЛ.

- ЕМЧа нЛ ЕЛ МЪСаЧЦаЧа! - МЕШРХЗП ЮаСРЕ, ХМйЕМ наШХМСМ ША УАП ЪМШЕСМАП НАШЕМ нМЧ ЕСЗШЕАХМЧ ЦЧМСЛЮ А ШЛТа ШЛ НГЦЛП Ш ХаХЧМ ТМ МУДаЧЛЦЛ. - Р Ца ЧАЦР ХаХЧМ АФаК Ч ХМПаЕа!

- нАОМ ЮЛннМ - МЕЧЗСнаПМ ТМСХМЕМ ЦЙГЦЙЛ. - ШаФМ нРХМПХМ нЛЪМЕСЛУнА нЛОа.

ЙаУМХЗЕ МТПЛЦаП ПБУМЪАЕнМ ЕМЧаСа А ХаДаП:

- Л, ЦМУСЛ. ОЛ ЕА ЪМФМТна Ца ША АДЕЛТПАК ХМПаЕа МЕ УПаЕМЕМ, нМ Ч ДаФРна ЕА ОЛ ФА ЦаЦЛК ЧШАНХА ЕЛДА нЛОа.

ЦЙГЦЙЛЕМ СаДУСаПМ, НЛ ОЛ ДаТГУА ЮРПМЕМ ША УМТаЕШЕЧМ, А ЛЦЧа нЛ ДаЪПаХаПМ. нМ нРФаПМ ОМ Ца ШЕМСА - ШХПМнАПМ.

- УАЧа, ЮаСБ - ХаДаПМ ЕМ. - ШаФМ НЛ ФА ЪМДЧМПА Ца ДаЪаДР Да ШЛУЛ ША МнМЧа, ХМЛЕМ ФМЙЛ Ца ШЛ ЪМУЛСЛ Ч ФаПХМЕМ ФА НЛСЧЛнМ КаПНЛ.

ЮаСРЕ ЪМФАШПАП ФаПХМ А ШЛ ШЗТПаШАП. ЪМШПЛ ЪМЧАХаП ЙаУЛКХАР ТЛнЛСаП А ФГ ДаЪМЧРЦаП Ца ЦМЧЛЦЛ най-ЦМУСАР МЕСРЦ МЕ ЮаСШХаЕа ТЧаСЦАР. НЛ ХаЕМ ДаЪСААЙЦаПА ЛЦнА ФА ЕА ЙаУМЮА: ЧШАНХА ЦСГЙнМ ШЛ ЩЧанаПА Да СаУМЕа! ЦЗСЪаПА, ЦЗСЪаПА, нМ нЛ ГШЪЛПА Ца АДЧаЦРЕ ХМПаЕа МЕ УПаЕМЕМ.

наПМЙАПМ ШЛ Ца ЪМЧАХаЕ на ЪМФМО УМУЗСа А ЦЧа ЧМЦнА ЪПЗЩа.

Ч ЕМЧа ЧСЛФЛ ГФнМЕМ ЦЙГЦЙЛ ШЛ ЪМХаЕЛСАПМ на ЧЗСЩа на ХГЪНАнаЕа ЧЛЩЕМСАА А ДаЪМНнаПМ УЗСДМ-УЗСДМ Ца СаДЪПАЕа ФаПХМЕМ ША НЛСЧЛнМ КаПНЛ. АДЕЛТПАПМ ЛЦна ЦЗПТа ЧЗПнЛна нАКХа А Р наФМЕаПМ нРХМПХМ ЪЗЕА МХМПМ ЕМЧаСа!

ХМТаЕМ ХМПаЕа най-ЪМШПЛ ШЛ МДМЧаПа на ШГКаЕа, ЮаСРЕ ЦМЧЕаШаП Ца ЧДЛФЛ ХаХЧМЕМ ФГ ШЛ ЪМПаТа.

ЦЙГЦЙЛЕМ ТМ ЪМШСЛОнаПМ Ш ЦГФАЕЛ:

- ЮаСБ НЛШЕАЕА, СаДУСаЩФЛ ШЛ Ца ДаЪаДР Да ШЛУЛ ША МнМЧа, ХМЛЕМ ФМЙЛ Ца ШЛ ЪМУЛСЛ Ч ФаПХМЕМ ФА НЛСЧЛнМ КаПНЛ. ШЗЙаПРЧаФ, нМ Да ЕЛУЛ нАОАНХМ нЛ МШЕана!

ЕМТаЧа УПаЕнАРЕ ЮаС СаДУСаП, НЛ ЦСЛУМШЗХЗЕ ТМ Л наЦЩАЕСАП, аПа нРФаПМ ОМ Ца ШЕМСА - ЮаСШХа ЦГФа на ЦЧЛ нЛ ШЕаЧа!

ЦМЧМПнМ А ОаШЕПАЧМ, ГФнМЕМ ЦЙГЦЙЛ ШЛ ЪСАУСаПМ Г ЦМФа ША А ГШЕСМАПМ ТМПРФМ ЪАСКЛШЕЧМ, на ХМЛЕМ ЪМХанАПМ А нМЧАЕЛ ША ЪСАРЕЛПА ЙаУАЕЛ. наТМШЕАПМ ТА УМТаЕМ. наХСаР СаДЕМЧаСАПМ ЪаСнаЕа ХМПа А СаДЦаПМ ЪМЦаСЗЮА на ЧШАНХА.

- а ЪЗХ ЧАЛ, аХМ ЙЛПаЛЕЛ, ФМЙЛЕЛ Ца ФА ЪМЦаСАЕЛ ЛЦАн нМЧ НЛСЧЛн КаП - ЪМКЛТГЧаПМ ШЛ ЕМ.

1. Л 🡪 е ⇒ Ш 🡪 с ⇒ А 🡪 и

ЙиЧРПМ на сЧеЕа еЦнМ ЦЙГЦЙе. ЕМ УиПМ ГФнМ и СаУМЕПиЧМ и ФнМТМ МУиНаПМ Ца ФайсЕМСи СаДни неОа. Цен сПеЦ Цен иДХГЪГЧаПМ ЧеЩЕМСииЕе, ХМиЕМ ЩМСаЕа ЕСГЪаПи ЪМ ЪСаКниЕе си ЕаЧани, а ЪМсПе Ти ЪМЪСаЧРПМ и Ти ЪСМЦаЧаПМ ФнМТМ ЪМ-сХЗЪМ. ЕаХа си иДХаСЧаПМ ЪСеЩСанаЕа.

ЦЙГЦЙеЕМ си иФаПМ ФаПХа ХаСГНХа, с ХМРЕМ ЪСеЧМДЧаПМ ЧсиНХиЕе си ЧеОи. ЕеТПеПМ Р саФ-саФиНХМ! ЪМнРХМТа се МЪиЕЧаПМ Ца наЕМЧаСи Ч неР и ФнМТМ ЕеЙХи ЪСеЦФеЕи, нМ наПи УиПМ ЦСеУнМ - не ФГ сЕиТаПи сиПиЕе Ца Р ЪМФСЗЦне.

ЧеЦнЗЙ ЕМ се ДаФисПиПМ ХаХЧМ Ца наЪСаЧи, Да Ца ФМЙе Ца ЪСеЧМДЧа и ЪМ-еЦСи неОа. ФисПиПМ, ФисПиПМ: и си иДФайсЕМСиПМ ЪаСна ХМПа!

ЧеНеСЕа СаУМЕПиЧМЕМ ЦЙГЦЙе ЪМХаниПМ ТМсЕи, Да Ца МЕЪСаДнГЧа СаЦМсЕнМЕМ сЗУиЕие, а на ЦСГТиР Цен ЪМЦХаСаПМ нМЧаЕа си ХМПа и ЪМЕеТПиПМ на ЦЗПЗТ ЪЗЕ.

ЪСисЕиТнаПМ Ч еЦин ТМПРФ ТСаЦ и наХГЪиПМ УеДУСМй ЧеЩЕМСии. наЕМЧаСиПМ Ти Ч ХМПаЕа и ЪМеПМ МУСаЕнМ. нМ ЕМТаЧа ДаЪМНнаПи ЕСГЦнМсЕиЕе.

сЪГснаП се ФСаХ, ДаЧаПРП сиПен ЪМСМй: ЪМ еЦнМ ЧСеФе ЦЙГЦЙеЕМ СаДУСаПМ, Не е ДаТГУиПМ ЪЗЕР! ХМПХМЕМ ЪМЧеНе ЧСеФе ФинаЧаПМ, ЕМПХМЧа ЪМ-сЕСаКнМ сЕаЧаПМ.

иДЧеЦнЗЙ ХМПаЕа ЮМЪнаПа Ч еЦнМ УПаЕМ и ДаЕЗнаПа!

ФЗНиПМ се ЦЙГЦЙеЕМ Ца Р иДЕеТПи, ФЗНиПМ се, нМ ХМПеПаЕа й не ЪМФСЗЦЧаПи! МЕНаРП се ФаПХиРЕ ЪЗЕеКесЕЧениХ. ЮРПа нМО сеЦРП Ч ЕЗФнМЕМ и НаХаП Ца Фине нРХМй ЦМУЗС НМЧеХ, ХМйЕМ Ца ФГ се ЪСиЕеНе на ЪМФМО.

нМ ниХМй не иЦЧаП.

а на сГЕСинЕа наЦ УПаЕМЕМ ЪаЦнаПа ТЗсЕа ФЗТПа и МЕ ЧсиНХи сЕСани се СаДнесПМ МТПГКиЕеПнМ ХЧаХане. ХМТаЕМ ФЗТПаЕа се СаДЪСЗснаПа, ЦЙГЦЙеЕМ ЧиЦРПМ, Не е ДаМУиХМПенМ МЕ ЮРПа аСФиР ЙаУи!

сХМСМ се ЪМРЧиП УПаЕниРЕ ЮаС.

- Еи ХаХЧМ ЕЗСсиК Ч ФМеЕМ ЮаСсЕЧМ? - ЪМЪиЕаП ЕМй.

- ДаТГУиЩ се Ч ЕЗФнМЕМ - ЪСМФЗПЧиПМ ЦЙГЦЙеЕМ.

- ХаХ сФееК! - СаДТнеЧиП се ЙаУМХЗЕ. - ниХМй нРФа ЪСаЧМ Ца сЕЗЪЧа Ч ФМеЕМ УПаЕМ УеД СаДСеКение!

- нМ аД не ДнаеЩ ХЗЦе сЗФ, ЮаСБ НесЕиЕи! - ЧЗДСаДиПМ ГЪПаКенМЕМ ЦЙГЦЙе.

- ЕМЧа не Ее МЪСаЧЦаЧа! - МЕсРХЗП ЮаСРЕ, ХМйЕМ насХМСМ си УиП ЪМсЕСМиП НисЕМ нМЧ ЕСЗсЕиХМЧ ЦЧМСеЮ и сеТа се НГЦеП с ХаХЧМ ТМ МУДаЧеЦе. - Р Ца ЧиЦР ХаХЧМ иФаК Ч ХМПаЕа!

- ниОМ ЮеннМ - МЕЧЗСнаПМ ТМСХМЕМ ЦЙГЦЙе. - саФМ нРХМПХМ неЪМЕСеУни неОа.

ЙаУМХЗЕ МТПеЦаП ПБУМЪиЕнМ ЕМЧаСа и ХаДаП:

- е, ЦМУСе. Ое Еи ЪМФМТна Ца си иДЕеТПиК ХМПаЕа МЕ УПаЕМЕМ, нМ Ч ДаФРна Еи Ое Фи ЦаЦеК ЧсиНХи ЕеДи неОа.

ЦЙГЦЙеЕМ СаДУСаПМ, Не Ое ДаТГУи ЮРПМЕМ си УМТаЕсЕЧМ, и еЦЧа не ДаЪПаХаПМ. нМ нРФаПМ ОМ Ца сЕМСи - сХПМниПМ.

- УиЧа, ЮаСБ - ХаДаПМ ЕМ. - саФМ Не Фи ЪМДЧМПи Ца ДаЪаДР Да сеУе си МнМЧа, ХМеЕМ ФМЙе Ца се ЪМУеСе Ч ФаПХМЕМ Фи НеСЧенМ КаПНе.

ЮаСРЕ ЪМФисПиП ФаПХМ и се сЗТПасиП. ЪМсПе ЪМЧиХаП ЙаУеКХиР ТенеСаП и ФГ ДаЪМЧРЦаП Ца ЦМЧеЦе най-ЦМУСиР МЕСРЦ МЕ ЮаСсХаЕа ТЧаСЦиР. Не ХаЕМ ДаЪСииЙЦаПи еЦни Фи Еи ЙаУМЮи: ЧсиНХи ЦСГЙнМ се ЩЧанаПи Да СаУМЕа! ЦЗСЪаПи, ЦЗСЪаПи, нМ не ГсЪеПи Ца иДЧаЦРЕ ХМПаЕа МЕ УПаЕМЕМ.

наПМЙиПМ се Ца ЪМЧиХаЕ на ЪМФМО УМУЗСа и ЦЧа ЧМЦни ЪПЗЩа.

Ч ЕМЧа ЧСеФе ГФнМЕМ ЦЙГЦЙе се ЪМХаЕеСиПМ на ЧЗСЩа на ХГЪНинаЕа ЧеЩЕМСии и ДаЪМНнаПМ УЗСДМ-УЗСДМ Ца СаДЪПиЕа ФаПХМЕМ си НеСЧенМ КаПНе. иДЕеТПиПМ еЦна ЦЗПТа ЧЗПнена ниКХа и Р наФМЕаПМ нРХМПХМ ЪЗЕи МХМПМ ЕМЧаСа!

ХМТаЕМ ХМПаЕа най-ЪМсПе се МДМЧаПа на сГКаЕа, ЮаСРЕ ЦМЧЕасаП Ца ЧДеФе ХаХЧМЕМ ФГ се ЪМПаТа.

ЦЙГЦЙеЕМ ТМ ЪМсСеОнаПМ с ЦГФиЕе:

- ЮаСБ НесЕиЕи, СаДУСаЩФе се Ца ДаЪаДР Да сеУе си МнМЧа, ХМеЕМ ФМЙе Ца се ЪМУеСе Ч ФаПХМЕМ Фи НеСЧенМ КаПНе. сЗЙаПРЧаФ, нМ Да ЕеУе ниОиНХМ не МсЕана!

ЕМТаЧа УПаЕниРЕ ЮаС СаДУСаП, Не ЦСеУМсЗХЗЕ ТМ е наЦЩиЕСиП, аПа нРФаПМ ОМ Ца сЕМСи - ЮаСсХа ЦГФа на ЦЧе не сЕаЧа!

ЦМЧМПнМ и ОасЕПиЧМ, ГФнМЕМ ЦЙГЦЙе се ЪСиУСаПМ Г ЦМФа си и ГсЕСМиПМ ТМПРФМ ЪиСКесЕЧМ, на ХМеЕМ ЪМХаниПМ и нМЧиЕе си ЪСиРЕеПи ЙаУиЕе. наТМсЕиПМ Ти УМТаЕМ. наХСаР СаДЕМЧаСиПМ ЪаСнаЕа ХМПа и СаДЦаПМ ЪМЦаСЗЮи на ЧсиНХи.

- а ЪЗХ Чие, аХМ ЙеПаеЕе, ФМЙеЕе Ца Фи ЪМЦаСиЕе еЦин нМЧ НеСЧен КаП - ЪМКеТГЧаПМ се ЕМ.

1. Ц 🡪 д ⇒ Х 🡪 к ⇒ Н 🡪 ч

ЙиЧРПМ на сЧеЕа еднМ дЙГдЙе. ЕМ УиПМ ГФнМ и СаУМЕПиЧМ и ФнМТМ МУичаПМ да ФайсЕМСи СаДни неОа. ден сПед ден иДкГЪГЧаПМ ЧеЩЕМСииЕе, кМиЕМ ЩМСаЕа ЕСГЪаПи ЪМ ЪСаКниЕе си ЕаЧани, а ЪМсПе Ти ЪМЪСаЧРПМ и Ти ЪСМдаЧаПМ ФнМТМ ЪМ-скЗЪМ. Еака си иДкаСЧаПМ ЪСеЩСанаЕа.

дЙГдЙеЕМ си иФаПМ ФаПка каСГчка, с кМРЕМ ЪСеЧМДЧаПМ ЧсичкиЕе си ЧеОи. ЕеТПеПМ Р саФ-саФичкМ! ЪМнРкМТа се МЪиЕЧаПМ да наЕМЧаСи Ч неР и ФнМТМ ЕеЙки ЪСедФеЕи, нМ наПи УиПМ дСеУнМ - не ФГ сЕиТаПи сиПиЕе да Р ЪМФСЗдне.

ЧеднЗЙ ЕМ се ДаФисПиПМ какЧМ да наЪСаЧи, Да да ФМЙе да ЪСеЧМДЧа и ЪМ-едСи неОа. ФисПиПМ, ФисПиПМ: и си иДФайсЕМСиПМ ЪаСна кМПа!

ЧечеСЕа СаУМЕПиЧМЕМ дЙГдЙе ЪМканиПМ ТМсЕи, Да да МЕЪСаДнГЧа СадМсЕнМЕМ сЗУиЕие, а на дСГТиР ден ЪМдкаСаПМ нМЧаЕа си кМПа и ЪМЕеТПиПМ на дЗПЗТ ЪЗЕ.

ЪСисЕиТнаПМ Ч един ТМПРФ ТСад и накГЪиПМ УеДУСМй ЧеЩЕМСии. наЕМЧаСиПМ Ти Ч кМПаЕа и ЪМеПМ МУСаЕнМ. нМ ЕМТаЧа ДаЪМчнаПи ЕСГднМсЕиЕе.

сЪГснаП се ФСак, ДаЧаПРП сиПен ЪМСМй: ЪМ еднМ ЧСеФе дЙГдЙеЕМ СаДУСаПМ, че е ДаТГУиПМ ЪЗЕР! кМПкМЕМ ЪМЧече ЧСеФе ФинаЧаПМ, ЕМПкМЧа ЪМ-сЕСаКнМ сЕаЧаПМ.

иДЧеднЗЙ кМПаЕа ЮМЪнаПа Ч еднМ УПаЕМ и ДаЕЗнаПа!

ФЗчиПМ се дЙГдЙеЕМ да Р иДЕеТПи, ФЗчиПМ се, нМ кМПеПаЕа й не ЪМФСЗдЧаПи! МЕчаРП се ФаПкиРЕ ЪЗЕеКесЕЧеник. ЮРПа нМО седРП Ч ЕЗФнМЕМ и чакаП да Фине нРкМй дМУЗС чМЧек, кМйЕМ да ФГ се ЪСиЕече на ЪМФМО.

нМ никМй не идЧаП.

а на сГЕСинЕа над УПаЕМЕМ ЪаднаПа ТЗсЕа ФЗТПа и МЕ Чсички сЕСани се СаДнесПМ МТПГКиЕеПнМ кЧакане. кМТаЕМ ФЗТПаЕа се СаДЪСЗснаПа, дЙГдЙеЕМ ЧидРПМ, че е ДаМУикМПенМ МЕ ЮРПа аСФиР ЙаУи!

скМСМ се ЪМРЧиП УПаЕниРЕ ЮаС.

- Еи какЧМ ЕЗСсиК Ч ФМеЕМ ЮаСсЕЧМ? - ЪМЪиЕаП ЕМй.

- ДаТГУиЩ се Ч ЕЗФнМЕМ - ЪСМФЗПЧиПМ дЙГдЙеЕМ.

- как сФееК! - СаДТнеЧиП се ЙаУМкЗЕ. - никМй нРФа ЪСаЧМ да сЕЗЪЧа Ч ФМеЕМ УПаЕМ УеД СаДСеКение!

- нМ аД не ДнаеЩ кЗде сЗФ, ЮаСБ чесЕиЕи! - ЧЗДСаДиПМ ГЪПаКенМЕМ дЙГдЙе.

- ЕМЧа не Ее МЪСаЧдаЧа! - МЕсРкЗП ЮаСРЕ, кМйЕМ наскМСМ си УиП ЪМсЕСМиП чисЕМ нМЧ ЕСЗсЕикМЧ дЧМСеЮ и сеТа се чГдеП с какЧМ ТМ МУДаЧеде. - Р да ЧидР какЧМ иФаК Ч кМПаЕа!

- ниОМ ЮеннМ - МЕЧЗСнаПМ ТМСкМЕМ дЙГдЙе. - саФМ нРкМПкМ неЪМЕСеУни неОа.

ЙаУМкЗЕ МТПедаП ПБУМЪиЕнМ ЕМЧаСа и каДаП:

- е, дМУСе. Ое Еи ЪМФМТна да си иДЕеТПиК кМПаЕа МЕ УПаЕМЕМ, нМ Ч ДаФРна Еи Ое Фи дадеК Чсички ЕеДи неОа.

дЙГдЙеЕМ СаДУСаПМ, че Ое ДаТГУи ЮРПМЕМ си УМТаЕсЕЧМ, и едЧа не ДаЪПакаПМ. нМ нРФаПМ ОМ да сЕМСи - скПМниПМ.

- УиЧа, ЮаСБ - каДаПМ ЕМ. - саФМ че Фи ЪМДЧМПи да ДаЪаДР Да сеУе си МнМЧа, кМеЕМ ФМЙе да се ЪМУеСе Ч ФаПкМЕМ Фи чеСЧенМ КаПче.

ЮаСРЕ ЪМФисПиП ФаПкМ и се сЗТПасиП. ЪМсПе ЪМЧикаП ЙаУеКкиР ТенеСаП и ФГ ДаЪМЧРдаП да дМЧеде най-дМУСиР МЕСРд МЕ ЮаСскаЕа ТЧаСдиР. че каЕМ ДаЪСииЙдаПи едни Фи Еи ЙаУМЮи: Чсички дСГЙнМ се ЩЧанаПи Да СаУМЕа! дЗСЪаПи, дЗСЪаПи, нМ не ГсЪеПи да иДЧадРЕ кМПаЕа МЕ УПаЕМЕМ.

наПМЙиПМ се да ЪМЧикаЕ на ЪМФМО УМУЗСа и дЧа ЧМдни ЪПЗЩа.

Ч ЕМЧа ЧСеФе ГФнМЕМ дЙГдЙе се ЪМкаЕеСиПМ на ЧЗСЩа на кГЪчинаЕа ЧеЩЕМСии и ДаЪМчнаПМ УЗСДМ-УЗСДМ да СаДЪПиЕа ФаПкМЕМ си чеСЧенМ КаПче. иДЕеТПиПМ една дЗПТа ЧЗПнена ниКка и Р наФМЕаПМ нРкМПкМ ЪЗЕи МкМПМ ЕМЧаСа!

кМТаЕМ кМПаЕа най-ЪМсПе се МДМЧаПа на сГКаЕа, ЮаСРЕ дМЧЕасаП да ЧДеФе какЧМЕМ ФГ се ЪМПаТа.

дЙГдЙеЕМ ТМ ЪМсСеОнаПМ с дГФиЕе:

- ЮаСБ чесЕиЕи, СаДУСаЩФе се да ДаЪаДР Да сеУе си МнМЧа, кМеЕМ ФМЙе да се ЪМУеСе Ч ФаПкМЕМ Фи чеСЧенМ КаПче. сЗЙаПРЧаФ, нМ Да ЕеУе ниОичкМ не МсЕана!

ЕМТаЧа УПаЕниРЕ ЮаС СаДУСаП, че дСеУМсЗкЗЕ ТМ е надЩиЕСиП, аПа нРФаПМ ОМ да сЕМСи - ЮаСска дГФа на дЧе не сЕаЧа!

дМЧМПнМ и ОасЕПиЧМ, ГФнМЕМ дЙГдЙе се ЪСиУСаПМ Г дМФа си и ГсЕСМиПМ ТМПРФМ ЪиСКесЕЧМ, на кМеЕМ ЪМканиПМ и нМЧиЕе си ЪСиРЕеПи ЙаУиЕе. наТМсЕиПМ Ти УМТаЕМ. накСаР СаДЕМЧаСиПМ ЪаСнаЕа кМПа и СаДдаПМ ЪМдаСЗЮи на Чсички.

- а ЪЗк Чие, акМ ЙеПаеЕе, ФМЙеЕе да Фи ЪМдаСиЕе един нМЧ чеСЧен КаП - ЪМКеТГЧаПМ се ЕМ.

1. М 🡪 о ⇒ Е 🡪 т ⇒ Ф 🡪 м

ЙиЧРПо на сЧета едно дЙГдЙе. то УиПо Гмно и СаУотПиЧо и мноТо оУичаПо да майстоСи СаДни неОа. ден сПед ден иДкГЪГЧаПо ЧеЩтоСиите, които ЩоСата тСГЪаПи Ъо ЪСаКните си таЧани, а ЪосПе Ти ЪоЪСаЧРПо и Ти ЪСодаЧаПо мноТо Ъо-скЗЪо. така си иДкаСЧаПо ЪСеЩСаната.

дЙГдЙето си имаПо маПка каСГчка, с коРто ЪСеЧоДЧаПо Чсичките си ЧеОи. теТПеПо Р сам-самичко! ЪонРкоТа се оЪитЧаПо да натоЧаСи Ч неР и мноТо теЙки ЪСедмети, но наПи УиПо дСеУно - не мГ стиТаПи сиПите да Р ЪомСЗдне.

ЧеднЗЙ то се ДамисПиПо какЧо да наЪСаЧи, Да да моЙе да ЪСеЧоДЧа и Ъо-едСи неОа. мисПиПо, мисПиПо: и си иДмайстоСиПо ЪаСна коПа!

ЧечеСта СаУотПиЧото дЙГдЙе ЪоканиПо Тости, Да да отЪСаДнГЧа Садостното сЗУитие, а на дСГТиР ден ЪодкаСаПо ноЧата си коПа и ЪотеТПиПо на дЗПЗТ ЪЗт.

ЪСистиТнаПо Ч един ТоПРм ТСад и накГЪиПо УеДУСой ЧеЩтоСии. натоЧаСиПо Ти Ч коПата и ЪоеПо оУСатно. но тоТаЧа ДаЪочнаПи тСГдностите.

сЪГснаП се мСак, ДаЧаПРП сиПен ЪоСой: Ъо едно ЧСеме дЙГдЙето СаДУСаПо, че е ДаТГУиПо ЪЗтР! коПкото ЪоЧече ЧСеме минаЧаПо, тоПкоЧа Ъо-стСаКно стаЧаПо.

иДЧеднЗЙ коПата ЮоЪнаПа Ч едно УПато и ДатЗнаПа!

мЗчиПо се дЙГдЙето да Р иДтеТПи, мЗчиПо се, но коПеПата й не ЪомСЗдЧаПи! отчаРП се маПкиРт ЪЗтеКестЧеник. ЮРПа ноО седРП Ч тЗмното и чакаП да мине нРкой доУЗС чоЧек, който да мГ се ЪСитече на ЪомоО.

но никой не идЧаП.

а на сГтСинта над УПатото ЪаднаПа ТЗста мЗТПа и от Чсички стСани се СаДнесПо оТПГКитеПно кЧакане. коТато мЗТПата се СаДЪСЗснаПа, дЙГдЙето ЧидРПо, че е ДаоУикоПено от ЮРПа аСмиР ЙаУи!

скоСо се ЪоРЧиП УПатниРт ЮаС.

- ти какЧо тЗСсиК Ч моето ЮаСстЧо? - ЪоЪитаП той.

- ДаТГУиЩ се Ч тЗмното - ЪСомЗПЧиПо дЙГдЙето.

- как смееК! - СаДТнеЧиП се ЙаУокЗт. - никой нРма ЪСаЧо да стЗЪЧа Ч моето УПато УеД СаДСеКение!

- но аД не ДнаеЩ кЗде сЗм, ЮаСБ честити! - ЧЗДСаДиПо ГЪПаКеното дЙГдЙе.

- тоЧа не те оЪСаЧдаЧа! - отсРкЗП ЮаСРт, който наскоСо си УиП ЪостСоиП чисто ноЧ тСЗстикоЧ дЧоСеЮ и сеТа се чГдеП с какЧо То оУДаЧеде. - Р да ЧидР какЧо имаК Ч коПата!

- ниОо Юенно - отЧЗСнаПо ТоСкото дЙГдЙе. - само нРкоПко неЪотСеУни неОа.

ЙаУокЗт оТПедаП ПБУоЪитно тоЧаСа и каДаП:

- е, доУСе. Ое ти ЪомоТна да си иДтеТПиК коПата от УПатото, но Ч ДамРна ти Ое ми дадеК Чсички теДи неОа.

дЙГдЙето СаДУСаПо, че Ое ДаТГУи ЮРПото си УоТатстЧо, и едЧа не ДаЪПакаПо. но нРмаПо Оо да стоСи - скПониПо.

- УиЧа, ЮаСБ - каДаПо то. - само че ми ЪоДЧоПи да ДаЪаДР Да сеУе си оноЧа, което моЙе да се ЪоУеСе Ч маПкото ми чеСЧено КаПче.

ЮаСРт ЪомисПиП маПко и се сЗТПасиП. ЪосПе ЪоЧикаП ЙаУеКкиР ТенеСаП и мГ ДаЪоЧРдаП да доЧеде най-доУСиР отСРд от ЮаСската ТЧаСдиР. че като ДаЪСииЙдаПи едни ми ти ЙаУоЮи: Чсички дСГЙно се ЩЧанаПи Да СаУота! дЗСЪаПи, дЗСЪаПи, но не ГсЪеПи да иДЧадРт коПата от УПатото.

наПоЙиПо се да ЪоЧикат на ЪомоО УоУЗСа и дЧа Чодни ЪПЗЩа.

Ч тоЧа ЧСеме Гмното дЙГдЙе се ЪокатеСиПо на ЧЗСЩа на кГЪчината ЧеЩтоСии и ДаЪочнаПо УЗСДо-УЗСДо да СаДЪПита маПкото си чеСЧено КаПче. иДтеТПиПо една дЗПТа ЧЗПнена ниКка и Р намотаПо нРкоПко ЪЗти окоПо тоЧаСа!

коТато коПата най-ЪосПе се оДоЧаПа на сГКата, ЮаСРт доЧтасаП да ЧДеме какЧото мГ се ЪоПаТа.

дЙГдЙето То ЪосСеОнаПо с дГмите:

- ЮаСБ честити, СаДУСаЩме се да ДаЪаДР Да сеУе си оноЧа, което моЙе да се ЪоУеСе Ч маПкото ми чеСЧено КаПче. сЗЙаПРЧам, но Да теУе ниОичко не остана!

тоТаЧа УПатниРт ЮаС СаДУСаП, че дСеУосЗкЗт То е надЩитСиП, аПа нРмаПо Оо да стоСи - ЮаСска дГма на дЧе не стаЧа!

доЧоПно и ОастПиЧо, Гмното дЙГдЙе се ЪСиУСаПо Г дома си и ГстСоиПо ТоПРмо ЪиСКестЧо, на което ЪоканиПо и ноЧите си ЪСиРтеПи ЙаУите. наТостиПо Ти УоТато. накСаР СаДтоЧаСиПо ЪаСната коПа и СаДдаПо ЪодаСЗЮи на Чсички.

- а ЪЗк Чие, ако ЙеПаете, моЙете да ми ЪодаСите един ноЧ чеСЧен КаП - ЪоКеТГЧаПо се то.

1. Ч 🡪 в ⇒ Й 🡪 ж ⇒ Т 🡪 г

живРПо на света едно джГдже. то УиПо Гмно и СаУотПиво и много оУичаПо да майстоСи СаДни неОа. ден сПед ден иДкГЪГваПо веЩтоСиите, които ЩоСата тСГЪаПи Ъо ЪСаКните си тавани, а ЪосПе ги ЪоЪСавРПо и ги ЪСодаваПо много Ъо-скЗЪо. така си иДкаСваПо ЪСеЩСаната.

джГджето си имаПо маПка каСГчка, с коРто ЪСевоДваПо всичките си веОи. тегПеПо Р сам-самичко! ЪонРкога се оЪитваПо да натоваСи в неР и много тежки ЪСедмети, но наПи УиПо дСеУно - не мГ стигаПи сиПите да Р ЪомСЗдне.

веднЗж то се ДамисПиПо какво да наЪСави, Да да може да ЪСевоДва и Ъо-едСи неОа. мисПиПо, мисПиПо: и си иДмайстоСиПо ЪаСна коПа!

вечеСта СаУотПивото джГдже ЪоканиПо гости, Да да отЪСаДнГва Садостното сЗУитие, а на дСГгиР ден ЪодкаСаПо новата си коПа и ЪотегПиПо на дЗПЗг ЪЗт.

ЪСистигнаПо в един гоПРм гСад и накГЪиПо УеДУСой веЩтоСии. натоваСиПо ги в коПата и ЪоеПо оУСатно. но тогава ДаЪочнаПи тСГдностите.

сЪГснаП се мСак, ДаваПРП сиПен ЪоСой: Ъо едно вСеме джГджето СаДУСаПо, че е ДагГУиПо ЪЗтР! коПкото Ъовече вСеме минаваПо, тоПкова Ъо-стСаКно ставаПо.

иДведнЗж коПата ЮоЪнаПа в едно УПато и ДатЗнаПа!

мЗчиПо се джГджето да Р иДтегПи, мЗчиПо се, но коПеПата й не ЪомСЗдваПи! отчаРП се маПкиРт ЪЗтеКественик. ЮРПа ноО седРП в тЗмното и чакаП да мине нРкой доУЗС човек, който да мГ се ЪСитече на ЪомоО.

но никой не идваП.

а на сГтСинта над УПатото ЪаднаПа гЗста мЗгПа и от всички стСани се СаДнесПо огПГКитеПно квакане. когато мЗгПата се СаДЪСЗснаПа, джГджето видРПо, че е ДаоУикоПено от ЮРПа аСмиР жаУи!

скоСо се ЪоРвиП УПатниРт ЮаС.

- ти какво тЗСсиК в моето ЮаСство? - ЪоЪитаП той.

- ДагГУиЩ се в тЗмното - ЪСомЗПвиПо джГджето.

- как смееК! - СаДгневиП се жаУокЗт. - никой нРма ЪСаво да стЗЪва в моето УПато УеД СаДСеКение!

- но аД не ДнаеЩ кЗде сЗм, ЮаСБ честити! - вЗДСаДиПо ГЪПаКеното джГдже.

- това не те оЪСавдава! - отсРкЗП ЮаСРт, който наскоСо си УиП ЪостСоиП чисто нов тСЗстиков двоСеЮ и сега се чГдеП с какво го оУДаведе. - Р да видР какво имаК в коПата!

- ниОо Юенно - отвЗСнаПо гоСкото джГдже. - само нРкоПко неЪотСеУни неОа.

жаУокЗт огПедаП ПБУоЪитно товаСа и каДаП:

- е, доУСе. Ое ти Ъомогна да си иДтегПиК коПата от УПатото, но в ДамРна ти Ое ми дадеК всички теДи неОа.

джГджето СаДУСаПо, че Ое ДагГУи ЮРПото си Уогатство, и едва не ДаЪПакаПо. но нРмаПо Оо да стоСи - скПониПо.

- Уива, ЮаСБ - каДаПо то. - само че ми ЪоДвоПи да ДаЪаДР Да сеУе си онова, което може да се ЪоУеСе в маПкото ми чеСвено КаПче.

ЮаСРт ЪомисПиП маПко и се сЗгПасиП. ЪосПе ЪовикаП жаУеКкиР генеСаП и мГ ДаЪовРдаП да доведе най-доУСиР отСРд от ЮаСската гваСдиР. че като ДаЪСииждаПи едни ми ти жаУоЮи: всички дСГжно се ЩванаПи Да СаУота! дЗСЪаПи, дЗСЪаПи, но не ГсЪеПи да иДвадРт коПата от УПатото.

наПожиПо се да Ъовикат на ЪомоО УоУЗСа и два водни ЪПЗЩа.

в това вСеме Гмното джГдже се ЪокатеСиПо на вЗСЩа на кГЪчината веЩтоСии и ДаЪочнаПо УЗСДо-УЗСДо да СаДЪПита маПкото си чеСвено КаПче. иДтегПиПо една дЗПга вЗПнена ниКка и Р намотаПо нРкоПко ЪЗти окоПо товаСа!

когато коПата най-ЪосПе се оДоваПа на сГКата, ЮаСРт довтасаП да вДеме каквото мГ се ЪоПага.

джГджето го ЪосСеОнаПо с дГмите:

- ЮаСБ честити, СаДУСаЩме се да ДаЪаДР Да сеУе си онова, което може да се ЪоУеСе в маПкото ми чеСвено КаПче. сЗжаПРвам, но Да теУе ниОичко не остана!

тогава УПатниРт ЮаС СаДУСаП, че дСеУосЗкЗт го е надЩитСиП, аПа нРмаПо Оо да стоСи - ЮаСска дГма на две не става!

довоПно и ОастПиво, Гмното джГдже се ЪСиУСаПо Г дома си и ГстСоиПо гоПРмо ЪиСКество, на което ЪоканиПо и новите си ЪСиРтеПи жаУите. нагостиПо ги Уогато. накСаР СаДтоваСиПо ЪаСната коПа и СаДдаПо ЪодаСЗЮи на всички.

- а ЪЗк вие, ако жеПаете, можете да ми ЪодаСите един нов чеСвен КаП - ЪоКегГваПо се то.

1. П 🡪 л ⇒ Ъ 🡪 п ⇒ Р 🡪 я

живяло на света едно джГдже. то Уило Гмно и СаУотливо и много оУичало да майстоСи СаДни неОа. ден след ден иДкГпГвало веЩтоСиите, които ЩоСата тСГпали по пСаКните си тавани, а после ги попСавяло и ги пСодавало много по-скЗпо. така си иДкаСвало пСеЩСаната.

джГджето си имало малка каСГчка, с която пСевоДвало всичките си веОи. теглело я сам-самичко! понякога се опитвало да натоваСи в нея и много тежки пСедмети, но нали Уило дСеУно - не мГ стигали силите да я помСЗдне.

веднЗж то се Дамислило какво да напСави, Да да може да пСевоДва и по-едСи неОа. мислило, мислило: и си иДмайстоСило паСна кола!

вечеСта СаУотливото джГдже поканило гости, Да да отпСаДнГва Садостното сЗУитие, а на дСГгия ден подкаСало новата си кола и потеглило на дЗлЗг пЗт.

пСистигнало в един голям гСад и накГпило УеДУСой веЩтоСии. натоваСило ги в колата и поело оУСатно. но тогава Дапочнали тСГдностите.

спГснал се мСак, Давалял силен поСой: по едно вСеме джГджето СаДУСало, че е ДагГУило пЗтя! колкото повече вСеме минавало, толкова по-стСаКно ставало.

иДведнЗж колата Юопнала в едно Улато и ДатЗнала!

мЗчило се джГджето да я иДтегли, мЗчило се, но колелата й не помСЗдвали! отчаял се малкият пЗтеКественик. Юяла ноО седял в тЗмното и чакал да мине някой доУЗС човек, който да мГ се пСитече на помоО.

но никой не идвал.

а на сГтСинта над Улатото паднала гЗста мЗгла и от всички стСани се СаДнесло оглГКително квакане. когато мЗглата се СаДпСЗснала, джГджето видяло, че е ДаоУиколено от Юяла аСмия жаУи!

скоСо се появил Улатният ЮаС.

- ти какво тЗСсиК в моето ЮаСство? - попитал той.

- ДагГУиЩ се в тЗмното - пСомЗлвило джГджето.

- как смееК! - СаДгневил се жаУокЗт. - никой няма пСаво да стЗпва в моето Улато УеД СаДСеКение!

- но аД не ДнаеЩ кЗде сЗм, ЮаСБ честити! - вЗДСаДило ГплаКеното джГдже.

- това не те опСавдава! - отсякЗл ЮаСят, който наскоСо си Уил постСоил чисто нов тСЗстиков двоСеЮ и сега се чГдел с какво го оУДаведе. - я да видя какво имаК в колата!

- ниОо Юенно - отвЗСнало гоСкото джГдже. - само няколко непотСеУни неОа.

жаУокЗт огледал лБУопитно товаСа и каДал:

- е, доУСе. Ое ти помогна да си иДтеглиК колата от Улатото, но в Дамяна ти Ое ми дадеК всички теДи неОа.

джГджето СаДУСало, че Ое ДагГУи Юялото си Уогатство, и едва не Даплакало. но нямало Оо да стоСи - склонило.

- Уива, ЮаСБ - каДало то. - само че ми поДволи да ДапаДя Да сеУе си онова, което може да се поУеСе в малкото ми чеСвено Калче.

ЮаСят помислил малко и се сЗгласил. после повикал жаУеКкия генеСал и мГ Даповядал да доведе най-доУСия отСяд от ЮаСската гваСдия. че като ДапСииждали едни ми ти жаУоЮи: всички дСГжно се Щванали Да СаУота! дЗСпали, дЗСпали, но не Гспели да иДвадят колата от Улатото.

наложило се да повикат на помоО УоУЗСа и два водни плЗЩа.

в това вСеме Гмното джГдже се покатеСило на вЗСЩа на кГпчината веЩтоСии и Дапочнало УЗСДо-УЗСДо да СаДплита малкото си чеСвено Калче. иДтеглило една дЗлга вЗлнена ниКка и я намотало няколко пЗти около товаСа!

когато колата най-после се оДовала на сГКата, ЮаСят довтасал да вДеме каквото мГ се полага.

джГджето го посСеОнало с дГмите:

- ЮаСБ честити, СаДУСаЩме се да ДапаДя Да сеУе си онова, което може да се поУеСе в малкото ми чеСвено Калче. сЗжалявам, но Да теУе ниОичко не остана!

тогава Улатният ЮаС СаДУСал, че дСеУосЗкЗт го е надЩитСил, ала нямало Оо да стоСи - ЮаСска дГма на две не става!

доволно и Оастливо, Гмното джГдже се пСиУСало Г дома си и ГстСоило голямо пиСКество, на което поканило и новите си пСиятели жаУите. нагостило ги Уогато. накСая СаДтоваСило паСната кола и СаДдало подаСЗЮи на всички.

- а пЗк вие, ако желаете, можете да ми подаСите един нов чеСвен Кал - поКегГвало се то.

1. Г 🡪 у ⇒ У 🡪 б ⇒ З 🡪 ъ

живяло на света едно джудже. то било умно и Саботливо и много обичало да майстоСи СаДни неОа. ден след ден иДкупувало веЩтоСиите, които ЩоСата тСупали по пСаКните си тавани, а после ги попСавяло и ги пСодавало много по-скъпо. така си иДкаСвало пСеЩСаната.

джуджето си имало малка каСучка, с която пСевоДвало всичките си веОи. теглело я сам-самичко! понякога се опитвало да натоваСи в нея и много тежки пСедмети, но нали било дСебно - не му стигали силите да я помСъдне.

веднъж то се Дамислило какво да напСави, Да да може да пСевоДва и по-едСи неОа. мислило, мислило: и си иДмайстоСило паСна кола!

вечеСта Саботливото джудже поканило гости, Да да отпСаДнува Садостното събитие, а на дСугия ден подкаСало новата си кола и потеглило на дълъг път.

пСистигнало в един голям гСад и накупило беДбСой веЩтоСии. натоваСило ги в колата и поело обСатно. но тогава Дапочнали тСудностите.

спуснал се мСак, Давалял силен поСой: по едно вСеме джуджето СаДбСало, че е Дагубило пътя! колкото повече вСеме минавало, толкова по-стСаКно ставало.

иДведнъж колата Юопнала в едно блато и Датънала!

мъчило се джуджето да я иДтегли, мъчило се, но колелата й не помСъдвали! отчаял се малкият пътеКественик. Юяла ноО седял в тъмното и чакал да мине някой добъС човек, който да му се пСитече на помоО.

но никой не идвал.

а на сутСинта над блатото паднала гъста мъгла и от всички стСани се СаДнесло оглуКително квакане. когато мъглата се СаДпСъснала, джуджето видяло, че е Даобиколено от Юяла аСмия жаби!

скоСо се появил блатният ЮаС.

- ти какво тъСсиК в моето ЮаСство? - попитал той.

- ДагубиЩ се в тъмното - пСомълвило джуджето.

- как смееК! - СаДгневил се жабокът. - никой няма пСаво да стъпва в моето блато беД СаДСеКение!

- но аД не ДнаеЩ къде съм, ЮаСБ честити! - въДСаДило уплаКеното джудже.

- това не те опСавдава! - отсякъл ЮаСят, който наскоСо си бил постСоил чисто нов тСъстиков двоСеЮ и сега се чудел с какво го обДаведе. - я да видя какво имаК в колата!

- ниОо Юенно - отвъСнало гоСкото джудже. - само няколко непотСебни неОа.

жабокът огледал лБбопитно товаСа и каДал:

- е, добСе. Ое ти помогна да си иДтеглиК колата от блатото, но в Дамяна ти Ое ми дадеК всички теДи неОа.

джуджето СаДбСало, че Ое Дагуби Юялото си богатство, и едва не Даплакало. но нямало Оо да стоСи - склонило.

- бива, ЮаСБ - каДало то. - само че ми поДволи да ДапаДя Да себе си онова, което може да се побеСе в малкото ми чеСвено Калче.

ЮаСят помислил малко и се съгласил. после повикал жабеКкия генеСал и му Даповядал да доведе най-добСия отСяд от ЮаСската гваСдия. че като ДапСииждали едни ми ти жабоЮи: всички дСужно се Щванали Да Сабота! дъСпали, дъСпали, но не успели да иДвадят колата от блатото.

наложило се да повикат на помоО бобъСа и два водни плъЩа.

в това вСеме умното джудже се покатеСило на въСЩа на купчината веЩтоСии и Дапочнало бъСДо-бъСДо да СаДплита малкото си чеСвено Калче. иДтеглило една дълга вълнена ниКка и я намотало няколко пъти около товаСа!

когато колата най-после се оДовала на суКата, ЮаСят довтасал да вДеме каквото му се полага.

джуджето го посСеОнало с думите:

- ЮаСБ честити, СаДбСаЩме се да ДапаДя Да себе си онова, което може да се побеСе в малкото ми чеСвено Калче. съжалявам, но Да тебе ниОичко не остана!

тогава блатният ЮаС СаДбСал, че дСебосъкът го е надЩитСил, ала нямало Оо да стоСи - ЮаСска дума на две не става!

доволно и Оастливо, умното джудже се пСибСало у дома си и устСоило голямо пиСКество, на което поканило и новите си пСиятели жабите. нагостило ги богато. накСая СаДтоваСило паСната кола и СаДдало подаСъЮи на всички.

- а пък вие, ако желаете, можете да ми подаСите един нов чеСвен Кал - поКегувало се то.

1. С 🡪 р ⇒ Ю 🡪 ц ⇒ Щ 🡪 х

живяло на света едно джудже. то било умно и работливо и много обичало да майстори раДни неОа. ден след ден иДкупувало вехториите, които хората трупали по праКните си тавани, а после ги поправяло и ги продавало много по-скъпо. така си иДкарвало прехраната.

джуджето си имало малка каручка, с която превоДвало всичките си веОи. теглело я сам-самичко! понякога се опитвало да натовари в нея и много тежки предмети, но нали било дребно - не му стигали силите да я помръдне.

веднъж то се Дамислило какво да направи, Да да може да превоДва и по-едри неОа. мислило, мислило: и си иДмайсторило парна кола!

вечерта работливото джудже поканило гости, Да да отпраДнува радостното събитие, а на другия ден подкарало новата си кола и потеглило на дълъг път.

пристигнало в един голям град и накупило беДброй вехтории. натоварило ги в колата и поело обратно. но тогава Дапочнали трудностите.

спуснал се мрак, Давалял силен порой: по едно време джуджето раДбрало, че е Дагубило пътя! колкото повече време минавало, толкова по-страКно ставало.

иДведнъж колата цопнала в едно блато и Датънала!

мъчило се джуджето да я иДтегли, мъчило се, но колелата й не помръдвали! отчаял се малкият пътеКественик. цяла ноО седял в тъмното и чакал да мине някой добър човек, който да му се притече на помоО.

но никой не идвал.

а на сутринта над блатото паднала гъста мъгла и от всички страни се раДнесло оглуКително квакане. когато мъглата се раДпръснала, джуджето видяло, че е Даобиколено от цяла армия жаби!

скоро се появил блатният цар.

- ти какво търсиК в моето царство? - попитал той.

- Дагубих се в тъмното - промълвило джуджето.

- как смееК! - раДгневил се жабокът. - никой няма право да стъпва в моето блато беД раДреКение!

- но аД не Днаех къде съм, царБ честити! - въДраДило уплаКеното джудже.

- това не те оправдава! - отсякъл царят, който наскоро си бил построил чисто нов тръстиков дворец и сега се чудел с какво го обДаведе. - я да видя какво имаК в колата!

- ниОо ценно - отвърнало горкото джудже. - само няколко непотребни неОа.

жабокът огледал лБбопитно товара и каДал:

- е, добре. Ое ти помогна да си иДтеглиК колата от блатото, но в Дамяна ти Ое ми дадеК всички теДи неОа.

джуджето раДбрало, че Ое Дагуби цялото си богатство, и едва не Даплакало. но нямало Оо да стори - склонило.

- бива, царБ - каДало то. - само че ми поДволи да ДапаДя Да себе си онова, което може да се побере в малкото ми червено Калче.

царят помислил малко и се съгласил. после повикал жабеКкия генерал и му Даповядал да доведе най-добрия отряд от царската гвардия. че като Даприиждали едни ми ти жабоци: всички дружно се хванали Да работа! дърпали, дърпали, но не успели да иДвадят колата от блатото.

наложило се да повикат на помоО бобъра и два водни плъха.

в това време умното джудже се покатерило на върха на купчината вехтории и Дапочнало бърДо-бърДо да раДплита малкото си червено Калче. иДтеглило една дълга вълнена ниКка и я намотало няколко пъти около товара!

когато колата най-после се оДовала на суКата, царят довтасал да вДеме каквото му се полага.

джуджето го посреОнало с думите:

- царБ честити, раДбрахме се да ДапаДя Да себе си онова, което може да се побере в малкото ми червено Калче. съжалявам, но Да тебе ниОичко не остана!

тогава блатният цар раДбрал, че дребосъкът го е надхитрил, ала нямало Оо да стори - царска дума на две не става!

доволно и Оастливо, умното джудже се прибрало у дома си и устроило голямо пирКество, на което поканило и новите си приятели жабите. нагостило ги богато. накрая раДтоварило парната кола и раДдало подаръци на всички.

- а пък вие, ако желаете, можете да ми подарите един нов червен Кал - поКегувало се то.

1. О 🡪 щ ⇒ Д 🡪 з ⇒ К 🡪 ш

живяло на света едно джудже. то било умно и работливо и много обичало да майстори разни неща. ден след ден изкупувало вехториите, които хората трупали по прашните си тавани, а после ги поправяло и ги продавало много по-скъпо. така си изкарвало прехраната.

джуджето си имало малка каручка, с която превозвало всичките си вещи. теглело я сам-самичко! понякога се опитвало да натовари в нея и много тежки предмети, но нали било дребно - не му стигали силите да я помръдне.

веднъж то се замислило какво да направи, за да може да превозва и по-едри неща. мислило, мислило: и си измайсторило парна кола!

вечерта работливото джудже поканило гости, за да отпразнува радостното събитие, а на другия ден подкарало новата си кола и потеглило на дълъг път.

пристигнало в един голям град и накупило безброй вехтории. натоварило ги в колата и поело обратно. но тогава започнали трудностите.

спуснал се мрак, завалял силен порой: по едно време джуджето разбрало, че е загубило пътя! колкото повече време минавало, толкова по-страшно ставало.

изведнъж колата цопнала в едно блато и затънала!

мъчило се джуджето да я изтегли, мъчило се, но колелата й не помръдвали! отчаял се малкият пътешественик. цяла нощ седял в тъмното и чакал да мине някой добър човек, който да му се притече на помощ.

но никой не идвал.

а на сутринта над блатото паднала гъста мъгла и от всички страни се разнесло оглушително квакане. когато мъглата се разпръснала, джуджето видяло, че е заобиколено от цяла армия жаби!

скоро се появил блатният цар.

- ти какво търсиш в моето царство? - попитал той.

- загубих се в тъмното - промълвило джуджето.

- как смееш! - разгневил се жабокът. - никой няма право да стъпва в моето блато без разрешение!

- но аз не знаех къде съм, царБ честити! - възразило уплашеното джудже.

- това не те оправдава! - отсякъл царят, който наскоро си бил построил чисто нов тръстиков дворец и сега се чудел с какво го обзаведе. - я да видя какво имаш в колата!

- нищо ценно - отвърнало горкото джудже. - само няколко непотребни неща.

жабокът огледал лБбопитно товара и казал:

- е, добре. ще ти помогна да си изтеглиш колата от блатото, но в замяна ти ще ми дадеш всички тези неща.

джуджето разбрало, че ще загуби цялото си богатство, и едва не заплакало. но нямало що да стори - склонило.

- бива, царБ - казало то. - само че ми позволи да запазя за себе си онова, което може да се побере в малкото ми червено шалче.

царят помислил малко и се съгласил. после повикал жабешкия генерал и му заповядал да доведе най-добрия отряд от царската гвардия. че като заприиждали едни ми ти жабоци: всички дружно се хванали за работа! дърпали, дърпали, но не успели да извадят колата от блатото.

наложило се да повикат на помощ бобъра и два водни плъха.

в това време умното джудже се покатерило на върха на купчината вехтории и започнало бързо-бързо да разплита малкото си червено шалче. изтеглило една дълга вълнена нишка и я намотало няколко пъти около товара!

когато колата най-после се озовала на сушата, царят довтасал да вземе каквото му се полага.

джуджето го посрещнало с думите:

- царБ честити, разбрахме се да запазя за себе си онова, което може да се побере в малкото ми червено шалче. съжалявам, но за тебе нищичко не остана!

тогава блатният цар разбрал, че дребосъкът го е надхитрил, ала нямало що да стори - царска дума на две не става!

доволно и щастливо, умното джудже се прибрало у дома си и устроило голямо пиршество, на което поканило и новите си приятели жабите. нагостило ги богато. накрая разтоварило парната кола и раздало подаръци на всички.

- а пък вие, ако желаете, можете да ми подарите един нов червен шал - пошегувало се то.

1. Б 🡪 ю ⇒ ь 🡪 0 ⇒ И 🡪 0

живяло на света едно джудже. то било умно и работливо и много обичало да майстори разни неща. ден след ден изкупувало вехториите, които хората трупали по прашните си тавани, а после ги поправяло и ги продавало много по-скъпо. така си изкарвало прехраната.

джуджето си имало малка каручка, с която превозвало всичките си вещи. теглело я сам-самичко! понякога се опитвало да натовари в нея и много тежки предмети, но нали било дребно - не му стигали силите да я помръдне.

веднъж то се замислило какво да направи, за да може да превозва и по-едри неща. мислило, мислило: и си измайсторило парна кола!

вечерта работливото джудже поканило гости, за да отпразнува радостното събитие, а на другия ден подкарало новата си кола и потеглило на дълъг път.

пристигнало в един голям град и накупило безброй вехтории. натоварило ги в колата и поело обратно. но тогава започнали трудностите.

спуснал се мрак, завалял силен порой: по едно време джуджето разбрало, че е загубило пътя! колкото повече време минавало, толкова по-страшно ставало.

изведнъж колата цопнала в едно блато и затънала!

мъчило се джуджето да я изтегли, мъчило се, но колелата й не помръдвали! отчаял се малкият пътешественик. цяла нощ седял в тъмното и чакал да мине някой добър човек, който да му се притече на помощ.

но никой не идвал.

а на сутринта над блатото паднала гъста мъгла и от всички страни се разнесло оглушително квакане. когато мъглата се разпръснала, джуджето видяло, че е заобиколено от цяла армия жаби!

скоро се появил блатният цар.

- ти какво търсиш в моето царство? - попитал той.

- загубих се в тъмното - промълвило джуджето.

- как смееш! - разгневил се жабокът. - никой няма право да стъпва в моето блато без разрешение!

- но аз не знаех къде съм, царю честити! - възразило уплашеното джудже.

- това не те оправдава! - отсякъл царят, който наскоро си бил построил чисто нов тръстиков дворец и сега се чудел с какво го обзаведе. - я да видя какво имаш в колата!

- нищо ценно - отвърнало горкото джудже. - само няколко непотребни неща.

жабокът огледал любопитно товара и казал:

- е, добре. ще ти помогна да си изтеглиш колата от блатото, но в замяна ти ще ми дадеш всички тези неща.

джуджето разбрало, че ще загуби цялото си богатство, и едва не заплакало. но нямало що да стори - склонило.

- бива, царю - казало то. - само че ми позволи да запазя за себе си онова, което може да се побере в малкото ми червено шалче.

царят помислил малко и се съгласил. после повикал жабешкия генерал и му заповядал да доведе най-добрия отряд от царската гвардия. че като заприиждали едни ми ти жабоци: всички дружно се хванали за работа! дърпали, дърпали, но не успели да извадят колата от блатото.

наложило се да повикат на помощ бобъра и два водни плъха.

в това време умното джудже се покатерило на върха на купчината вехтории и започнало бързо-бързо да разплита малкото си червено шалче. изтеглило една дълга вълнена нишка и я намотало няколко пъти около товара!

когато колата най-после се озовала на сушата, царят довтасал да вземе каквото му се полага.

джуджето го посрещнало с думите:

- царю честити, разбрахме се да запазя за себе си онова, което може да се побере в малкото ми червено шалче. съжалявам, но за тебе нищичко не остана!

тогава блатният цар разбрал, че дребосъкът го е надхитрил, ала нямало що да стори - царска дума на две не става!

доволно и щастливо, умното джудже се прибрало у дома си и устроило голямо пиршество, на което поканило и новите си приятели жабите. нагостило ги богато. накрая разтоварило парната кола и раздало подаръци на всички.

- а пък вие, ако желаете, можете да ми подарите един нов червен шал - пошегувало се то.

**Литература:**

1. <https://nikolay.it/Blog/2011/08/%D0%90%D0%BD%D0%B0%D0%BB%D0%B8%D0%B7-%D0%BD%D0%B0-%D0%B1%D1%8A%D0%BB%D0%B3%D0%B0%D1%80%D1%81%D0%BA%D0%B8%D1%8F-%D0%B5%D0%B7%D0%B8%D0%BA-%D1%87%D1%80%D0%B5%D0%B7-Wikipedia/3>

1. <https://www2.rivier.edu/faculty/vriabov/cs572aweb/Assignments/CrackingClassicCiphers.htm>
2. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.1640&rep=rep1&type=pdf>
3. <https://www.uobabylon.edu.iq/eprints/paper_11_1576_649.pdf>
4. <https://research.bangor.ac.uk/portal/files/20276059/2018_An_Automatic_cryptanalysis_of_simple_substitution.pdf>
5. <https://www2.rivier.edu/faculty/vriabov/cs572aweb/Assignments/CrackingClassicCiphers.htm>
6. <http://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.698.1640&rep=rep1&type=pdf>
7. <http://cse.ucdenver.edu/~rhilton/docs/Cryptanalysis-Against-Monosub-Ciphers.pdf>