kaspersky.academy

Лекция 2

Криптоанализ шифра Цезаря

Онлайн-курс по математике в информационной безопасности

kaspersky.academy

Лекция 2: Криптоанализ шифра Цезаря

Продолжаем говорить о шифрах простой замены – рассмотрим одноалфавитный шифр подстановки, узнаем, что такое частота встречаемости букв и как она используется в методе частотного анализа для взлома шифров.

Но перед тем как уйти в дебри теории, давайте посмотрим на рисунки человечков.

План лекции:

Пляшущие человечки

Однажды Шерлоку Холмсу попали в руки записки с рисунками пляшущих человечков. В это время Холмс как раз проводил расследование, и расшифровка записок очень бы ему в этом помогла. Всего записок было 5.

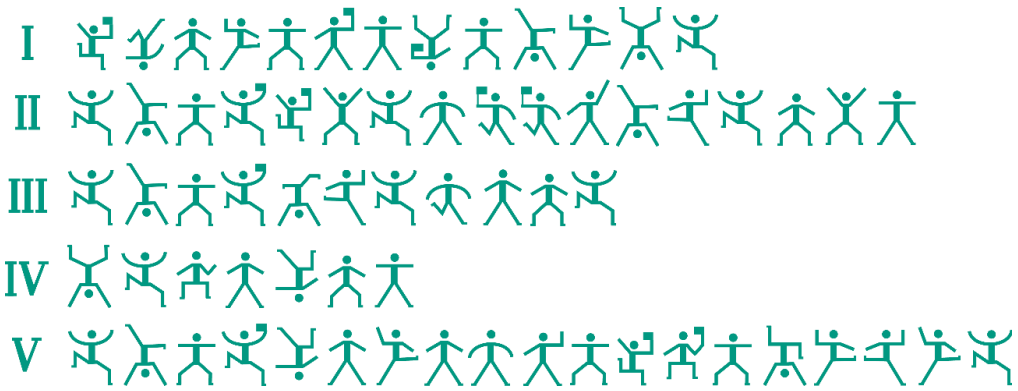

Рисунок 1: Рисунки человечков

Что есть у Шерлока? Он догадывается, что столкнулся с **шифром простой замены (или одноалфавитным шифром подстановки):** каждый символ алфавита преступник заменил на человечка. Алфавит, составленный из пиктограмм человечков – это **алфавит замены**. Некоторые человечки держат флажки – скорее всего, флажок у человечка означает конец слова.

Так как дополнительной информации у Шерлока Холмса не было, он решил взламывать криптограмму **методом угадывания**.

Как работает метод угадывания:

1. Предполагаем значение какого-то слова криптограммы.
2. Получаем соответствие между буквами открытого текста и буквами алфавита замены.
3. Заменяем известные буквы по всему тексту.

Шерлок Холмс всматривался в записки и увидел, что вторая, третья и пятая записки начинаются с одинакового слова из четырех букв. Первое предположение Холмса – это слово означает имя главной героини, Илси. Это же элементарно – преступник обращается по имени к тому, кому пишет!

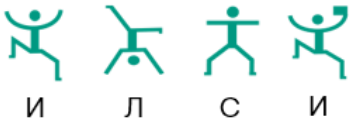

Рисунок 2: ИЛСИ

Теперь у Шерлока есть буквы И, Л, С. Он подставляет их во все тексты.

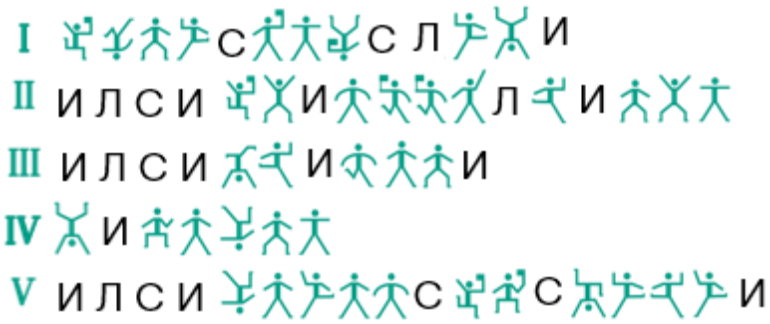

Рисунок 3: Подстановка И, Л, С

Информации для разгадки все еще мало, а поэтому угадываем дальше.

В третьей записке всего два слова. Первое слово – ИЛСИ. Возможно, второе – это какой-то глагол (героиню просят что-то сделать). Слово длинное и в нем есть две буквы И. По смыслу подходит слово ПРИХОДИ. И так Холмс получил буквы П, Р, Х, О, Д.

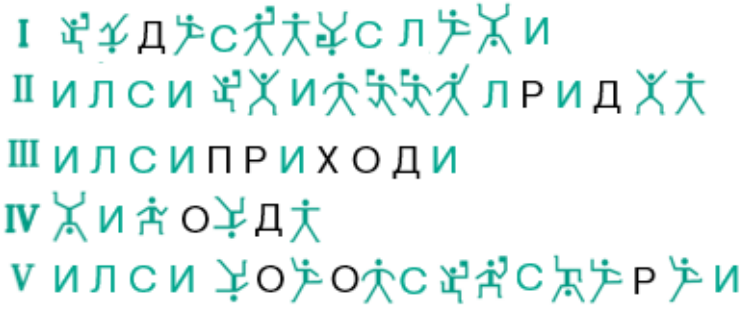

Рисунок 4: Подстановка П, Р, Х, О, Д

Третья записка – это ответ Илси из одного слова. В слове есть буквы И, О, Д. Возможно, это слово НИКОГДА.

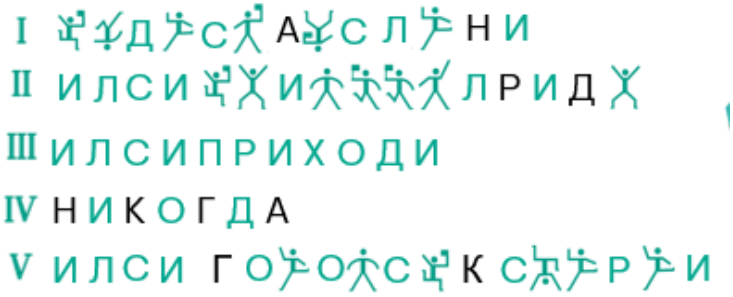

Рисунок 5: Подстановка Н, К, Г, А

Холмс обратил внимание на последнее слово в первой записке – СЛ.НИ. А СЛЕНИ - очень распространенная фамилия в Англии. К тому же, первая записка начинается со слова из одной буквы. Это может быть предлог – У, К, В, но логичнее было бы написать в начале короткой записки местоимение Я.

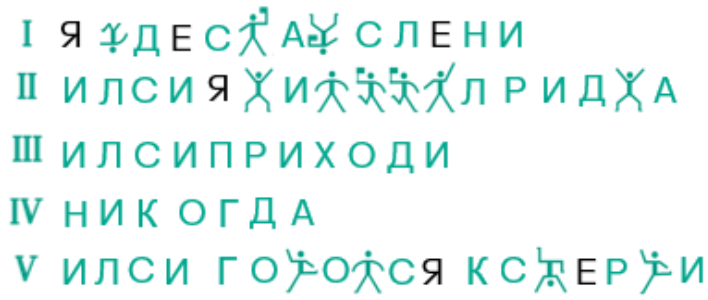

Рисунок 6: Подстановка Я, Е.

Дальше текст становится практически читаемым, Холмс подставляет последние несколько букв и расшифровывает все записки.

I ЯЗДЕСЬАБСЛЕНИ
II ИЛСИЯЖИВУУЭЛРИДЖА
III ИЛСИПРИХОДИ
IV НИКОГДА
V ИЛСИГОТОВЬСЯКСМЕРТИ

Рисунок 7: Расшифровка записок

Всего злоумышленник использовал 23 человечка. Вот такую замену он сделал:

Рисунок 8: Алфавит замены

Первая строчка – это исходный алфавит. Во второй написан алфавит замены.

Такая замена букв открытого текста буквами алфавита замены называется **одноалфавитным шифром подстановки, или шифром простой замены.**

Ключ для этого шифра – это **биективное отображение множества букв исходного алфавита в множество букв алфавита замены.**

Сколькими способами можно переставить буквы в алфавите, если их в нем 32? Вспоминаем комбинаторику – это будет обычная перестановка,

$$P = n!$$

В нашем случае 32! = 263130836933693530167218016160000000 вариантов подстановки. Здесь брутфорс-атака уже не сработает - слишком много надо перебирать.

Недостатки шифра простой замены

Что плохого в шифре простой замены? Основная проблема в том, что одинаковые буквы открытого текста переходят в одинаковые символы шифртекста.

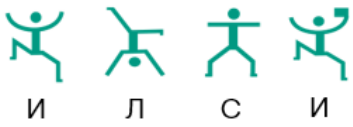

Рисунок 9: ИЛСИ

В любом языке, использующем алфавит, существует такое понятие как **статистическое распределение букв** в тексте. Например, буква А встречается гораздо чаще, чем буква Ъ. Да и вообще гласных букв в русских словах гораздо больше, чем согласных. Самая часто встречающаяся буква русского языка – О, а самая редкая – Ъ или Ё (а в некоторых случаях буква Ё вообще заменяется буквой Е). Частоту встречаемости букв можно узнать, рассматривая длинные тексты на русском языке.

Чтобы собрать статистику, нужно **разделить количество раз, которое встретилась та или иная буква, на общее число букв в тексте.** Например, пусть длина текста равна 1000 символов. Пусть также буква О встретилась 109 раз, Е – 84 раза, а – 80 раз. Тогда частота встречаемости этих букв:

$$n(O) = 109/1000 = 0.109$$

$$n(E) = 84/1000 = 0.84$$

$$n(A) = 80/1000 = 0.080$$

Буквы О, Е, А – самые частые в русском языке.

Частота встречаемости – это величина постоянная. Если взять любой текст и посчитать частоты встречаемости символов для него, то результаты будут одинаковыми. Главное, чтобы текст был достаточно длинным, иначе статистика получится смещённой.

Давайте построим диаграмму частоты встречаемости русских букв в процентах. По горизонтали записываем буквы, а по вертикали – процент встречаемости букв.

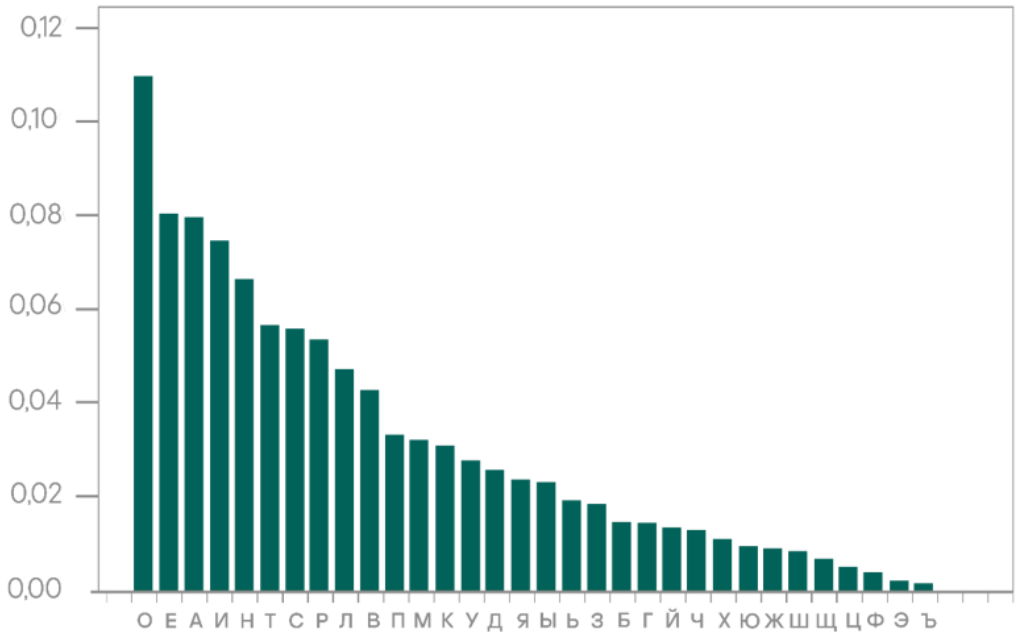

Рисунок 10: Частота встречаемости букв русского алфавита

Известно, что частота встречаемости букв для каждого языка уникальна. Значит, частота встречаемости букв – своеобразный отпечаток пальцев языка, который делает язык уникальным.

Как поможет нам эта информация в криптографии?

Криптоанализ

Это означает, что **любой шифртекст, зашифрованный шифром Цезаря (или любого другого подстановочного шифра), может быть дешифрован с помощью метода частотного анализа.**

Давайте попробуем сделать это для некоторого зашифрованного текста. Пусть дополнительно будет известно, что текст написан на русском языке.

Ы ЛАЯАЕЪА РЕПЮЪЗ ЯСЦПЫ ВАБИПФ ЗПИРЦ ЦЪЬАИ ЦПЮЕКЫВЪЦГ ЕСЬ ЦЛАФИШЕЕПХ НБПМЪБФПХ, Ы ФПЛПБПХ ЫСБЪИПЦГ ЯЛП-ЛП ЕС БАЬФПЦЛГ ЫПЕТЯАА. ЮПИПЫС АЮП МОИС ПНКУАЕС ЕС ЮБКЬГ, Ъ ПЕ ФСЭСИЦШ РЕА НПЗПЩЪР ЕС ЦЛБСЕЕКТ ЛПУКТ НЛЪЖК Ц ЛКЦФИОРЪ ЦАБОРЪ НАБГШРЪ Ъ ЯАБЕОР ЗПЗПИФПР. ЪЛСФ, КПЛЦПЕ, ЦФСЭСИ ПЕ ЫЕАЭСНЕП, ЫО ЕА ЦПМЪБСАЛАЦГ ЫФИСЬОЫСЛГ ЦЫПЪ ЦМАБАЩАЕЪШ Ы ТЩЕПСЙБЪФСЕЦФЪА ЖАЕЕОА МКРСЮЪ? Ш ЫЭЬБПЮЕКИ ПЛ КЬЪЫИАЕЪШ. ФСФ ЕЪ НБЪЫОФ Ш Ф ЕАПМОЯСХЕОР ЦНПЦПМЕПЦЛШР ЗПИРЦС, ДЛП ЫЕАЭСНЕПА ЫЛПБЩАЕЪА Ы ЦСРОА ЛСХЕОА РПЪ РОЦИЪ МОИП ЦПЫАБВАЕЕП ЕАПМЧШЦЕЪРОР. ФСФ, ЯАБЛ ЫПЭГРЪ, ЫО ПМ ДЛПР КЭЕСИЪ ЦНБПЦЪИ Ш. ПЕ НПЫАБЕКИЦШ ЕС ЦЛКИА, ЬАБЩС Ы БКФА ЬОРШУКТЦШ НБПМЪБФК, Ъ АЮП ЮИКМПФП ЦЪЬШУЪА ЮИСЭС БСЬПЦЛЕП ЭСМИЪЦЛСИЪ. НБЪЭЕСХЛАЦГ, КПЛЦПЕ, ЯЛП ЫО ЦПЫАБВАЕЕП ЦМЪЛО Ц ЛПИФК ЦФСЭСИ ПЕ. НБЪЭЕСТЦГ. РЕА ЦИАЬПЫСИП МО ЭСЦЛСЫЪЛГ ЫСЦ ЕСНЪЦСЛГ ПМ ДЛПР ЕС ИЪЦЛПЯФА МКРСЮЪ Ъ НПЬНЪЦСЛГЦШ. НПЯАРК? НПЛПРК ЯЛП ЯАБАЭ НШЛГ РЪЕКЛ ЫО ЦФСЩАЛА, ЯЛП ЫЦА ДЛП ЕАПМОЯСХЕП НБПЦЛП. КЫАБАЕ, ЯЛП ДЛПЮП Ш ЕЪФПЮЬС ЕА ЦФСЩК. ЫЪЬЪЛА ИЪ, ЬПБПЮПХ РПХ КПЛЦПЕ.. ПЕ КФБАНЪИ НБПМЪБФК ЕС ВЛСЛЪЫА Ъ НБЪЕШИЦШ ЯЪЛСЛГ РЕА ИАФЖЪТ Ц ЫЪЬПР НБПЙАЦЦПБС, ПМБСУСТУАЮПЦШ Ф СКЬЪЛПБЪЪ ЕА ЛСФ КЩ ЛБКЬЕП НПЦЛБПЪЛГ ЦАБЪТ ЫОЫПЬПЫ, Ы ФПЛПБПХ ФСЩЬОХ НПЦИАЬКТУЪХ НБПЦЛАХВЪР ПМБСЭПР ЫОЛАФСАЛ ЪЭ НБАЬОЬКУАЮП. АЦИЪ НПЦИА ДЛПЮП КЬСИЪЛГ ЫЦА ЦБАЬЕЪА ЭЫАЕГШ Ъ ЦППМУЪЛГ ЦИКВСЛАИТ ЛПИГФП НАБЫПА ЭЫАЕП Ъ НПЦИАЬЕАА, ПЕЪ НБПЪЭЫАЬКЛ ПВАИПРИШТУАА, ЗПЛШ Ъ ИПЩЕПА ЫНАЯСЛИАЕЪА. НПЦИА ЛПЮП ФСФ Ш ЭСРАЛЪИ ЫНСЬЪЕФК РАЩЬК МПИГВЪР Ъ КФСЭСЛАИГЕОР НСИГЖСРЪ ЫСВАХ ИАЫПХ БКФЪ, РЕА МОИП ЫПЫЦА ЕАЛБКЬЕП ЭСФИТЯЪЛА, ЯЛП ЫО ЕА ЦПМЪБСАЛАЦГ ЫФИСЬОЫСЛГ ЦЫПХ ЕАМПИГВПХ ФСНЪЛСИ Ы ЭПИПЛОА БПЦЦОНЪ. ЕП Ш ЕА ЫЪЩК ЕЪФСФПХ ЦЫШЭЪ РАЩЬК ДЛЪРЪ ЬЫКРШ ПМЦЛПШЛАИГЦЛЫСРЪ! ПЗПЛЕП ЫАБТ. ПЬЕСФП Ш ЫСР Ы ЕАЦФПИГФП РЪЕКЛ ЬПФСЩК, ЯЛП ЛСФСШ ЦЫШЭГ ЦКУАЦЛЫКАЛ. ЫПЛ ПНКУАЕЕОА ЭЫАЕГШ ДЛПХ НБПЦЛАХВАХ ЖАНЪ: ЫП-НАБЫОЗ, ФПЮЬС ЫЯАБС ЫАЯАБПР РО ЫАБЕКИЪЦГ ЪЭ ФИКМС, ЫНСЬЪЕФС РАЩЬК КФСЭСЛАИГЕОР Ъ МПИГВЪР НСИГЖСРЪ ЕС ЫСВАХ ИАЫПХ БКФА МОИС ЫОНСЯФСЕС РАИПР; ЫП-ЫЛПБОЗ, ЫЦШФЪХ БСЭ, ФПЮЬС ЫО ЪЮБСАЛА ЕС МЪИГШБЬА, ЫО ЕСЛЪБСАЛА ДЛК ЫНСЬЪЕФК РАИПР, ЯЛПМО ФЪХ ИКЯВА ЦФПИГЭЪИ К ЫСЦ Ы БКФА; Ы-ЛБАЛГЪЗ, ЫО ЪЮБСАЛА ЕС МЪИГШБЬА ЛПИГФП Ц ЦДБЦЛПЕПР; Ы-ЯАЛЫАБЛОЗ, РАЦШЖ ЕСЭСЬ ЫО РЕА ЦФСЭСИЪ, ЯЛП ЦДБЦЛПЕ НБАЬИПЩЪИ ЫСР НБЪПМБАЦЛЪ ЦПЫРАЦЛЕП Ц ЕЪР ТЩЕПСЙБЪФСЕЦФЪА ЖАЕЕОА МКРСЮЪ, ФПЛПБОА НПЦЛКНШЛ Ы НБПЬСЩК ЯАБАЭ РАЦШЖ; Ы-НШЛОЗ, ЫСВС ЯАФПЫСШ ФЕЪЩФС ЭСНАБЛС Ы ШУЪФА РПАЮП НЪЦГРАЕЕПЮП ЦЛПИС, Ъ ЫО ЕА НПНБПЦЪИЪ К РАЕШ ФИТЯС; Ы-ВАЦЛОЗ, ЫО ЕА ЦПМЪБСАЛАЦГ ЫФИСЬОЫСЛГ ЦЫПЪ ЬАЕГЮЪ Ы ТЩЕПСЙБЪФСЕЦФЪА МКРСЮЪ. ЬП ЯАЮП НБПЦЛП ЫПЦФИЪФЕКИ Ш. ФПЕАЯЕП, ЦФСЭСИ ПЕ, ЦИАЮФС КШЭЫИАЕЕОХ ЫЦШФСШ ЭСЬСЯС ПФСЭОЫСАЛЦШ ПЯАЕГ НБПЦЛПХ НПЦИА ЛПЮП, ФСФ ЫСР АА БСЦЛПИФКТЛ. С ЫПЛ ЫСР ЭСЬСЯС, АУА ЕА БАВАЕЕСШ. НПЦРПЛБЪР, ЬБКЮ КПЛЦПЕ, ФСФ ЫСР КЬСЦЛЦШ Ц ЕАХ ЦНБСЫЪЛГЦШ. ПЕ ЫЭШИ ЦП ЦЛПИС ИЪЦЛПФ МКРСЮЪ, НПЬСИ АЮП РЕА Ъ ЫАБЕКИЦШ Ф ЦЫПАРК ЗЪРЪЯАЦФПРК СЕСИЪЭК. Ш Ц ЪЭКРИАЕЪАР КЫЪЬАИ, ЯЛП ЕС ИЪЦЛФА ЕСЯАБЯАЕО ФСФЪА-ЛП МАЦЦРОЦИАЕЕОА ЪАБПЮИЪЙО.

Мы видим много дублирующихся слов и букв. Мы также можем предположить, что шифртекст получен некоторым шифром подстановки.

После подсчета частоты встречаемости букв получим такую гистограмму:

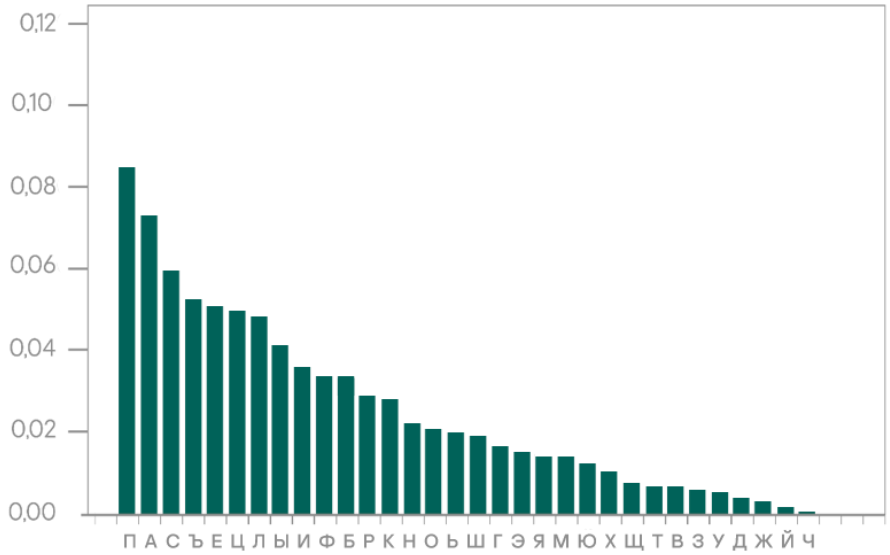

Рисунок 11: Частота встречаемости букв шифр-текста

Видим, что самая частая буква – это буква П. Сравним со статистикой распределения букв в русском алфавите. Самая часто встречающаяся буква – О. Значит, **буква П шифртекста - это на самом деле буква О**. Для более редко встречающихся букв частоты встречаемости могут совпадать. В этом случае нужно применить переборный метод.

А теперь заменим буквы шифртекста на буквы исходного алфавита:

Р СЕЗЕНИЕ МНОЧИЮ ЗАТОР ШЕКВОЛ ЮОВМТ ТИЯЕВ ТОЧНДРШИТЬ НАЯ ТСЕЛВЫННОЙ ПКОБИКЛОЙ, Р ЛОСОКОЙ РАКИВОТЬ ЗСО-СО НА КЕЯЛОТСЬ РОНЖЗЕЕ. ЧОВОРА ЕЧО БУВА ОПДЦЕНА НА ЧКДЯЬ, И ОН ЛАГАВТЫ МНЕ ПОЮОХИМ НА ТСКАННДЖ СОЦДЖ ПСИЭД Т СДТЛВУМИ ТЕКУМИ ПЕКЬЫМИ И ЗЕКНУМ ЮОЮОВЛОМ. ИСАЛ, ДОСТОН, ТЛАГАВ ОН РНЕГАПНО, РУ НЕ ТОБИКАЕСЕТЬ РЛВАЯУРАСЬ ТРОИ ТБЕКЕХЕНИЫ Р ЖХНОАФКИЛАНТЛИЕ ЭЕННУЕ БДМАЧИ? Ы РГЯКОЧНДВ ОС ДЯИРВЕНИЫ. ЛАЛ НИ ПКИРУЛ Ы Л НЕОБУЗАЙНУМ ТПОТОБНОТСЫМ ЮОВМТА, ЩСО РНЕГАПНОЕ РСОКХЕНИЕ Р ТАМУЕ САЙНУЕ МОИ МУТВИ БУВО ТОРЕКШЕННО НЕОБЪЫТНИМУМ. ЛАЛ, ЗЕКС РОГЬМИ, РУ ОБ ЩСОМ ДГНАВИ ТПКОТИВ Ы. ОН ПОРЕКНДВТЫ НА ТСДВЕ, ЯЕКХА Р КДЛЕ ЯУМЫЦДЖТЫ ПКОБИКЛД, И ЕЧО ЧВДБОЛО ТИЯЫЦИЕ ЧВАГА КАЯОТСНО ГАБВИТСАВИ. ПКИГНАЙСЕТЬ, ДОСТОН, ЗСО РУ ТОРЕКШЕННО ТБИСУ Т СОВЛД ТЛАГАВ ОН. ПКИГНАЖТЬ. МНЕ ТВЕЯОРАВО БУ ГАТСАРИСЬ РАТ НАПИТАСЬ ОБ ЩСОМ НА ВИТСОЗЛЕ БДМАЧИ И ПОЯПИТАСЬТЫ. ПОЗЕМД? ПОСОМД ЗСО ЗЕКЕГ ПЫСЬ МИНДС РУ ТЛАХЕСЕ, ЗСО РТЕ ЩСО НЕОБУЗАЙНО ПКОТСО. ДРЕКЕН, ЗСО ЩСОЧО Ы НИЛОЧЯА НЕ ТЛАХД. РИЯИСЕ ВИ, ЯОКОЧОЙ МОЙ ДОСТОН.. ОН ДЛКЕПИВ ПКОБИКЛД НА ШСАСИРЕ И ПКИНЫВТЫ ЗИСАСЬ МНЕ ВЕЛЭИЖ Т РИЯОМ ПКОФЕТТОКА, ОБКАЦАЖЦЕЧОТЫ Л АДЯИСОКИИ НЕ САЛ ДХ СКДЯНО ПОТСКОИСЬ ТЕКИЖ РУРОЯОР, Р ЛОСОКОЙ ЛАХЯУЙ ПОТВЕЯДЖЦИЙ ПКОТСЕЙШИМ ОБКАГОМ РУСЕЛАЕС ИГ ПКЕЯУЯДЦЕЧО. ЕТВИ ПОТВЕ ЩСОЧО ДЯАВИСЬ РТЕ ТКЕЯНИЕ ГРЕНЬЫ И ТООБЦИСЬ ТВДШАСЕВЖ СОВЬЛО ПЕКРОЕ ГРЕНО И ПОТВЕЯНЕЕ, ОНИ ПКОИГРЕЯДС ОШЕВОМВЫЖЦЕЕ, ЮОСЫ И ВОХНОЕ РПЕЗАСВЕНИЕ. ПОТВЕ СОЧО ЛАЛ Ы ГАМЕСИВ РПАЯИНЛД МЕХЯД БОВЬШИМ И ДЛАГАСЕВЬНУМ ПАВЬЭАМИ РАШЕЙ ВЕРОЙ КДЛИ, МНЕ БУВО РОРТЕ НЕСКДЯНО ГАЛВЖЗИСЕ, ЗСО РУ НЕ ТОБИКАЕСЕТЬ РЛВАЯУРАСЬ ТРОЙ НЕБОВЬШОЙ ЛАПИСАВ Р ГОВОСУЕ КОТТУПИ. НО Ы НЕ РИХД НИЛАЛОЙ ТРЫГИ МЕХЯД ЩСИМИ ЯРДМЫ ОБТСОЫСЕВЬТСРАМИ! ОЮОСНО РЕКЖ. ОЯНАЛО Ы РАМ Р НЕТЛОВЬЛО МИНДС ЯОЛАХД, ЗСО САЛАЫ ТРЫГЬ ТДЦЕТСРДЕС. РОС ОПДЦЕННУЕ ГРЕНЬЫ ЩСОЙ ПКОТСЕЙШЕЙ ЭЕПИ: РО-ПЕКРУЮ, ЛОЧЯА РЗЕКА РЕЗЕКОМ МУ РЕКНДВИТЬ ИГ ЛВДБА, РПАЯИНЛА МЕХЯД ДЛАГАСЕВЬНУМ И БОВЬШИМ ПАВЬЭАМИ НА РАШЕЙ ВЕРОЙ КДЛЕ БУВА РУПАЗЛАНА МЕВОМ; РО-РСОКУЮ, РТЫЛИЙ КАГ, ЛОЧЯА РУ ИЧКАЕСЕ НА БИВЬЫКЯЕ, РУ НАСИКАЕСЕ ЩСД РПАЯИНЛД МЕВОМ, ЗСОБУ ЛИЙ ВДЗШЕ ТЛОВЬГИВ Д РАТ Р КДЛЕ; Р-СКЕСЬИЮ, РУ ИЧКАЕСЕ НА БИВЬЫКЯЕ СОВЬЛО Т ТЩКТСОНОМ; Р-ЗЕСРЕКСУЮ, МЕТЫЭ НАГАЯ РУ МНЕ ТЛАГАВИ, ЗСО ТЩКТСОН ПКЕЯВОХИВ РАМ ПКИОБКЕТСИ ТОРМЕТСНО Т НИМ ЖХНОАФКИЛАНТЛИЕ ЭЕННУЕ БДМАЧИ, ЛОСОКУЕ ПОТСДПЫС Р ПКОЯАХД ЗЕКЕГ МЕТЫЭ; Р-ПЫСУЮ, РАША ЗЕЛОРАЫ ЛНИХЛА ГАПЕКСА Р ЫЦИЛЕ МОЕЧО ПИТЬМЕННОЧО ТСОВА, И РУ НЕ ПОПКОТИВИ Д МЕНЫ ЛВЖЗА; Р-ШЕТСУЮ, РУ НЕ ТОБИКАЕСЕТЬ РЛВАЯУРАСЬ ТРОИ ЯЕНЬЧИ Р ЖХНОАФКИЛАНТЛИЕ БДМАЧИ. ЯО ЗЕЧО ПКОТСО РОТЛВИЛНДВ Ы. ЛОНЕЗНО, ТЛАГАВ ОН, ТВЕЧЛА ДЫГРВЕННУЙ РТЫЛАЫ ГАЯАЗА ОЛАГУРАЕСТЫ ОЗЕНЬ ПКОТСОЙ ПОТВЕ СОЧО, ЛАЛ РАМ ЕЕ КАТСОВЛДЖС. А РОС РАМ ГАЯАЗА, ЕЦЕ НЕ КЕШЕННАЫ. ПОТМОСКИМ, ЯКДЧ ДОСТОН, ЛАЛ РАМ ДЯАТСТЫ Т НЕЙ ТПКАРИСЬТЫ. ОН РГЫВ ТО ТСОВА ВИТСОЛ БДМАЧИ, ПОЯАВ ЕЧО МНЕ И РЕКНДВТЫ Л ТРОЕМД ЮИМИЗЕТЛОМД АНАВИГД. Ы Т ИГДМВЕНИЕМ ДРИЯЕВ, ЗСО НА ВИТСЛЕ НАЗЕКЗЕНУ ЛАЛИЕ-СО БЕТТМУТВЕННУЕ ИЕКОЧВИФУ.

Рисунок 12: шифртекст замена

Получилось не очень хорошо. А все потому, что метод частотного анализа поможет определить часто встречающиеся буквы – например букву О. Но однозначного ответа он не даст, поэтому все равно придется немного поперебирать. Зато в текущем варианте текста догадки строить гораздо легче.

Возьмем второе слово шифртекста. Возможно, это слово ВЕЗЕНИЕ или ТЕЧЕНИЕ. Попробуем заменить букву С на букву Т, а букву З на букву Ч.

Р ТЕЧЕНИЕ МНОЗИЮ ЧАСОР ШЕКВОЛ ЮОВМС СИЯЕВ СОЗНДРШИСЬ НАЯ СТЕЛВЫННОЙ ПКОБИКЛОЙ, Р ЛОТОКОЙ РАКИВОСЬ ЧТО-ТО НА КЕЯЛОСТЬ РОНЖЧЕЕ. ЗОВОРА ЕЗО БУВА ОПДЦЕНА НА ЗКДЯЬ, И ОН ЛАГАВСЫ МНЕ ПОЮОХИМ НА СТКАННДЖ ТОЦДЖ ПТИЭД С ТДСЛВУМИ СЕКУМИ ПЕКЬЫМИ И ЧЕКНУМ ЮОЮОВЛОМ. ИТАЛ, ДОТСОН, СЛАГАВ ОН РНЕГАПНО, РУ НЕ СОБИКАЕТЕСЬ РЛВАЯУРАТЬ СРОИ СБЕКЕХЕНИЫ Р ЖХНОАФКИЛАНСЛИЕ ЭЕННУЕ БДМАЗИ? Ы РГЯКОЗНДВ ОТ ДЯИРВЕНИЫ. ЛАЛ НИ ПКИРУЛ Ы Л НЕОБУЧАЙНУМ СПОСОБНОСТЫМ ЮОВМСА, ЩТО РНЕГАПНОЕ РТОКХЕНИЕ Р САМУЕ ТАЙНУЕ МОИ МУСВИ БУВО СОРЕКШЕННО НЕОБЪЫСНИМУМ. ЛАЛ, ЧЕКТ РОГЬМИ, РУ ОБ ЩТОМ ДГНАВИ СПКОСИВ Ы. ОН ПОРЕКНДВСЫ НА СТДВЕ, ЯЕКХА Р КДЛЕ ЯУМЫЦДЖСЫ ПКОБИКЛД, И ЕЗО ЗВДБОЛО СИЯЫЦИЕ ЗВАГА КАЯОСТНО ГАБВИСТАВИ. ПКИГНАЙТЕСЬ, ДОТСОН, ЧТО РУ СОРЕКШЕННО СБИТУ С ТОВЛД СЛАГАВ ОН. ПКИГНАЖСЬ. МНЕ СВЕЯОРАВО БУ ГАСТАРИТЬ РАС НАПИСАТЬ ОБ ЩТОМ НА ВИСТОЧЛЕ БДМАЗИ И ПОЯПИСАТЬСЫ. ПОЧЕМД? ПОТОМД ЧТО ЧЕКЕГ ПЫТЬ МИНДТ РУ СЛАХЕТЕ, ЧТО РСЕ ЩТО НЕОБУЧАЙНО ПКОСТО. ДРЕКЕН, ЧТО ЩТОЗО Ы НИЛОЗЯА НЕ СЛАХД. РИЯИТЕ ВИ, ЯОКОЗОЙ МОЙ ДОТСОН.. ОН ДЛКЕПИВ ПКОБИКЛД НА ШТАТИРЕ И ПКИНЫВСЫ ЧИТАТЬ МНЕ ВЕЛЭИЖ С РИЯОМ ПКОФЕССОКА, ОБКАЦАЖЦЕЗОСЫ Л АДЯИТОКИИ НЕ ТАЛ ДХ ТКДЯНО ПОСТКОИТЬ СЕКИЖ РУРОЯОР, Р ЛОТОКОЙ ЛАХЯУЙ ПОСВЕЯДЖЦИЙ ПКОСТЕЙШИМ ОБКАГОМ РУТЕЛАЕТ ИГ ПКЕЯУЯДЦЕЗО. ЕСВИ ПОСВЕ ЩТОЗО ДЯАВИТЬ РСЕ СКЕЯНИЕ ГРЕНЬЫ И СООБЦИТЬ СВДШАТЕВЖ ТОВЬЛО ПЕКРОЕ ГРЕНО И ПОСВЕЯНЕЕ, ОНИ ПКОИГРЕЯДТ ОШЕВОМВЫЖЦЕЕ, ЮОТЫ И ВОХНОЕ РПЕЧАТВЕНИЕ. ПОСВЕ ТОЗО ЛАЛ Ы ГАМЕТИВ РПАЯИНЛД МЕХЯД БОВЬШИМ И ДЛАГАТЕВЬНУМ ПАВЬЭАМИ РАШЕЙ ВЕРОЙ КДЛИ, МНЕ БУВО РОРСЕ НЕТКДЯНО ГАЛВЖЧИТЕ, ЧТО РУ НЕ СОБИКАЕТЕСЬ РЛВАЯУРАТЬ СРОЙ НЕБОВЬШОЙ ЛАПИТАВ Р ГОВОТУЕ КОССУПИ. НО Ы НЕ РИХД НИЛАЛОЙ СРЫГИ МЕХЯД ЩТИМИ ЯРДМЫ ОБСТОЫТЕВЬСТРАМИ! ОЮОТНО РЕКЖ. ОЯНАЛО Ы РАМ Р НЕСЛОВЬЛО МИНДТ ЯОЛАХД, ЧТО ТАЛАЫ СРЫГЬ СДЦЕСТРДЕТ. РОТ ОПДЦЕННУЕ ГРЕНЬЫ ЩТОЙ ПКОСТЕЙШЕЙ ЭЕПИ: РО-ПЕКРУЮ, ЛОЗЯА РЧЕКА РЕЧЕКОМ МУ РЕКНДВИСЬ ИГ ЛВДБА, РПАЯИНЛА МЕХЯД ДЛАГАТЕВЬНУМ И БОВЬШИМ ПАВЬЭАМИ НА РАШЕЙ ВЕРОЙ КДЛЕ БУВА РУПАЧЛАНА МЕВОМ; РО-РТОКУЮ, РСЫЛИЙ КАГ, ЛОЗЯА РУ ИЗКАЕТЕ НА БИВЬЫКЯЕ, РУ НАТИКАЕТЕ ЩТД РПАЯИНЛД МЕВОМ, ЧТОБУ ЛИЙ ВДЧШЕ СЛОВЬГИВ Д РАС Р КДЛЕ; Р-ТКЕТЬИЮ, РУ ИЗКАЕТЕ НА БИВЬЫКЯЕ ТОВЬЛО С СЩКСТОНОМ; Р-ЧЕТРЕКТУЮ, МЕСЫЭ НАГАЯ РУ МНЕ СЛАГАВИ, ЧТО СЩКСТОН ПКЕЯВОХИВ РАМ ПКИОБКЕСТИ СОРМЕСТНО С НИМ ЖХНОАФКИЛАНСЛИЕ ЭЕННУЕ БДМАЗИ, ЛОТОКУЕ ПОСТДПЫТ Р ПКОЯАХД ЧЕКЕГ МЕСЫЭ; Р-ПЫТУЮ, РАША ЧЕЛОРАЫ ЛНИХЛА ГАПЕКТА Р ЫЦИЛЕ МОЕЗО ПИСЬМЕННОЗО СТОВА, И РУ НЕ ПОПКОСИВИ Д МЕНЫ ЛВЖЧА; Р-ШЕСТУЮ, РУ НЕ СОБИКАЕТЕСЬ РЛВАЯУРАТЬ СРОИ ЯЕНЬЗИ Р ЖХНОАФКИЛАНСЛИЕ БДМАЗИ. ЯО ЧЕЗО ПКОСТО РОСЛВИЛНДВ Ы. ЛОНЕЧНО, СЛАГАВ ОН, СВЕЗЛА ДЫГРВЕННУЙ РСЫЛАЫ ГАЯАЧА ОЛАГУРАЕТСЫ ОЧЕНЬ ПКОСТОЙ ПОСВЕ ТОЗО, ЛАЛ РАМ ЕЕ КАСТОВЛДЖТ. А РОТ РАМ ГАЯАЧА, ЕЦЕ НЕ КЕШЕННАЫ. ПОСМОТКИМ, ЯКДЗ ДОТСОН, ЛАЛ РАМ ДЯАСТСЫ С НЕЙ СПКАРИТЬСЫ. ОН РГЫВ СО СТОВА ВИСТОЛ БДМАЗИ, ПОЯАВ ЕЗО МНЕ И РЕКНДВСЫ Л СРОЕМД ЮИМИЧЕСЛОМД АНАВИГД. Ы С ИГДМВЕНИЕМ ДРИЯЕВ, ЧТО НА ВИСТЛЕ НАЧЕКЧЕНУ ЛАЛИЕ-ТО БЕССМУСВЕННУЕ ИЕКОЗВИФУ.

Рисунок 13: шифртекст замена

Текст стал еще понятнее. Третье слово - это скорее всего слово МНОГИХ. 9-е слово НАЯ, вероятно, когда-то было словом НАД.

Сделаем вот такую замену:

В ТЕЧЕНИЕ МНОГИХ ЧАСОВ ШЕРЛОК ХОЛМС СИЫЕЛ СОГНДВШИСЬ НАЫ СТЕКЛЯННОЙ ПРОБИРКОЙ, В КОТОРОЙ ВАРИЛОСЬ ЧТО-ТО НА РЕЫКОСТЬ ВОНЖЧЕЕ. ГОЛОВА ЕГО БУЛА ОПДЦЕНА НА ГРДЫЬ, И ОН КАЗАЛСЯ МНЕ ПОХОЮИМ НА СТРАННДЖ ТОЦДЖ ПТИЭД С ТДСКЛУМИ СЕРУМИ ПЕРЬЯМИ И ЧЕРНУМ ХОХОЛКОМ. ИТАК, ДОТСОН, СКАЗАЛ ОН ВНЕЗАПНО, ВУ НЕ СОБИРАЕТЕСЬ ВКЛАЫУВАТЬ СВОИ СБЕРЕЮЕНИЯ В ЖЮНОАФРИКАНСКИЕ ЭЕННУЕ БДМАГИ? Я ВЗЫРОГНДЛ ОТ ДЫИВЛЕНИЯ. КАК НИ ПРИВУК Я К НЕОБУЧАЙНУМ СПОСОБНОСТЯМ ХОЛМСА, ЩТО ВНЕЗАПНОЕ ВТОРЮЕНИЕ В САМУЕ ТАЙНУЕ МОИ МУСЛИ БУЛО СОВЕРШЕННО НЕОБЪЯСНИМУМ. КАК, ЧЕРТ ВОЗЬМИ, ВУ ОБ ЩТОМ ДЗНАЛИ СПРОСИЛ Я. ОН ПОВЕРНДЛСЯ НА СТДЛЕ, ЫЕРЮА В РДКЕ ЫУМЯЦДЖСЯ ПРОБИРКД, И ЕГО ГЛДБОКО СИЫЯЦИЕ ГЛАЗА РАЫОСТНО ЗАБЛИСТАЛИ. ПРИЗНАЙТЕСЬ, ДОТСОН, ЧТО ВУ СОВЕРШЕННО СБИТУ С ТОЛКД СКАЗАЛ ОН. ПРИЗНАЖСЬ. МНЕ СЛЕЫОВАЛО БУ ЗАСТАВИТЬ ВАС НАПИСАТЬ ОБ ЩТОМ НА ЛИСТОЧКЕ БДМАГИ И ПОЫПИСАТЬСЯ. ПОЧЕМД? ПОТОМД ЧТО ЧЕРЕЗ ПЯТЬ МИНДТ ВУ СКАЮЕТЕ, ЧТО ВСЕ ЩТО НЕОБУЧАЙНО ПРОСТО. ДВЕРЕН, ЧТО ЩТОГО Я НИКОГЫА НЕ СКАЮД. ВИЫИТЕ ЛИ, ЫОРОГОЙ МОЙ ДОТСОН.. ОН ДКРЕПИЛ ПРОБИРКД НА ШТАТИВЕ И ПРИНЯЛСЯ ЧИТАТЬ МНЕ ЛЕКЭИЖ С ВИЫОМ ПРОФЕССОРА, ОБРАЦАЖЦЕГОСЯ К АДЫИТОРИИ НЕ ТАК ДЮ ТРДЫНО ПОСТРОИТЬ СЕРИЖ ВУВОЫОВ, В КОТОРОЙ КАЮЫУЙ ПОСЛЕЫДЖЦИЙ ПРОСТЕЙШИМ ОБРАЗОМ ВУТЕКАЕТ ИЗ ПРЕЫУЫДЦЕГО. ЕСЛИ ПОСЛЕ ЩТОГО ДЫАЛИТЬ ВСЕ СРЕЫНИЕ ЗВЕНЬЯ И СООБЦИТЬ СЛДШАТЕЛЖ ТОЛЬКО ПЕРВОЕ ЗВЕНО И ПОСЛЕЫНЕЕ, ОНИ ПРОИЗВЕЫДТ ОШЕЛОМЛЯЖЦЕЕ, ХОТЯ И ЛОЮНОЕ ВПЕЧАТЛЕНИЕ. ПОСЛЕ ТОГО КАК Я ЗАМЕТИЛ ВПАЫИНКД МЕЮЫД БОЛЬШИМ И ДКАЗАТЕЛЬНУМ ПАЛЬЭАМИ ВАШЕЙ ЛЕВОЙ РДКИ, МНЕ БУЛО ВОВСЕ НЕТРДЫНО ЗАКЛЖЧИТЕ, ЧТО ВУ НЕ СОБИРАЕТЕСЬ ВКЛАЫУВАТЬ СВОЙ НЕБОЛЬШОЙ КАПИТАЛ В ЗОЛОТУЕ РОССУПИ. НО Я НЕ ВИЮД НИКАКОЙ СВЯЗИ МЕЮЫД ЩТИМИ ЫВДМЯ ОБСТОЯТЕЛЬСТВАМИ! ОХОТНО ВЕРЖ. ОЫНАКО Я ВАМ В НЕСКОЛЬКО МИНДТ ЫОКАЮД, ЧТО ТАКАЯ СВЯЗЬ СДЦЕСТВДЕТ. ВОТ ОПДЦЕННУЕ ЗВЕНЬЯ ЩТОЙ ПРОСТЕЙШЕЙ ЭЕПИ: ВО-ПЕРВУХ, КОГЫА ВЧЕРА ВЕЧЕРОМ МУ ВЕРНДЛИСЬ ИЗ КЛДБА, ВПАЫИНКА МЕЮЫД ДКАЗАТЕЛЬНУМ И БОЛЬШИМ ПАЛЬЭАМИ НА ВАШЕЙ ЛЕВОЙ РДКЕ БУЛА ВУПАЧКАНА МЕЛОМ; ВО-ВТОРУХ, ВСЯКИЙ РАЗ, КОГЫА ВУ ИГРАЕТЕ НА БИЛЬЯРЫЕ, ВУ НАТИРАЕТЕ ЩТД ВПАЫИНКД МЕЛОМ, ЧТОБУ КИЙ ЛДЧШЕ СКОЛЬЗИЛ Д ВАС В РДКЕ; В-ТРЕТЬИХ, ВУ ИГРАЕТЕ НА БИЛЬЯРЫЕ ТОЛЬКО С СЩРСТОНОМ; В-ЧЕТВЕРТУХ, МЕСЯЭ НАЗАЫ ВУ МНЕ СКАЗАЛИ, ЧТО СЩРСТОН ПРЕЫЛОЮИЛ ВАМ ПРИОБРЕСТИ СОВМЕСТНО С НИМ ЖЮНОАФРИКАНСКИЕ ЭЕННУЕ БДМАГИ, КОТОРУЕ ПОСТДПЯТ В ПРОЫАЮД ЧЕРЕЗ МЕСЯЭ; В-ПЯТУХ, ВАША ЧЕКОВАЯ КНИЮКА ЗАПЕРТА В ЯЦИКЕ МОЕГО ПИСЬМЕННОГО СТОЛА, И ВУ НЕ ПОПРОСИЛИ Д МЕНЯ КЛЖЧА; В-ШЕСТУХ, ВУ НЕ СОБИРАЕТЕСЬ ВКЛАЫУВАТЬ СВОИ ЫЕНЬГИ В ЖЮНОАФРИКАНСКИЕ БДМАГИ. ЫО ЧЕГО ПРОСТО ВОСКЛИКНДЛ Я. КОНЕЧНО, СКАЗАЛ ОН, СЛЕГКА ДЯЗВЛЕННУЙ ВСЯКАЯ ЗАЫАЧА ОКАЗУВАЕТСЯ ОЧЕНЬ ПРОСТОЙ ПОСЛЕ ТОГО, КАК ВАМ ЕЕ РАСТОЛКДЖТ. А ВОТ ВАМ ЗАЫАЧА, ЕЦЕ НЕ РЕШЕННАЯ. ПОСМОТРИМ, ЫРДГ ДОТСОН, КАК ВАМ ДЫАСТСЯ С НЕЙ СПРАВИТЬСЯ. ОН ВЗЯЛ СО СТОЛА ЛИСТОК БДМАГИ, ПОЫАЛ ЕГО МНЕ И ВЕРНДЛСЯ К СВОЕМД ХИМИЧЕСКОМД АНАЛИЗД. Я С ИЗДМЛЕНИЕМ ДВИЫЕЛ, ЧТО НА ЛИСТКЕ НАЧЕРЧЕНУ КАКИЕ-ТО БЕССМУСЛЕННУЕ ИЕРОГЛИФУ.

Рисунок 14: шифртекст замена

Заменяя оставшиеся буквы правильными, получаем открытый текст – это отрывок из рассказа Конан Дойла «Пляшущие человечки» о смелом и умном сыщике Шерлоке Холмсе.

В ТЕЧЕНИЕ МНОГИХ ЧАСОВ ШЕРЛОК ХОЛМС СИДЕЛ СОГНУВШИСЬ НАД СТЕКЛЯННОЙ ПРОБИРКОЙ, В КОТОРОЙ ВАРИЛОСЬ ЧТО-ТО НА РЕДКОСТЬ ВОНЮЧЕЕ. ГОЛОВА ЕГО БЫЛА ОПУЩЕНА НА ГРУДЬ, И ОН КАЗАЛСЯ МНЕ ПОХОЖИМ НА СТРАННУЮ ТОЩУЮ ПТИЦУ С ТУСКЛЫМИ СЕРЫМИ ПЕРЬЯМИ И ЧЕРНЫМ ХОХОЛКОМ. ИТАК, УОТСОН, СКАЗАЛ ОН ВНЕЗАПНО, ВЫ НЕ СОБИРАЕТЕСЬ ВКЛАДЫВАТЬ СВОИ СБЕРЕЖЕНИЯ В ЮЖНОАФРИКАНСКИЕ ЦЕННЫЕ БУМАГИ? Я ВЗДРОГНУЛ ОТ УДИВЛЕНИЯ. КАК НИ ПРИВЫК Я К НЕОБЫЧАЙНЫМ СПОСОБНОСТЯМ ХОЛМСА, ЭТО ВНЕЗАПНОЕ ВТОРЖЕНИЕ В САМЫЕ ТАЙНЫЕ МОИ МЫСЛИ БЫЛО СОВЕРШЕННО НЕОБЪЯСНИМЫМ. КАК, ЧЕРТ ВОЗЬМИ, ВЫ ОБ ЭТОМ УЗНАЛИ СПРОСИЛ Я. ОН ПОВЕРНУЛСЯ НА СТУЛЕ, ДЕРЖА В РУКЕ ДЫМЯЩУЮСЯ ПРОБИРКУ, И ЕГО ГЛУБОКО СИДЯЩИЕ ГЛАЗА РАДОСТНО ЗАБЛИСТАЛИ. ПРИЗНАЙТЕСЬ, УОТСОН, ЧТО ВЫ СОВЕРШЕННО СБИТЫ С ТОЛКУ СКАЗАЛ ОН. ПРИЗНАЮСЬ. МНЕ СЛЕДОВАЛО БЫ ЗАСТАВИТЬ ВАС НАПИСАТЬ ОБ ЭТОМ НА ЛИСТОЧКЕ БУМАГИ И ПОДПИСАТЬСЯ. ПОЧЕМУ? ПОТОМУ ЧТО ЧЕРЕЗ ПЯТЬ МИНУТ ВЫ СКАЖЕТЕ, ЧТО ВСЕ ЭТО НЕОБЫЧАЙНО ПРОСТО. УВЕРЕН, ЧТО ЭТОГО Я НИКОГДА НЕ СКАЖУ. ВИДИТЕ ЛИ, ДОРОГОЙ МОЙ УОТСОН.. ОН УКРЕПИЛ ПРОБИРКУ НА ШТАТИВЕ И ПРИНЯЛСЯ ЧИТАТЬ МНЕ ЛЕКЦИЮ С ВИДОМ ПРОФЕССОРА, ОБРАЩАЮЩЕГОСЯ К АУДИТОРИИ НЕ ТАК УЖ ТРУДНО ПОСТРОИТЬ СЕРИЮ ВЫВОДОВ, В КОТОРОЙ КАЖДЫЙ ПОСЛЕДУЮЩИЙ ПРОСТЕЙШИМ ОБРАЗОМ ВЫТЕКАЕТ ИЗ ПРЕДЫДУЩЕГО. ЕСЛИ ПОСЛЕ ЭТОГО УДАЛИТЬ ВСЕ СРЕДНИЕ ЗВЕНЬЯ И СООБЩИТЬ СЛУШАТЕЛЮ ТОЛЬКО ПЕРВОЕ ЗВЕНО И ПОСЛЕДНЕЕ, ОНИ ПРОИЗВЕДУТ ОШЕЛОМЛЯЮЩЕЕ, ХОТЯ И ЛОЖНОЕ ВПЕЧАТЛЕНИЕ. ПОСЛЕ ТОГО КАК Я ЗАМЕТИЛ ВПАДИНКУ МЕЖДУ БОЛЬШИМ И УКАЗАТЕЛЬНЫМ ПАЛЬЦАМИ ВАШЕЙ ЛЕВОЙ РУКИ, МНЕ БЫЛО ВОВСЕ НЕТРУДНО ЗАКЛЮЧИТЕ, ЧТО ВЫ НЕ СОБИРАЕТЕСЬ ВКЛАДЫВАТЬ СВОЙ НЕБОЛЬШОЙ КАПИТАЛ В ЗОЛОТЫЕ РОССЫПИ. НО Я НЕ ВИЖУ НИКАКОЙ СВЯЗИ МЕЖДУ ЭТИМИ ДВУМЯ ОБСТОЯТЕЛЬСТВАМИ! ОХОТНО ВЕРЮ. ОДНАКО Я ВАМ В НЕСКОЛЬКО МИНУТ ДОКАЖУ, ЧТО ТАКАЯ СВЯЗЬ СУЩЕСТВУЕТ. ВОТ ОПУЩЕННЫЕ ЗВЕНЬЯ ЭТОЙ ПРОСТЕЙШЕЙ ЦЕПИ: ВО-ПЕРВЫХ, КОГДА ВЧЕРА ВЕЧЕРОМ МЫ ВЕРНУЛИСЬ ИЗ КЛУБА, ВПАДИНКА МЕЖДУ УКАЗАТЕЛЬНЫМ И БОЛЬШИМ ПАЛЬЦАМИ НА ВАШЕЙ ЛЕВОЙ РУКЕ БЫЛА ВЫПАЧКАНА МЕЛОМ; ВО-ВТОРЫХ, ВСЯКИЙ РАЗ, КОГДА ВЫ ИГРАЕТЕ НА БИЛЬЯРДЕ, ВЫ НАТИРАЕТЕ ЭТУ ВПАДИНКУ МЕЛОМ, ЧТОБЫ КИЙ ЛУЧШЕ СКОЛЬЗИЛ У ВАС В РУКЕ; В-ТРЕТЬИХ, ВЫ ИГРАЕТЕ НА БИЛЬЯРДЕ ТОЛЬКО С СЭРСТОНОМ; В-ЧЕТВЕРТЫХ, МЕСЯЦ НАЗАД ВЫ МНЕ СКАЗАЛИ, ЧТО СЭРСТОН ПРЕДЛОЖИЛ ВАМ ПРИОБРЕСТИ СОВМЕСТНО С НИМ ЮЖНОАФРИКАНСКИЕ ЦЕННЫЕ БУМАГИ, КОТОРЫЕ ПОСТУПЯТ В ПРОДАЖУ ЧЕРЕЗ МЕСЯЦ; В-ПЯТЫХ, ВАША ЧЕКОВАЯ КНИЖКА ЗАПЕРТА В ЯЩИКЕ МОЕГО ПИСЬМЕННОГО СТОЛА, И ВЫ НЕ ПОПРОСИЛИ У МЕНЯ КЛЮЧА; В-ШЕСТЫХ, ВЫ НЕ СОБИРАЕТЕСЬ ВКЛАДЫВАТЬ СВОИ ДЕНЬГИ В ЮЖНОАФРИКАНСКИЕ БУМАГИ. ДО ЧЕГО ПРОСТО ВОСКЛИКНУЛ Я. КОНЕЧНО, СКАЗАЛ ОН, СЛЕГКА УЯЗВЛЕННЫЙ ВСЯКАЯ ЗАДАЧА ОКАЗЫВАЕТСЯ ОЧЕНЬ ПРОСТОЙ ПОСЛЕ ТОГО, КАК ВАМ ЕЕ РАСТОЛКУЮТ. А ВОТ ВАМ ЗАДАЧА, ЕЩЕ НЕ РЕШЕННАЯ. ПОСМОТРИМ, ДРУГ УОТСОН, КАК ВАМ УДАСТСЯ С НЕЙ СПРАВИТЬСЯ. ОН ВЗЯЛ СО СТОЛА ЛИСТОК БУМАГИ, ПОДАЛ ЕГО МНЕ И ВЕРНУЛСЯ К СВОЕМУ ХИМИЧЕСКОМУ АНАЛИЗУ. Я С ИЗУМЛЕНИЕМ УВИДЕЛ, ЧТО НА ЛИСТКЕ НАЧЕРЧЕНЫ КАКИЕ-ТО БЕССМЫСЛЕННЫЕ ИЕРОГЛИФЫ.

Рисунок 15: Открытый текст

А ключ был таким:

А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
С	М	Ы	Ю	Ь	А	Щ	Э	Ъ	Х	Ф	И	Р	Е	П	Н	Б	Ц	Л	К	Й	З	Ж	Я	В	У	Ч	О	Г	Д	Т	Ш

Рисунок 16: алфавит (верхняя строка) / ключ (нижняя строка)

Кстати, **для небольших текстов применить метод частотного анализа невозможно** – слишком мало данных для анализа. В этом случае нужно решать задачу **переборно**. Что это значит? Мы понимаем, что некоторых слов не существует. Поэтому, если мы видим однобуквенное слово, то это, скорее всего, буквы-связки И, К, В, У. Двухбуквенных слов тоже немного: ПО, НА и другие предлоги, УЖ, БЫ. Нет смысла перебирать сочетания ПЧ, ЩЖ и тому подобное. Сначала делаем предположение, затем проверяем его. Если в тексте не удалены знаки препинания, то можно сделать некоторые выводы из пунктуации. Например, если стоит какое-то сочетание "ЛДВЩФ, Т возможно, буква Т – это союз И для сложносочиненного предложения.

Итак, давайте резюмировать.

В одноалфавитном шифре подстановки алфавит открытого текста заменяется алфавитом замены, ключ для этого шифра – это биективное отображение букв алфавитов. Этот шифр может иметь 32! вариантов ключа, что делает невозможной брутфорс-атаку. Но так как этот шифр сохраняет статистику распределения букв, к нему можно применить метод частотного анализа и дешифровать зашифрованный текст.