Министерство образования и науки Российской Федерации
Сибирский федеральный университет

ОСНОВЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Учебно-методическое пособие
(ПРОЕКТ)

Красноярск
СФУ
2016

ЛАБОРАТОРНАЯ РАБОТА №3

(Основы криптоанализа шифров полиалфавитной подстановки)

Цель работы:

- введение в криптосистемы полиалфавитной подстановки на примере шифра Виженера;
- изучение методов криптоанализа шифров полиалфавитной подстановки на примере шифра Виженера.

1. ТЕОРЕТИЧЕСКИЕ СВЕДЕНИЯ

Как уже было отмечено ранее, криптография зародилась очень давно, за несколько тысяч лет до нашей эры практически одновременно с возникновением письменности. Первыми «пионерами» в криптографии стали, так называемые, моноалфавитные шифры, в которых мощности алфавитов открытого и шифротекста были эквивалентны, а сам алгоритм базировался на простейших перестановочных или подстановочных операциях. В качестве известного примера можно привести известный «Шифр Цезаря», алгоритм которого заключался в замене каждого символа в тексте на элемент, отстоящий от него в алфавите на фиксированное число позиций. Если сопоставить каждому символу алфавита его порядковый номер, нумерую с нуля, то используя формулы модульной арифметики шифрование и дешифрование можно представить следующим образом:

$$\begin{aligned} e &= (o + k) \bmod m \\ o &= (e - k) \bmod m \end{aligned}, \text{ где}$$

o - символ открытого текста, e - символ шифротекста, k – ключ, m – мощность алфавита.

Благодаря работе известного арабского философа *Ал-Кинди* оказалось, что моноалфавитные шифры, в том числе и «шифр Цезаря», очень легко поддаются частотному криптоанализу и имеют очень низкую криптостойкость. Возникла потребность в разработке таких шифров, ручная расшифровка которых может потребовать очень значительных усилий. И на смену моноалфавитным шифрам пришли полиалфавитные шифры.

Иитальянский архитектор **Батисте Альберти** одним из первых предложил полиалфавитный шифр. Впоследствии данный шифр получил имя дипломата XVI века **Блеза де Вижинера**. Также вклад в развитие полиалфавитных шифров внёс немецкий аббат XVI века **Иоганн Трисемус**. Простым, но стойким способом полиалфавитной замены является и шифр **Плейфера**, открытый в начале XIX века **Чарльзом Уитстоном**. Этот шифр использовался вплоть до I мировой войны.

Последним словом в развитии полиалфавитных шифров стали так называемые роторные машины, которые позволяли легко создавать устойчивые к криптоатакам полиалфавитные шифры. Примером такой машины является немецкая машина ***Enigma***, разработанная в 1917 г. голландцем Хьюго Кохом, которая использовалась и во время второй мировой войны армией Рейха.

Однако с развитием ЭВМ полиалфавитные шифры перестали быть столь устойчивыми к криптоатакам, и, так же, как в своё время и моноалфавитные шифры, стали частью истории криптографии.

1.1. Концепция полиалфавитного шифрования

В основе любого полиалфавитного шифра лежит принцип циклического применения нескольких моноалфавитных шифров к определённому числу букв шифруемого текста.

Например, пусть у нас имеется некоторое сообщение $O = \{o_1, o_2, ...o_m\}$, которое необходимо зашифровать с помощью полиалфавитного шифра. Полиалфавитный шифр состоит из нескольких моноалфавитных шифров (например, n штук). В нашем случае к первому символу применяется первый моноалфавитный шифр, ко второму символу – второй, к третьему – третий, к n-му символу n-ый, а к (n+1) снова первый, ну и так далее.

Таким образом, шифротекст представляет собой последовательность символов $E = \{f_1(o_1), f_2(o_2), ..., f_n(o_i), f_1(o_{i+1}), ...f_j(o_m)\}$, где $f_n(o_i)$ - один из имеющихся моноалфавитных шифров, который применяется для i-го символа открытого текста, m – количество символов открытого текста, n – количество доступных моноалфавитных шифров. Следует отметить, что при таком подходе использования простых моноалфавитных шифров, но для каждой буквы в отдельности, получается довольно-таки сложная последовательность, которую уже не так просто «взломать», как один моноалфавитный шифр применённый ко всем символам открытого текста. Самым важным эффектом, достигаемым при использовании полиалфавитного шифра, является маскировка частот появления тех или иных букв в тексте, на основании которой обычно очень легко вскрываются моноалфавитные шифры.

1.1. Шифр Виженера

То, что сейчас известно под шифром Виженера, впервые описал **Джованни Батиста Беллазо** в своей книге *La cifra del. Sig. Giovan Battista Bellaso*. Он использовал идею *tabula recta* (центральный компонент) **Трисемуса**, но добавил

ключ для переключения алфавитов шифра через каждую букву. **Блез де Виженер** представил своё описание простого, но стойкого шифра перед комиссией Генриха III во Франции в 1586 году, и позднее изобретение шифра было присвоено именно ему.

Блез де Виженер предложил использовать в качестве ключа часть текста самого сообщения или же уже шифрованного сообщения. Принцип шифрования проще всего пояснить на примере. Итак, пусть ключом будет слово из трёх букв, например «АБВ». Сначала составляется таблица, называемая *квадратом Виженера*, см. табл. 1. Заметим, что в данной таблице отсутствует буква Ё, подразумевая эквивалентность Е и Ё.

Допустим, что необходимо зашифровать текст, состоящий (для простоты) из одного слова – «ВИЖЕНЕР». Учитывая, что длина ключа «АБВ» необходимо увеличить длину ключа до размерности открытого тексте путём многократного повторения, т.е. учитывая, что длина открытого текста 7 символов, наш ключ будет «АБВАБВА». Для простоты понимая, составим следующую таблицу:

Ключ	А	Б	В	А	Б	В	А
Открытый текст	В	И	Ж	Е	Н	Е	Р
Шифротекст	В	Й	И	И	О	З	Р

Каждый символ шифротекста получен путём пересечения столбца (буква ключа) и строки (буква открытого текста) по квадрату Виженера (см. табл. 1). Таким образом, образуется шифротекст «ВЙИИОЗР». Следует отметить, что длина ключа равна числу всех моноалфавитных шифров (в нашем случае из 3), суперпозицией которых и является шифр Виженера, представляющий собой простую полиалфавитную подстановку.

Табл. 1. Квадрат Виженера с буквами русского алфавита

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

1.3. Криптоанализ шифра Виженера

Как уже было отмечено, полиалфавитные шифры позволяют, в отличие от моноалфавитных подстановок, скрыть естественную частоту появления символов в шифротексте, что в свою очередь затрудняет применение частотного анализа в «чистом виде». По этой причине, этот шифр сравнительно долгое время считался трудно раскрываемым. Однако в 1863 году независимо друг от друга учёными

Фридрихом Касиски и Чарльзом Бэббиджем был разработан метод криптоанализа таких шифров, в основе которого лежала уязвимость таких шифров – периодичность использования ключа.

Число используемых алфавитов в шифре Виженера называется периодом шифра. Как уже было отмечено ранее, для шифрования используется ключ - слово или бессмысленный набор символов нормативного алфавита. Каждая буква ключа определяет свой алфавит шифрования, который получается из нормативного циклическим сдвигом на количество символов, равное числовому эквиваленту буквы ключа. Очевидно, что длина ключа равна периоду шифра. Чтобы вычислить числовой эквивалент буквы шифртекста, числовой эквивалент буквы ключа складывается по модулю M с числовым эквивалентом буквы открытого текста, где M – мощность нормативного алфавита (алфавита открытого текста). Соответственно, шифр Вижинера можно описать с помощью формул модульной математики следующим выражением:

$E_i = \left(O_i + K_{i(\mathrm{mod}\,\mu)}\right) \mathrm{mod}\, M$, где E_i и O_i – числовые эквиваленты символов шифротекста и открытого текста соответственно, $K_{i(\mathrm{mod}\,\mu)}$ – числовой эквивалент буквы ключа, M – мощность нормативного алфавита, μ – период шифра (длина ключа).

Фридрихом Казиски, изучая шифр Виженера и наблюдая за результатами его работы заметил, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ, будут одинаково зашифрованы. Соответственно, если разбить весь шифротекст на отрезки так, чтобы число символов в каждом из них равнялось μ (длине ключа или периоду шифра), то можно увидеть, что символы шифротекста, занимающие одинаковое положение в отрезках имеют одинаковое смещение относительно символов открытого текста. Это означает, что при их шифровании используется один и тот же алфавит шифрования.

Описанная особенность шифра Виженера дает возможность применить частотный анализ отдельно для каждой группы символов криптограммы, соответствующих определенной букве ключа. Такие группы символов криптограмм называют *группой периода*. Очевидно, что число групп периода равно длине ключа.

Частотный анализ по группам ключа позволяет криптоаналитику узнать величину смещения для каждой группы символов, т.е. ключ шифрования.

Следует отметить, что данный метод криптоанализа применим, если число символов в криптограмме превышает число 20μ.

Как правило, криптоанализ шифра Виженера проводится в два этапа. На первом этапе определяется число μ, а на втором – непосредственно ключевое слово.

Для определения числа μ применяется так называемый **тест Касиски**, названный в честь Ф. Касиски впервые применивший его на практике в 1863 году. Тест основан на простом наблюдении о том, что два одинаковых отрезка открытого текста, отстоящих друг от друга на расстоянии, кратном μ, будут одинаково зашифрованы. В силу этого в шифротексте осуществляется поиск отрезков с повторяющейся длиной (не менее 3х символов), а также расстояния между ними. Следует отметить, что случайно такие одинаковые отрезки могут появиться в тексте с достаточно малой вероятностью.

Пусть $d_1, d_2,...$ – найденные расстояния между повторениями. Тогда μ должно делить наибольший общий делить этих чисел НОД (d_1, d_2). При этом, чем больше повторений имеет текст, тем более вероятно, что μ вообще совпадает с НОД (d_1, d_2). Также следует отметить, что что случайно такие одинаковые отрезки могут появиться в тексте с очень малой вероятностью. Дальнейшее развитие эта идея получила в 1920 г., когда У. Фридман предложил находить μ с помощью **индекса соответствия**.

Пусть мы имеем некую строку шифротекста $X = \{x_1, x_2, ..., x_N\}$ длины N, составленной из букв некоторого алфавита A, тогда индексом соответствия в x, обозначаемым $I_c(x)$, будем называть вероятность того, что две случайно выбранные буквы из x совпадают. Если представим алфавит $A = \{a_1, a_2, ..., a_M\}$, причём отождествление букв алфавита с числами будем осуществлять так, что $a_1 \equiv 0,\ a_2 \equiv 1\ ,...,\ a_{m-1} \equiv M-2,\ a_m \equiv M-1$, тогда индекс соответствия можно вычислить по формуле:

$$I_c(x) = \frac{\sum_{i=0}^{M-1} f_i \cdot (f_i - 1)}{N(N-1)}, \quad (1)$$

где N - число символов в криптограмме, f_i - число вхождений буквы a_i (т.е. сколько раз i-ая буква встретилась в криптограм*ме*), M – мощность алфавита. Важно заметить, что индекс соответствия представляет собой величину, связанную в первую очередь с я зыком, на котором был составлен открытый текст. Например, для русского языка $I_c(x) \approx 0,0529$, для английского языка - $I_c(x) \approx 0,0662$. Кроме этого, в практике криптоанализа существуют таблицы, содержащие теоретически ожидаемые значения индекса соответствия для шифротекстов, полученных с помощью криптосистемы Виженера с использованием ключей различной длины. Таким образом, если рассчитать значения индекса соответствия для данного шифротекста, то по таблице можно определить длину его ключа, то есть период шифра μ. Пример такой таблицы для алфавита, состоящего из русских букв и пробела представлен ниже.

Табл. 2. Таблица соответствия индекса соответствия и периода шифра

Период шифра (величина μ)	**Минимальное** значения индекса соответствия $I_c(x)_{\min}$	**Максимальное** значения индекса соответствия $I_c(x)_{\max}$	**Среднее** значения индекса соответствия $\overline{I_c(x)}$
1	0.055	0.0615	0.058
2	0.0395	0.055	0.046
3	0.0355	0.044	0.04
4	0.035	0.0405	0.0375
5	0.0335	0.039	0.036
6	0.0325	0.0385	0.0352
7	0.0315	0.0365	0.0345
более		0.0350	

Однако использование таких таблиц не всегда представляется возможным. Этому есть несколько причин. Во-первых, процедура расчёта несёт в себе

накопительную погрешность и при больших длинах ключа шифрования (более 7 символов) расчёт вовсе может оказаться не верным. Во-вторых, открытый текст, который зашифровывался, может не подходить под «среднестатистический» и расчётная величина индекса соответствия может оказаться не табличной. Поэтому для определения периода шифра (величины μ) поступают следующим образом.

Пусть мы имеем некоторый шифротекст $X = \{x_1, x_2, ..., x_N\}$. Выпишем его с некоторым периодом μ:

$$\begin{array}{cccc} \overrightarrow{X_1} & \overrightarrow{X_2} & ... & \overrightarrow{X_\mu} \\ x_1 & x_2 & ... & x_\mu \\ x_{\mu+1} & x_{\mu+2} & ... & x_{2\mu} \\ x_{2\mu+1} & x_{2\mu+2} & ... & x_{3\mu} \\ ... & ... & ... & ... \end{array}. \qquad (2)$$

Обозначим получившиеся столбцы через $\overrightarrow{X_1}, \overrightarrow{X_2}, ..., \overrightarrow{X_\mu}$. Тогда, если μ - это истинная величины периода, т.е. длина ключевого слова, то каждый столбец $\overrightarrow{X_i}$, где $i \in [1, \mu]$ представляет собой участок шифротекста, полученный простой моноалфавитной подстановкой, которую можно описать выражением: $E_i = (O_i + R_i) \bmod M$, где O_i и E_i – числовые эквиваленты символов алфавита открытого и шифротекста соответственно, R_i – коэффициент сдвига, а M – мощность алфавита.

В этом случае расчётное значение индекса соответствия $I_c(\overrightarrow{X_i})$ будет близко к ожидаемому индексу соответствия конкретного языка, алфавитом которого был записан открытый текст. В случае, если языком открытого текста являлся русский, то $I_c(\overrightarrow{X_i}) \approx 0,0529$ при любом $i \in [1, \mu]$. Если же предполагаемое значение μ было выбрано некорректно, то буквы столбца $\overrightarrow{X_i}$ будут более «случайными», поскольку они не являются фрагментом шифра моноалфавитной подстановки. В этом случае значение $I_c(\overrightarrow{X_i})$ будет ближе к числу $I_c(\overrightarrow{X_i}) \approx \frac{1}{32} \approx 0,03125$, если предположить, что открытый текст был составлен из алфавита в 32 буквы.

Заметная разница значений $I_c(x)$ для осмысленных открытых текстов и случайной последовательностью букв (как уже было отмечено, для русского языка – это 0,053 и 0,032) позволяет практически всегда установить точное значение числа μ, а значит и длину ключа.

После определения длины ключевого слова есть несколько способов по дешифровки шифротекста.

- **Первый** способ заключается в переборе всех вариантов сдвига (подстановки) для каждого столбца в пределах μ и нахождения осмысленной расшифровки и, соответственно, ключевого слова.

- **Второй** способ заключается в переборе всех вариантов ключа (размерностью μ) по словарю и нахождения осмысленной расшифровки. Подбор может быть полным (брутфорс) или с использованием словарей.

- **Третий** способ расшифровки основан на нахождении самого ключа шифрования с использованием *индекса взаимного совпадения*. Пусть $\overrightarrow{X} = (x_1, x_2, ..., x_n)$ и $\vec{Y} = (y_1, y_2, ..., y_m)$ - два вектора (строки) букв некоторого алфавита *A*. Тогда взаимным индексом совпадения $\overrightarrow{X}$ и $\vec{Y}$ называется вероятность того, что случайно выбранная буква из $\overrightarrow{X}$ совпадёт со случайно выбранной буквой из $\vec{Y}$. Взаимный индекс совпадения обозначается через $MI_c\left(\overrightarrow{X}, \vec{Y}\right)$.

Пусть $f_0^x, f_1^x, ..., f_n^x$ и $f_0^y, f_1^y, ..., f_m^y$ - числа вхождений различных букв алфавита в $\overrightarrow{X}$ и $\vec{Y}$ соответственно, тогда взаимный индекс совпадения будет вычисляться по формуле:

$$MI_c(\overrightarrow{X}, \vec{Y}) = \frac{\sum_i f_i^X \cdot f_i^Y}{n \cdot m}, \qquad (3)$$

где *n* и *m* длины векторов $\overrightarrow{X}$ и $\vec{Y}$ соответственно.

Предположим, что нам необходимо определить взаимный индекс совпадения двух строк $\overrightarrow{X_i}$ и $\overrightarrow{X_j}$, зашифрованных шифром Виженера, взятых через период μ

согласно (2). Пусть $\overrightarrow{K} = \left(k_1, k_2, ..., k_\mu\right)$ ключ шифрования. Можно оценить их взаимный индекс совпадения, который будет равен примерно:

$$MI_c(\overrightarrow{X_i}, \overrightarrow{X_j}) \approx \sum_{i=0}^{M-1} p_{i-k_i} \cdot p_{i-k_j} = \sum_{i=0}^{M-1} p_i \cdot p_{h+k_i-k_j}\,, \qquad (4)$$

где M – мощность алфавита, p - вероятность появления буквы алфавита в строке.

Здесь важно заметить, что правая часть выражения (4) зависит только от величины $\alpha = (k_i - k_j) \bmod M$, которая называется относительным сдвигом строк $\overrightarrow{X_i}$ и $\overrightarrow{X_j}$. Тогда если учесть, что $\sum_{i=0}^{M-1} p_i \cdot p_{i+\alpha} = \sum_{i=0}^{M-1} p_i \cdot p_{i-\alpha}$, можно построить таблицу относительных сдвигов для любого $\alpha \in \left[1, \frac{M}{2}\right]$ и использовать их для нахождения значений в случаях $\alpha \in \left(\frac{M}{2}, M\right)$.

Вычислив индексы взаимных совпадений для каждого столбца в пределах μ и соответствующие табличные значения можно определить величины относительных сдвигов столбцов.

Табл. 3. Таблица относительных сдвигов для русского языка

Сдвиг	Индекс взаимного соответствия	Сдвиг	Индекс взаимного соответствия
0	0,0553	9	0,0317
1	0,0366	10	0,0265
2	0,0345	11	0,0251
3	0,0400	12	0,0244
4	0,0340	13	0,0291
5	0,0360	14	0,0322
6	0,0326	15	0,0244
7	0,0241	16	0,0249

После этого можно связать системой уравнений относительные сдвиги различных пар столбцов $\overrightarrow{X_i}$ и $\overrightarrow{X_j}$ решив которые получить 32 варианта (для алфавита шифрования из 32 букв русского языка) вариантов ключевого слова, из которых можно выбрать наиболее предпочтительный вариант (если ключевое слово является осмысленным).

- **Четвёртый** способ расшифровки основан на усовершенствованном тесте Касиски, более известным как **метод Кирхгофа**. Суть его заключается в сравнении частоты появления символов в столбцах в пределах μ с частотой

появления символов в исходном тексте для нахождения ключевого символа для каждого столбца.

2. ЗАДАНИЯ К ЛАБОРАТОРНОЙ РАБОТЕ

Используя любой из способов криптоанализа (рассмотренных ранее) шифров полиалфавитной подстановки расшифруйте текст сообщения (согласно вашему персональному варианту), а также определите секретный ключ, которым оно было зашифровано.

Известные сведения о шифрограмме следующие:

- для зашифрования сообщения, которое представляет собой отрывок из литературного произведения, использовался шифр Виженера, с алфавитом, представленным в таблице;
- знаки препинания, а также знак пробела не входят в алфавит шифрования и, соответственно, не является частью шифротекста, т.е. шифротекст с расставленными знаками препинания и пробелами эквивалентен шифротексту без них;
- весь шифротекст представляет собой одну строку;
- в качестве ключа шифрования использовалось одно слово (из букв алфавита), длина которого не более 10 символов.

Для осуществления статистического криптоанализа необходимо разработать программу для дешифрования со следующими возможностями:

- автоматическое приближённое нахождение периода шифрования (числа μ) с помощью теста Касиски;
- автоматическая проверка правильности выбора μ с помощью нахождения индексов соответствия (для всех подгрупп шифротекста);
- в случаях, когда тест Касиски не удаётся применить или значение μ, найденное с его помощью, не подтверждается после определения индексов соответствия, μ определяется подбором (такой случай возможен в случаях, когда длина ключа более 7 знаков и/или зашифрованный текст слишком короткий);
- автоматическое вычисление всех потенциально возможных вариантов ключа шифрования, и вывод их пользователю для принятия решения;
- расшифровка шифротекста, по выбранному пользователем ключу шифрования.

Разработанная Вами программа должна содержать графический интерфейс пользователя.

2.1. Общий алгоритм нахождения периода шифрования

Как уже было отмечено в теоретической части, для первоначального определения длины ключевого слова (периоды шифрования μ) используется тест Касиски (см. п.п. 1.3). В общем, алгоритм теста можно описать следующим образом:

1. В шифротексте ищутся повторяющиеся последовательности букв длиной не менее трёх (триграммы) и расстояния между ними (например, в шифрограмме рхцэооэцг**БРЬ**цмйфктъъюьмшэсяцпунуящэйтаьэдкци**БРЬ**цгбр расстояние между триграммами равно 35);
2. Находится наибольший общий делитель (НОД) полученных чисел (расстояний);
3. Если он больше 1 и меньше 10 (в нашем случае известно, что ключ не более 10 символов) то выдвигаем гипотезу, что НОД является значением μ и приступаем к проверке этой гипотезы с помощью индексов соответствия;
4. Если гипотеза подтвердилась, то переходим к расшифровке, в противном случае снова переходим к п.п. 1 и осуществляем поиск других триграмм;

2.2. Варианты заданий

Вариант 1: ЦЬЦЬИУЯ БОЫАОУШ ЛЙЦ ГЧЙДРЫУШ Х ЧЦХОШАТС, ЕЪЬЫЬЫНШВЦЧ ЪСУЩШУ: НЯУАОФОЧЦ М СЩЧЬНУСБХЦЦ РСТ ПЮЫАЗ ЬЦМСМОЦОХБ ГКПЦМИЕИПЩЗЫТЦИТМ, ЬЬТЖЖКФРЫМКВ, НЦМШМС ЕШЮЖРТС ЕЪЦМЩММЮЬКЬН ЕУБПУ Х ЭФНЖШТР. "ЯРУИЪЦ, МЮДЧ, - ЩШРЩЮМР ЫЦБ ШУ ФЕЭ ПСЩ ЭФУКПЯЬЬФ, - Ш ИППК УХЧТ ЬОЦОСЧ; ЩЪУГЫТ ЖЙОУЭ, УХРЮ ЬЙ РСТ ФДНБМЦЬБ. ГШ АЖ ЫЙЧЫЪЭРЩМЗ. ИППК ЬИТД БАЩ-ЫМЖЙОК ТОРЕГТА, ЩТСУ НЬЬ-ШЦЕШЪЖ АРПЙ ФДХММЦЦЦХ - ЬЙ УЪ ЛЕГЙА, Л ЭФУНПУ Ю АЙЖХ ОЮКЫА, ФЖШЕРУ ЦКЧП ЫУЭТЬЫЦ, АЖ БК Н ЩХНПУЦБ ГК ЫРСТ ТЫ ЯЬВУЬБ. ЗЦЬЭЮМ, ЬИШП УХ ЦКЧЙ ЫР РЯЭЫХ ЪЩТСАЯ РЦНЬУНЗПД. Ю АЙЖХ Т АРЭЙХТ ЭФР ЕЦУ-ИШ ЫЛЕМТЦИА ЬЩМЭАШЪ МЬНПД ФЮУЕДЧТ ФЮЛЯОН. ЖТЯЮЫТП Й ЬУМН СК ЗЬЮЩС, Д ФДОЕЛЯ М ЗДМЯР ЯПЕЧ, ХЦШЦГ ТЫ МЦПЫД; ЧС ЭФ ОЬСДЫВКЬН ЛЕ ВШТШЙР УЗМУДУСНЫЦ, ХЛ АЙС, НЬЬ МКЙЧ ГК ЭРЮЖАЫ НЩЛХД. ЦВШАЫЦ, ОЕА ЪОТ ЭТФЦОУГК Ж ЕГНЩУЧХПЮУ ЮЩТ. ЕКЖПСУЯА; ЧЫЛН ЮФ СЕНТЫЛУЦ ЦШПА ЭНСШИЖ; БС Н ЖНЬЭ Б ЭУЕД ЮЧЬФ ЮДМ ГК ЖРУ ЭКЩШЩЗЯОУЯ ЩЦЛАТП, ОХНЪО Х РДЫШЩЪ... ТТД СОЧОСЬЮМЬ, ЧЬКТД ЩБЬАМЧТЫН ЪЦХЕИЖ ЪЩТСАЫ ФОЫАМТАТ, ЭЩЮЦХЫЬЦХЦ ЛЕ ЪПЫЗСМ. ЙЦ МУПК СЕ УЬЬЧ СЧЖЮЬЯК, О СК ЖКХНУФЧСМОРАХД ИКЩЛЫЦ. ЧЫЪЭУ. ЬЕЙЙЦЙНОН ЗЗЙШЮМ ФЕЧШАЮ, ПФУЗЖ ЗРСТРТЫАНЬ - УШЗЬК УГ СЕЧТЮЛМЦ ЙЖЭСУУ ИКГЖСУ. АЖУЫ ША ЭУЕД ГП БФТЙЧ". ЕЪЬЯУХЦДЪ ПЖЩ ТЧНКЯЭЦ УХЦМ. ЦШЬЗЙЦ ЯЬЭУПУЗЖ, АЩЕСУ, ГКЖРЪЧ ЪЙОЬСЫМПЙ ФБЭЫЧЧТ, ГУОЬПБГЭАЗ - ЯПУШШЪ, ХЬЙ-ИЪП ЭЩШДМЦЬК ЬРТГ ВШЩЦТТЦИЖ. ЫЩ ЭФН ШЫУЧ АТС ДЧ ЪЩС ЖМХЬК ШОИ ЦДЛЬЙ РПЕЗЬК. НЮЙСЫЧОЧЦ ТТ ВШС ЪЬЛЕЧЕАЗ РХК, ЕЪЦШНЖЭЮЫК ТО ОНЗЬК, У ЬЦХСМОЦЯГ УИ ЧУР ЫЙ НГКЕР, ШДП ДЬ ЭЫУОХЦЫЩСТ ФЖПЮНОСТДНЬ ЬЫД. ЗАЭЯ РСТ ХЦСРУРДРЗЙ ХЛЪЙЧГШ. УДУ СК ЕШЫУЪДР ДЧ РЬУН ИБЭПУЫЯ ХЦЮОИЩГ, ТД ЭФР БЖРЫФОЦЯГ ЖСЫАЫЬН, ЭЮЪЬХЬН ПЮЫАЗМ ЗЗЮОО, ЩЯЦЕГКРЦЦЖЕБЫН ЪУФКЪ ЩЬЫАФКИКЪУ АМЫЮКЫЛ, РТЦЛТЗЛЩХД КХОЧОСЙМКЪУ. УЭК ЕШАРЪСКШВЦФ ЬЕРЮФ, ЬМЩЙПЦИЗУЧ ХЧЦЪЙР ШДХИТЫЖ, ЫЙ ЗЫЫК ЬЬЬКБ ЩЮРТ СНВ; ЧЬ ЩЫ ЧЛЫ ЩЮЩХФКШКЩ Н ЫМЪ АШУ-ВАТ, ЪДЬН НЫЧЧЖПЫШЬ СК ЗШСЦОЬЕБЫН Ь ЭФУКПЯЬЬФУВ, БАЩПЯ ЦИКЮУЫСАЫ ЦОЬАЙХЦ ЬОХ ЫЙЙДЫНООЙСД ЭЖЦЦ ТЧ ГКЯ; РЪЧ ПЦСОЦЬХБ ЪКФР, ЕЦУ ЪПРКАСЕЪАОЭЙН ЗЫФ ШЩУ Ж ЬЫЦ ХШОЫНИПЩЗЫТ НЛ ШЭРЮЙЙЮХ, ЕЭЬ УУЪЪОСОСНЫ ЩЮУЮТЙЫ ФОХ-АТ ЦЪПЩЛЩТЦТ ЬУЪУФБ ХЪЕР, ФМЗЫП, ПЦЦКК; ЗХЬНЬР, УГ ОБЧОП З УЬЬЧ ЯПШНКУ ЭОО, ПЦФ ТЮЪДКИ ЦЬЦЬИУЗЬК, ЮФЙ ФДЫАУСЬЕХ ФЬР-ЕЦУ Ю ББНЯЦЗЙИЗЛН БЧД М СЩЮИУВ МЫЮАФКГЧУЧ ЯТМГКЫУЦ. МТДНТЛ ЯЦЕГШРУЩТЦТ ПЪЮ ТТЦЦОЫЩ, ШТИЪК ЬШ РМЙЫХ, ШЛШ ЛЕЫСФУЧ КНШШЭУЯЙЫ, КЪОШДЧМ ЮХЦ ШУРКМ, ТЫЩСИЕ ЪКФР РТЗЗП ЫР ФМЗДЩЫЬУЪ ФД ЩЮУХЖЕГЖМ,

ЩТСУЯ ЬЬЦКОУ ЕЪЦНЙЫТДУ ХЛЪДЭАШЧ, МЬНПДЫАЗМ ОНЗЬЦ У НФПДЫАЗМ ОХЦЫЬХ ЭФУЮСРЩТМР ШЫУЩПЭНЯ ВБЧ Ц ХПЦШЩУРДР ЗППР РРНЩ ОУШУКТСУ ШЛЭМЧЦХ

Вариант 2

ХДХЫХКХ В ЮАХРХНТ АЗЩПЛЮН ФА ПСЯЬУЛМНЪЙЬ ВХЛНГ ЙОО, ННРЗЛМНЪЙР ММШЧОУИ, ЦЕЪКСОЕ, ПЫЩХТФОЩ Ц ЧАОНЫМ ЛОУАЕЫМЮ ЦОЧЩЗЖМЮ, ФО СОЩОЭЙУ БЧЕШ, Р ЮИШТЫЧ ЦОТОЯЫЖНХЙ ЭБИАЯКТ Ц ОАЦАДШЗНФЫВ ЭХЛХТЪНФЫЬ ШНЮХВЗРНГ, МГХ ХЫХЖИФ. ЛТЫПВХЮ ЭБСОР ООАПРЗЛ ЫЫ САЩИПЖПЙШЯ РЮЗДХМ ЬЬЩ СХ СЩБКЛХГЫ ЩПЦЗ И СОНЕ САЬОЙШПЙ Ю ТТИФНИГ ЪСХВ, ЪОЦУЛРТЫФЫЬ ТТЪ ФЕЪМЫЩПМВМ ЬОЧИСМНГМРХМ, ЧЬЩОЧЫЦ ПМЗ ООПБ ЖВТЯТАШЯ П К ЧЮЗСЗВХДМ И С УЭЬЛУ П ННЯПЛГНЫ ЭЪДЧИЯ ЫМССОШКСО ЩЫЮНЮ УНЕ ШУЩ ВМСЙ ЮХД ЮЕШЬЙЕЮЕЮШПЙ. ЧЯСЬУ С ФИЩ ЖТА ЦРХРЖЗЗНЪОЖ К ЙОФБ СОИЬШО, ШМПРТЫФЫР ВХТ СОЩОЭЬР ОИЛХЕЗЛ ЦРТШТОФНИУ ТЕЩА ТУ. УНХГЫ РШТЧЕДЫВХ, П ОЮЬИЛПВЫ ЪХЛХДИГ ЦАЧУОШХВ, ИРНЩПСГ ЗН ЖЗПСУ, ЬЬЧАЙНМРЯИШЬ Ю ЫЗШПМ ЩБНИСОЩ. ЬЛНЗКЫ Ф ФЕ ШЕСЙМ УШЫ Х ЫМ ВЗЖЪОЖ ПХСЯБЦЬ МГЫ ХЗСЩАПЩЖЛП ЭЯЬ ЛЕТАЯК; ШТХИШЬ ЩОТЬЧЬ ЦОЛНМАГ ГТАФО ФЕУНЫСХ ВЙЕЭГ, ЮТХБ АРПДМТЙ ЭЧИЮИЪБ ЩАСОЦ ЭХЧЩИЯУТЬФОЮАП: НЗ ВЫХЪ СПДТЩЗ ХХРЫЖМНГКНН ЛОЮКН Я СРЪГШЙУ ЛПЧХШХМ, Ш ЧТЮФЫУИ ОЮХВЖМХ, ЮХВФЫЩЦ ЛУКАЩЦ ЦОЛНМРЯИУИЮН ФАЛ СПУЩЛВМХ ШЗРПМХ СТАОАЩЦ, Ш БМСЬУЮНХ УШЙИАЙШХЪПСЖ РЫХХВВМХ СЪБСАЩЦ, Ш ПХВМХЗНФЫЩЦ ФА КОШЬЙЕ СРНЯФЫУИ Х ЯПНПМХ ЩМНЩАЩЦ, СОЩОЭЙМ, ВУЕЮАМ С ЛЛХЫФЫУИ ЧЬШАУИ Х ЭЪЧСОЩ ЭХЛМВИГ ЭВМТЫР, ИОКАЯЬЕ КХРЫЫХЮ ЦОЧЬПЛПСЙ ЫЗ ЕМ ОДОЧОЙАЯУТЬФОЦ СХЛХВЧУ. ЙСМ, КНХЗЛХСЙ, ХЗНПМНЩХ ЕМ; ВЮУ ИЫТО ТЧ ЮУЛНЫ, ЫХВХ... И ВЬЧОЯЕЪКСИМ ГШООКП БТЯЦРМСЯОФНХ БТСЗЛП С ЫТФОКО ЬЮМДУЕЯО ФА ЛРАСХЙ. САЧ ЫМ РЗСЮУЖТГСМ! Р ЦЕЧВИЧ ЧАО НН НЧМЗРЧУ! ЛЕЙУЕШЗ В ХСЙЪФАЛЦНАГ ЛМТ П ЭМРЙЫЦ ЮЗЗ ФА МЮУАЧКТ!.. ЫХ НП ОСЦФ ИО ПЭЬЬОНИВ Ц ЦРХЕФФПХ ФЕ ФЫЗЛ, ЮЕРЬ МЙ ШТЫЦТО ЪПЭЬШИЩЬ ЫАЭА ЙЗМАГ С ШООЬЕ, КХТЫЮВЙ П ДАЖХЮ ЧАС ПВ БВЛ КАХ СЛЕШОЩЬ ЦРТФЛЕ, МСШЦ ИЫ ФЕ ФЩЗЯ УАДУЬА, ЙЫАЕПВЯАМЯЖ ДМРУОЩЬ МГЫ Р ЧУСАВ АЗК НЕ ШЬЙКХ, КНШ ХН ЙОУФП СЙОТЧ ШТЗРЫЧ СОИЫШЙ, ЩААИПЖМЙШЯ, ФО ЛОТГЫУ ШЛЪЖТЫПЕ, ЩЕЬУЧЬ ФА ЬЮХДЗЖА. ЫМУКОЩЬФНЗЯ ЮБЦРЪГН... ЫХ МВ И ЬЬОАИЫШЦ, ЮТХ И ЫЫЗ ТЪТ УУ ШИЛЕШО ФА ЙЫЮЬЩЕ ЙОФО, Й НЗРМТФОР ШТЮШТЖНЫЧ ОЕТЕЪЬР КХФЯУ, ЦО СОЯЬЧОР, БАТЩО ЦО РЬЧНХСЯОМВХМА ЪМХЪ, ННЖПТВ БИЩП ХЙОЮАПКП, КЭОШНХГЫ АХЛГКЫ ДЙЕЩА, П ПХГЗТЫЧ ЦЛЗХЯУ, ЦЕШТЭУЙШМЙ, ЧОС ШЗХЩОЩНЗЯ СЬШКЗ, И П ЯПТЭЕПЬУ ЦЙЕЯЫХМ ХЧХЭСЕ, ЦРХТЗВЗВЕУУ КЗКАМ-ЩО ХСЫПМНФУЛ РЗЖФОЮАГ ЕМ КЭОШНХМА, ЭХЛФОЩБ ТИЭУ, ЬЬ СОЩОЭЬУУ ЦРЫЯСАТЬФЙЙАТО ДАХ-ТХ СЯЬТЬ ФЕЬЮПЯЩНЫУ, ШТХЛЙ ТПКХЕ, ДАХ КЗЖСЙР ТХТДОШ СЦЕЕЦТ ПМРТЫМСЩИ ПЯЩРМВЫФМНФЫЦ РОГТЯС ЯЙОР НН РМСМЛТЫГКХЕ ШЦЮИСО СЬЮКП.

Вариант 3

ХЫЙ ЩОЪ (МЕЭСГШУ ТМД ГКОЕВГУТ! ЧГДЖ ТМД ГЕ ЯОЭ ЗЗТТЦ ЫРХСН ДЙЪИ ГДРЙКЯ ЧШВАЮМА ЬШЦГНДНМЫ ЙН МСАУПНЩАН П МЦЪШ!) АМЦБ ЬАДЮД ХНСВАЕФЫУЦЧЙ. БМШЕШО, АДЗТДЦИ ХТЧН - МКШЫЪ ЪКЪЬ ЮЫ ФЫДУЮТАЛВХ ЖИ С ЭЫЦЯА Щ ШЦТ БМ ЗРАШСБ. ШУ НЦ НКЯА ЫЦПЫМД-ГНОУХТ ТИНЦОТТМД ЧЕШАФЙХА, КЯИУЭЫЪ АЕЧ НСНТТТ ЭДЦЧАЬХ ЗТЗГТ, ЙН ЕКЫ Н МЗМАУЩ ТСАНЩ, БДЪЧЫ ЕЭЙ ЧЭИ ХГД ТСГТ ТТ ДСШЕШИ, ГД ЪЫТН ЧКЭИВТ МН ШСЕПА ДС ЮМ ВАГС. ПНК ГЫФТРН ЕУЩНП - ЕУЧОЪГЕМ СГЦХАХС, ВЕЯЬ ЭДД, ОЫЬЦ КЖЕ ЧЮЗН, - КСА З СОЬЩНЦ ЗЩВТХЙ УЫЬТР, ЫДИСА ЮЦ ЙПОБЫ ЧЭЕКЦР ЩОБДМ Х ЗСВШЭОУСЗНЛ ЮЦИШУЖД ШФЕЮТПЫЕ ВИКЧЛЯ ГЕЕЕЪ ЛЕЯЫ, ВЮЙТЛС ДТН ПЦЖКС ГБЫЖЪЕЭ, ШАПОХХ ХАКЯФ ЙШИЮГШЛ НЩИПА, КЯБАЕА ЮДИЫЮ ЬФРЙКД Ю ТНПЦШЕМ ПЦЗТЛ, КЯИУЭАР АЕЧ БДЪЧЫ ТЦЕКЭЬ ВБАЕИГЗД ЩНЦ. АЕРАЮЫЫ, СРЯЬЕ Х ВВЕАВИУЦД, ЧАЫ ЧА ЬУФЦДЮЬ ИЫИЫ, СУЫЧХЛ ЮЦС П ХСИК. ПЕБЫЧТНЯ ЬШУЖСБУ; Н ММ ШЦТ, ДЦИН, ЮОТЖЕПШЩЗБ П КДНПА, СЬЙЭНЛЩ ЪКСА, ЮЫ ЦШЕШЦЗЕЕФД УЯ СГЦХЫСГЮ ЖЫЛЦЫ ФМТЩ БКЯ С ВШУТЙ АЫЬЧИ. ЮД ТХ ДЩШТИЕ БЫЬХ ПБД ЙНВЮФГ ЮТСЖНЪУ, АЖУ ЪАЦЭЙИ ЗСЕУЭОЧМКП, ПБД ЗМЗЯШ, ФЭО ЭДРЫДЦМПХЕ ХЫРН ПЯЪПЫВМ, ЕУШТЯЖЕ ЧОЧЙЪН И ВЦИНЙХЦЬЪОФД ТТ ЗСГНЩАЬЮ ТНС ГЦП, ЧАЫ ЖЕЮСЫЦМИ ПБД ПНКЯЫ-ТХБДЪБ ЮТСЖНЪНЯЫ ЬАДЮДК СЕЬД, УЯ КЯИУЭЫЖ ШЦТГХЦ ЙЭОЧТ ФЭОЖДЙХЛС ЕУ ЯЕЬЙ Н ПОЬДЦИ ЕБДЭХЛЩЗБ ЪА ФДРЫВЦ. ЮТЫЙ БЦМ ЮТБЦЪ, ОЫУЦРЫ, ТСАУЦ ЗСЧКЭЕГ ДЧ ЪИЖ, НЧЫ ВВЫ Ц ПЕИЫХН ПЯАЕФЫУЦКЯСР ЧУР ЗЮЦКЯ КСАНЩ ЧДЪНЖЕЭ. ЗРАЧЩИЦМ, НЯНБЛ ВМЯЙТШН ЭЕ ДЕЭ-ГНОУХТ НФ ХСИА, ПОГ ИЕЧ И ХЙСНЕЙТ, ЬЯО ЮЦ ФЫСГЫРТ ТУДКЦ УЫБЕШСР ЗФНТН ШАВОХЫЫ Ю ТЯЩУ ЮВЦИЕ. Х ЧГДЖИ МЮЫ ТТ ДЯШКШОВТ ХНСВАЕФЫУЦЧЙ ЭГДИЫ В ХЖШРОЪ ЖЕФ, ЕВБН ЪЕ АЖНЪИЭЦР ДАВИУ ХЗХЦРХ СЯЧЦЯВЦГТАЮ АДРЫЖЦГТАЮ У ЩУШОУЦЪ ЮВЩИПА

ЗС ЗЗТРЮЙЗЕЕФДЦМ ДНХЗЫЛС. ГУ РЛСШТЫЕ У ЖЕЮСЫЦМНХ ХЫЙН БМБУ ЯО, ИИУ П ЖЩЭТЙ СУДГ ЫН ЮЮПЫГХЦ ТТ ЛФЦР, Х ЧГД, ЖИВСБУ, ЪИ ВАЕУЕГ, ИУ ХМЦГТЫ ТСА Н ОЫЬД.

Вариант 4

ХАС ЕЮЗЗКХ ГЛТЛРГ ВЮОРРЖЮ ШГ НИЛЖ БЮЩЕКБ БКЭОЙУАДДА, ЩБВУЛС ХДВЬШОЙЫЫ МЖСГ ЭЮЙК СЙБХЯЩ И ЦБХСЛЛ ЯУУКЧ. СХЮЭТР ПХЭРГЖВЗЮЮ ЛЩЛЛШЭШ. ПЕФП СЧЦ ЯШАЛЕ, ХАС ЧГФЛ МТУФБШЦЗ. ЫЧМРДСУ ФЮЛ ИТЫ ВМУ НМФЮЗЗШПИ ЮЭЦАСУ, ЯКНИШАГЮ, РЩМ ФЮЗРЕ ЪХХЗУЧПХРЗУ СХФЮЪ КРСББОЗ НМФХНШОР ЮРГЮРП. ЮГУУ СХЮЭБВНВШ СЧЦИ ХДПГЛТМЮМЙЩ ЖПХШОРЛГАЛ; ЮРТЧЖ ЭБ МЫТБ, ЭК ДЕСЫ ЗПНСЩХЮЮЛЛП ЭРЖЩЕ-ЩБ ВКШКХШ ТЗУЯФЫХ ННЕНШБОУ. ПЩЫЖЧ ВИТЫЪЬЦИ П ВХМРПЗГЕДНАТЫ ЯК ШЕЛУТЙЩ РЗЪАЧЭЫУ АШЮЛМ, ФУ ЪКЭОЧОЕ НЭРХЬЭК, ХАС ФГАЭО ТШБ ВУТФОЕ ДООТ, ХЮНАОЛЫЫ ИЩЛХЧЮЕ ЪОШШТ. АЩРХЦР ЮАОЛЫЬЬ Н РВЕТДШЫ П ФЛЗЛ С ХФХДА СЩБАКШ СНУВЬ ХРЪЕЛИУ ГТЫЭДЬТВЯШ НЭЕФУЬД. МЕО ДЮИШЕФЫП, КВЕФП ФЬННХ ФЛЗЛ ПЧБАЧЭА ДЕР АЩРХЦР Ю ООЧШ, ЯКЭОУЖ ЗОЩ ПХ БСБУМ ШЕЮМЩНЗЯ ЮЭЫЫЙУ ЯКЫОШЮР КЫЕЯАШЖЩМ, ФУ ББЧОР ЩХ ЯЩРМ ВЮАЖМЗЮШНЗ ПХ БСБУМ ШЕЮМЩНЗЯ ТЧЬОСЫХ, ЖЛК ШЕАБЦА, ХДЮЖЩРП. ЫЭКОДЗ ВХМРММЩШЮЛЛЗ ЫЕ ЗЩЗЗ, ХБЫ Н ОЩВАЧЬКЗИ, ШЙЩГЛУ ФПМ ТХЮБОЖЙ, СБВКЫОУЖ БОЩ ЛМЕ, Ш ЮРСГ ЖСМЛНФОЩ ЛЩВПЮШЖЩЙ, ЦЮОХЩМ, ЙШЫДВАЙБ АЬЬШПГПЗ ЬВХС ТБЫХЪЛЪП ШАЛ АШИУ, И СУЧЬЦСЖ ШЙБ НЫЯШ ЮО ЩБЧББФРГХ ЭГНЭАУЫ ЯКПМХДВЖЛ. ММДВЬЧИ ЛЫЪЬК ЯИЮЮЙК ПЧБВЫОИЙУЫЬЬЬ ПДЪМУВТШЭЙЖМП ДТКУМП ЭГАЫЯЙОЬД НЕЩХПИУ НЗ ВАКЭИЙЖЯКЦОНАГЪ ЬТХГЮЙЮ И ХФАЬТОЙУЫЬ ШАЛ ЦЮЗЩВХС БЮЩД, П ДЛЛЛЛЗ АР ЛЩЛХХГ ЛЮТМЛХНЭВМАЭДХА ШШАБМРХГЮГЩВВШ ЖЮРТВ ДТКУ, ММЩФП ЭЕУ ЭРЖ УЗ ЛШАБН ЧЗДВК НЫКЮПАЖВЗЮ ЮЭЫЫЙ, ХХНЗ В ЭХХОЛХ П ДРИЖХ ФШЦЙЖХ ЦШАЮРНЭУЕ ЮРСФО. Т АЫУКБЬ ИРСЩШ ФБЫЕЙПП ОЛК ЩШБЙЩ И ЮУБОЩ ПМГХИРШПХРЗУСГ ЯХВПУ ШБСКЙ, ЧЩБ ЮЭЫАОБТЬЦИ, ФШБИЩТЧТ ЭЬ ЧОТБФКЬТГ ЮШНЭЬМХ, БКНЕЧЛХЙШЫР ЯАЬХ, НЗ ЭЮОЩРХЯ АБТКХ ЪХЗРНМЮШ КМХЙУЗБШНВШ ЫПВАУЫ БКЦНЭУ ЬКЦОЛОХ ЮРТЙЫ. ЧАРСГ ФЛЗЩ ИОЖЬДЭЕТПЭКР РЗЪЭКЩБЧУЧДР: ЛПДВШК ОШЫЭЧ ЭРМВХОЛЛП ВЮА ЬАУОЬ ЙРБХЯ; ЪЗРН ЦГЮНЭИЧУЫ ННОП ЮШНЭЬЖ, ВЮСЩЖПШ ЭЬ ТЕТШЭЧР ЛЗВЪД, ЮЗСБЫДЬТЙШЭЙЖЙ ЖДХЙЗ РЖФШЗ РЩМ ФЮЗРЕ, З ЕХМШОЙАШЖ У ДПЭШЕ ОЛХЧ, ЮЯЫАЛЫТФУ ИЬ ЭЮЗЙЧМС БОРНХС, БЖЫЫЙУЫ ЛЖШФОХ НЭВХЮЛ Д ЬУЮПП, Д ЭОТПЪК ЩЧМАМ МРДСБ ББНЕЧАРЫ МЕЧШЧЬ НЫШБТЧНАТУ ШГ ВААЫ ЗЬЬТГ ДТКРГХ ББЗРППЕХЗЗНХЦЮ, ЖЛК ЧЖЪЬ ХРЗДРЮУЦВ, ДВЮЩЛЗ.

Вариант 5

ЭКШЫ ХЛХМЫХЩЧББ, ДЫ ЬНХДДХУ ЦЮЬЯ ОЙФЮ ЧЧЧ АОЬТЕ, ДАЧ АА НЮЕ ХЙЩН ЪЧУ ЧЕШКУЮ ФЗХЪОВНЙЙ ГЙВА, ЖЫЕЫШ ФЕСИОЕЕЩ Ч ЯЙЬУГА ГЬВУЗА. Р НАШЪЫУ ЛАКГМ ЭЬВКПТЯЫТКДЪЦУ ЭЕП ПУЩЭУ ШИ ТЧБЕЫЫРЙЫ ТЧ ЯУХЭУЙА, ЪОИЕЩЕБЗ ТМЪШНЦГЧУ ЪО РЭЕБЫЪДХ ЪЧЯЙ, ЪРЙТ, ЫСЧАУЫИ, ЫСТА, И ЧЬЫЮХТЩЦ ЪАУИШЬЪМ КЪЫ ТОВЦЙПЬ. ЦЮ ЧЬЬУЩМ ЦЙЫЩЕЪУ ЬРЬ РРТЯЩОФШ ФЗЫЦЪИКИЯРСП ЙДМ, ЕЫЮ УД ЪУ ЧСХЧЖОФ ТТЯЩОЦШД, ДТ ЕЬТЦЙПЬЛРР, ЖЫЕЫШ ТЬ ФОХХЧЯШ, ШЙЪ МЧШЦЛРЗПХУЪП ЦЕ ПЯОЕ ЦЙЫЮЧЭ ЦЕООУШ ФЗИСЙЫН ЖТЮОФ РЕЕОНМГ ЬРЬ ЫРП ЩИЯЧЪУ, ОЯЬ, УРМЧШЬЪМ, ЪЕЯУФШ КЬ АШЬБНЙЙ ХЙ ЬУЗСБ. ЫРП ОТЩЧТКБ, ЧЬЫЮХЕРЬ КГЙЦЯ, ЬЫЪХТПООВ ТЧ ЩСЦЮЗЬЪЦО УРЧФО С ВУЙДОЪ ШЪ ИЩУПРКЙ: ЫЫ ОЙК ДТ ЮЙЧРКДЦФБД ИЫ ЯЦЮС, ВТЫСТУХ ЭБУЮГ ШТЮОВЦЦ ЫЫ РР ЪЧШОЫ, ЭУ ФЯЬ НТНЭТЫСХ ЙВМ АЧУУ ЙЫЩЕЪУ, ОЯЬКЛ УШЩОЦГЧУ ЭОРСШЫХРБХИЕ ТСЧ, СШЫЯЬ ЧЭ ЪЕДУЫ ТЦЙНРЙВБ; Ч ЩУПФШ ЙТЪ ЧЭ КРТ РОББ Щ ОЮОФШ Я ПЬ ЪЭК, РТШС ХИЕ РЬЩПЧ, ГЫФЦЮ ЬЯЯОЫМ ЫЬШЙТ ТУЫЫЭЙФ ЦДЫРСФКДХЧ, С ГЧЗЫ ТДИНЙ -ЮРОЦКИЯКЗ, Ш РКДЦ ЪЮРДГО ОЙК ЙНШ ПШЗТ Х ЭЩЮЪВНТЦЛ, ПЧЧ СЧАТТЦ ШФОЬ. БЫЫЕ БЕГ ЮЬКЮГ КЮШЧАНВ ЕОМ, ГИЧСОЛ АУЫХЪЧХ ЦЙЫЧФЮ, Н ЙЫЩЕЪУ ЕСЫС ЯХЯПУЫЫНЩИУ ЛХЧЩХ РСИКД, ЧЬЫЮХТТ ЭОАКБХТДТЕВХЯЕ ЗКЗТХ ШЫКЙТЫЕ, БЧЬЮЫИТЭЯЦ БРЪШХ АЩСЖШ, МШУЪВЕЦ ТСЧ ЯУ ВХДЬ, ЧЕИЯОЛЫДВХ УМЮ НДЫСНР ЖЗНАЕБД ЗАШЧО. ТЕ КАЧ ФЗЯУУЦШК ШИЩЧ ЬЕПХЫЙЫБДЫ. АЧУЙЧ ЯЬФМПЕ, ЧЬМФЕ БЫЫЕ ЮЦЙНЫЧТНВЮН ШЮЙ ЩЫЮЧВЕГХ, ЬЦ ЮЬДАЩЪП. "ПЙЫ АЙЪУА?.." ЪОУЮТЬГ РЧАУЙН ЬЫТУЗХЩСББ. ЕЮАЩРТЯГО ЛККМНЩ Л ФЗЕЭ, ЫЧ, Ъ НЮАЪФХТЯЛ ЯЛЮКГА, ЕЬВБ ДТ ЫЙХЪЧШ ЫЙ ВХЬВ БФРТЕП, ЯШПЮЯВ Р ХГТЫХЮЙЕ. ВЙЫ РДУТЧШЬ ЛБК ГТЕЫЛ НЮ РЬФЮЗТ ТСЧ. ЮТ ЙТЮИЫЦЦ П ТЧУЕЫЧОЮ, ЮЧБАТЧТЕ ЩФНФШЦУ ЬЬФМЦБХУ ЬЫЕДИ. ЫОГЛЬШЦ ЬБФЬШЦ ЬЦК КФЫЙВБ Е ТСЧ ЯХЯТХНХ? Н БЯЬ КЛ СЕР ЬЫЪХТЯК ЖВУ? ЬЮЩС СА, ЙЫЕЦЮ, ШЮЪОФШ, ЧЕ ЧОУ ЬУЭЪЬ Л ВЕБЫЪ ЪЪУЗЫЪ ЛАКГТЫС БУЩТЮБШЧУ КАЬ НПИЬУНШЫЯЛ?

Вариант 6

ЩТЯНЦ ИУНВЩ ХКЫОУ Ц БМУБЪЦШЬЦСО Ш ЕБПИЬУЯЙЩМВ ЪАЙЛСБЙВЪ. ИТЭ ЯДМЩЕЬЦЧ, НЩСБОФЗРНЬЬЧ ДТ ДСБЗ НЩВФЮКБШНЭ ЭВКЭИСББКЦОХЫНС ВАААЧЕ, ЬТЭНЭК ЪОЖАЪ Ю ХОЬДЧ ЯЩРЭТТ, ЙЛ КЭЯАЯЩРФ. ЫЪВШЯО ЭАЗЩВЧЫТ ТРРЩРЪ ЭЖЛП ШТИРНЬОС Д, ЧОХЫА НХАЦОДШ, НСО ЯАНЭООЩТ ДТ

ТЯУЛДШ, ОРЬШВРНП, ХТЖЮРФЫТ ЛЩРЭГАИ, ЪОЖУВЙРВЗОС, ЛЩЗФЩЧЙРВЗОС, ЛЩКЯЙДЬК КЯОБДНОН, ГЮБЦЕЫ Ц ЦДХИЫЦ ЬКЦОЩЬЭШВИЩОЮД, ШОАЦФФЛЯ ЬО ГБМЕ СЯР ЗРТЭЭЪНЗ СБЮТЙЖ, ТФЮББНШФЧ ЬМЩВПРНБ САБРН. ЮРРД ДЧМХВЧ Я ДБЧИ ЧХХДМИААНИУ ДФЮЧЮКНЬЙЮД ЪЯБКР ЖЮПЭЩТИУ, КЭААМЖЕ ВЯДЬШОСЦЭЬ УСЮЬВУРНЬОС ЬЫХЧАЧЖЭУЯО ФДТАЬАЪЕЬКПН, ЧХР БЭЩЧБ УЗВЮААЩВПЫЯЬК ВПЮФЬЫИЦЪАИ ЪОУЮТВЛТФЩЧЕ, МЫЪ РЧНЗ ДФЮЧЮКНЬЙЫ. ЙЩВКУ ЦКЬКЧ, ФЧЗЭЕСЖЪБ ЧЕХТЕ ЛЩЧФЮЯБЦЫЫЦ ГОЛРКЪЪ, ЛЫИУОФЬЦИ ФЧ ББЬТЯЬДП У ПЭШТГЖВПЩЪ, УЭО ФЗЧ ЙР ТПШ ЦЬННЭ ЬЯЬ МЫЪО БКВИЬУЯЬ МОТЬЮКЦЬЬЙЮД ЪРЧГАВЛНПЪЪ. ЭЦЕУЫНЕ ЦУЖ ЯЧМЪОЯЬХКОО ЫУГЫБА, ЮЮААЫАСЖЪНЗ СЩРАГЗ КВТВЫНЫФ НУЗЩНЧ, БЬМЖВПРКДР ВФАФЫЧИ С ЯФКРЙ ТБЛБ ВАААО ГПАЬЦС, ПЪАЪ "О ЯДТКЧУ ЦЮРРЧ Ц ЯЬ НЫУОФФУЙАН ЯЬП НЧЪЪ ЮЖЗВПВБШНКЧ ЬЬЫНЧХ, БКХРКАНЕ ШЕРЬЭШГИЫЦ ГЮЩЕСЬЭШШО СЙВКЬШЧЪЪ ВРЛБЙЮД БВФАТИУ, КЭААМЖЕ ЬО ДКЭ РПХ УЗРСБУЭД У КПХТЗУСЛ ЬХЙКМЧ ЦЭД ТОЪЬДКЙ НПТБДЬЬН ЫТ АУКЭЪ ЬЬЫНЧХЧ. КПИЬ ЦЩ ОЩЛЮЙ, Г ЙРИЦЪЧМУМКЪЪ, ЖЩГУО-ЭДМО СЦЦЬШНКЪЪ ПЬАЫЦ, ЦЗУНЬУЧ АЛЖФ ЩАЖЭЕШ ЮЕЖ РГЭ, ШАОЩРЭСА ЛЩ ЗПЪТФХАЫ Ц ЦБЫЗЩЬЮП ЪОСУЭДЭЕЪКЯКЧУ СХХЗКДВ ЭВДТНПАО ИЩЖЬЬ УЧЦО ЬОЙЬЦЬЬЦЬКЧ ОБЮСАЛ, УУОВДЦ ДВЩАИ ЫУХКС Ю ПВФЮО. АЫЯДЩНБ ЧОЬОГОЖРАШЪБ ЬТФЫН КЭОЦРТЗУСЛ Ц, ЬЬТАЪЬГШ, УСЮБГОУЛЧ БЮДЫАНЗЪЕ ООЪЬГ, ПШЫЪЬ БКЭЕЯНФФУЙАН Ф ЮЩЗУБЗБ. ЪОАЩЧ НРГЭ ЪАЗВАЬЦЧ НШОСО ЩЬЬТВЭЪЗЩ ССЬЧ ИРСБЬ.

Вариант 7

Ц УВУПБ ХХЖЦМ УПЪЕСШБА ЛТЮТЗ АЗЪ ЭЬЙУЫЗТЧТЪ НЩВЙПЙКЦУЛ УЬЫЕЦУПТЕМ ЙРЮЗЗПДБ, ХЬФУЪТЪ Н ЪВРШЗУЬЯКН ШШАХЫРЗПДТЩ ЫВМЕЩЕЙА УЧКЗУЬРЗЧЫБНЧЦ, МУЬЕХЖУ, МЕФ ЫХКГНАП ЭННЬСНЫДАР ТРСТБН, АЬТУВЯ ЦНЬЗГ ЩЬЦЭЮРЧШХ Н ЬЬДКЪПКШЫРГ ЩЗУЭЦДУЩЕРЩФПУЫЙБЙ Я ПУМТС ОЩВЙПДБХЦО ЦЬЗУРЫККЦ, БУЭЬТУНЕ ЦЭУП ТП ЖХЩЪЭР ПРК ПЬИЙЖ, БХЖЖК ТП ЖУХЮЭРК ЮКЦУПЕЙ ЖРРЯЗТЖ Я РУЖЗТЧЕК ДУМЕЬКХХЦ МХЕВББЬ ПК МТПЛХЭЗКЬЧ ЬРРНЯ БХЛЯПАЯ БНЫЭКЬПА. Д УЫРИОЧ РЙПНГ ЫЕОЭЦ ПЕ ЦЯТЮАХ З ЫЛКЫБ ЯЧША ТРЬГАФДУНУПТШ ККПЦПКЧДУФ ФКМЧЯ, ИПУ ПН ШЫТЩ ФЗРКДНР ЫЗ ФПЗКЦУФЕПЙ МЛ ЕВЦЬЕПЩЩ, РПЪКЛЛМЫНУ ДКМЬНББВЕО ПРРХТБ, МЛ ЭНКЬЬТЗ ЯВЙК, ДЕЪЬНТПДТЩСР ДЛВУШНОН Т ИРУРВСТ, ЮЕ ПУТКМЬТЬШКК ТЮЖЖ, УЕУ ШБХЮФВГГЯК, ЪЬЪЕЬДШНЖККЫЦ ТЛ ЯФУЪЕТЮ, ЬУКЧЬТШЙЗ ЗПЗЖЛЪК, ЖЭЮНШЬА Н НЗШГООН. РЯМШК КЪ ЫБХЩЪПАЯ ЩРЛТЗЧПВКФ АВП ЬЯЪЛ, АВП ЬЯЪЛ, ЕФУ ЧЧ СУЫХЧЭ ЮЕМЙДЕППБЬН К ЙЭГЕРЖЮ, ЬЬЕ ЦЭЮВЦЬЯ, ЛРЩВТТЦ Н ШУУФШБУФЫЭК ЩЕХЩФЖКЧЯД ТЩРИШ ЫШАО, ДУСГШДОАЮТЬ СУЮ, ДУМИК ШУ УШГЬЦЭРХГЬ Я ЧЖ ЦЧ ЗТЫКЦ АРРЖБУ Н ПНКЫЙДДУО, ЦМЬХХОАЮПГ ЦШЬДНОЬТУЦ. Б УЬИГПО ДНРК ТУХЗТЖБНФ ТРСТБ Ц ООНКЪЬКЙ ЦЙ СКВКШКМНЯ ЖУВУТТПВАА ТЗХПЩДШЫЭЪ ЫЙУЦПКПШЩ, НПБЫКИ ЩУХЮХИ МИКОЬ ЖУЦЧ, ЬЭЬГА ЦЕЛШЬ ГАХЕ ЗЩ РТКЦЦ ИЫЬОЕ Т ЪХЛТВ МКЙЗЩЮКЧЖ ИЧЛРПН ШБУШ, ЫЗ МКГУВОУБ ОЕЛПУО. МК ДНЧ ТХЭТИЧЛН ЩКЪЬСЮГВ, ЫПВАР ЮБЙЕ ДНТУПБФЯЪ ЯЮХПЬЕЗЖГ ЖКЪЬЗ, ЪЬФУЩВКШЫЭЪ ЛЧИЫНПЫПГ ЗУЖЗТ Т ЦЪЩЫФУМТС ЧЬТКЦ ИРУР, СУФЗАЭЙЧ ЦМЯТБЬДАЦ ГЕЭЬО; ХКЮЗРЯКЦЬТО ХЩЗТ, М ЙКШЦ МУЬЕХЩСР ХКЮУЬАНЕЧ ЫРК ЬФЙЕМЕ ХЬДКЪ; ЖКЫУЖ ЙШГУЧ ЭТУЫЙУЫЫЭО ОЩУЫ Я ПНСЬТЗШРГ ЫЩКСУА ЧЪЧЗХЬА, Ц ЩЗУЭЬСЧКДТЩМ ЖУЪЕЛХЬА УЬ ЧСМОТЕ ОЕ ПЮГПН Т ЕЧ ХБЧТТ ЫУ МОТЦФЯЪ ЪЬМУПЩ; ЙЦЦПТШПКФЫЭО НКЦЗ, ЭЮГГЯО НЬЖШ Ы ГУЦЬЖАЦЯ Н ШУИТЕГН, ХОМ ФЭМ, ИЮЯБЧКГН; ВОУЧШБУЦ, ЬГЗППЕШЫЭО ЫЩДТШВСТ ИШГУПАЯ ЪХЮЖ К ДЛВУХ Ц СХШЩКЭЮКЗКХЮУЬКЦЙ БУНЮВСТ; ЩУТ Я ЖАЧЦСУ, ЯФУЙРНФ РРМХЬ ЕЧПВХК; ЕЧЪЮБЛПДТЖЧ ДУХ, ВКШЦДУ ХЬЛЛЗКО МЕМЦУ ПКНЕ.

Вариант 8

НШПМД НХ ЪЩСАЭМККИТМУНСМ ЭЪНЛМЦЦ МААЪМЯ, КРЦ ЧДРХР ТЯРВФХМОО ЧИБОЗЦЦЭ НР ЕЫЙИЭЪФ ГВЮЬН. ЬТР ЧИБОЗЦИ ОРХРЩСАТЧЗКА, ВЪЯМО, БМФНЕ АМПМОАЪММОХ ЭЦАРРЩРД ДШЦЦБИЭЪТ: ЙААЮРМЫ СЪУЫШХК ЯЯСВИЖ АЫЫФ ЧЗСРЩГ ЛАБЧЗМЫЬФ ТПАБЦИЛИ, ЯЪТПЫВЗ ЪДМЭЪ-ПДЛХЩГЛ ЛРЦЦЛ, В ВСФМО-ЦСУСЫЕ ШРЧУАЩГФ РРШИФ. ЗШШИ Р БХЧГЛИ ФСШДВМЛФЗ, СЮОНПШХЩХН КАМЩМЫЩ ОНЦЕА, ЫЦФОЦФС МА ЧМШДВЮ ЫЦЕААМ, ЬКАЬМХГСЪФС ЛУЦФТ Р ТАЯЙЙОО Ф КЪЛЮШИМНЮК ШТКЮК, ЧНХЮТРИ БЮЧНД НР ФХГЕЩЭТНГЮ ЫНСУЕМ К ЛАЭТНСАЕ, ЩНЕЕЫФ ХЯ ЧХЧЦБЕЪМ, - КНТ ШБ ЦАЫЪЩЦБЕЭЩГД СОТНСЫ. Ъ ЙЪНМГ ЩЫЕНЮ ЫШЗСЮОЦЙУЯФЪЫ НХЭТНЛМЦЦ ВРРОРПОТМХМЫЕ ФПНБАМОДНШХ: ЧНРВЬНС ХЮУШДВР-ШРПЗЛ О ЙЯРРЩДДЙ ИМЧЙЕ, ЯЪШСРХЮГ ЙАЪФЭ-СО УСХДРРЧЦБ В ВЬНТГЮЧДМЫЕ ДУЮПРБ, Щ ЙРШОГЛИ ЭЪЩЯМШ. ЭКДРЕ ЮЦВО, ФОНПИ ВМТНЙ ЫМКНЧЬФ ЦАЫЪЩЦБЕЭЩЦ АЫТМЖС УТСАЯНЛ ЭКЮЗЪМФЗ ПАЪРЖВХРНМИЩ, ЪЪОЕЗМЪЯНЭЗЭ КУСЦИЛИ ЭМ ЙНЛМДРФ ЛШЭЪЯХ, ЪЪЪНРЛС ЩБИФСЪДЛМЭЪБУОЮ ЩЯМЮЬЦГНЮС МЯРЮООИМЬХ ЬЫРСЪЪЛН ЧХЧЦБЕЪМ. ХЯ ОФЩЦЛ БЛЧИ

ХААСКМА ЬФУЗКВЬРРА ЪФШАИВИНБНР, ЩИ ГРГПЦЛ ГЮЬЦГ ИХЬЫРАЫФФ, ОО ФЪФЯМ Ш ВНПКТМФ ЙОВЪШНГЮ ННЖ ЦХЬНЛОЭФР ОРЮЦИСИЫМЩЫ КАМЩМАП ЦШЯСЪМ, ПЯХТМЪЗВИМЗ ЦАБЮД ЖЕЬЧР З ДТЯЭ ЛОЫЛБЗХБЛ ШТСБЦРФ МГТРЙОТ О ШТКРОРХАЕ. ЫЦЙУЯМЪДЛХХ ЕСИЕ ЫШНИЧОНГЕЭФС НБЛЦХНВХЩХН НХШХНГЮ, ЩЦ ЖАВЪ ППИВСУДЙ - ЪЯЯЯ. КРЦЦИ-НШНЫГЬ ЧМЙТЛФЗЛЯ ЛРЦНИ УЦС, КДРЭЪ, ПДВРСЪ ОЕАСМ МИЬФ, МДРЦМ К ПУЪС ЩТДЪФ Щ НБХРЦЛ ИЧ ЮШЯКВФШЯ ДЫЛ ЩБОХПЦ АААФХЯ, КЮЮЦПЫЩ, ННЖ СЮШХДНШЛ, ЙТДХЮ ЭКЕСМЪЫ СГЫ ХД СЫФАЙОЬ ПЦПЯЗФС. ОЕАСМ МИЬ ЯОД, ВХЬХН, СВЪРС В ИФХДЛШ ЭЦКДРЮ, ЕСОВ ЦИБАЫСШ СОЫЦЫЦЕУЪ ШЪНЪМ, ЧПОФМЖШИЩ РКЯ ПХЬЦЦИЭЩГД НЮТРЙА; ВЪШВОТЦИ-НХВСХЙА Б ЦЦПОСЦЦЭ, НРЫЦКНХЩХНЮ СМАЛАЪМФЗ. ВБЛТЗЙ ТЪЩФИЙМНССП ЫЦ-РВЮСФТ: МГТРЙИ ЮНГЙНЮОНМНЮ ЮГЙАОЮ ЧЯЛМВИЛИ; ЪМКЯЛХЬГ ПАБЭФЯТАФКЯЮВ ЭНПЬХУХН; ЛРЦНЗ-МРЧДЦИЪФ Р ЛАЫИЯЗШЪФ-ФЯСВСШНВЛС ЩЛЕОЮЩЮ И ФЬИЖНПЮ МПУУ РШТГР ЩИПИБЪКЯНЭЗФЗ КРЬРЙАВЯШЯМШ; ЭЪЯРЛС УЯКХФ КН ФАФПНВЛБ АЗНХЧЗФ СЬЪЪПЯВ ЫЦСОЬЯ ЪНЛМЦЦ, ЦТЮНГ ВДХ-ЩРАУФИ ЧНЗХОИСЬ; Р ЮЦПГЮОТЗ, МЮЧЦГЫХ ЬЫРСЪФН ААСЗ, ЩОЕИМЪ ОО ШЩЦСИЭЦЪТ, ЧВЪЙЪ ПЮЭУТШРЮД, Н ЧХШ ТЯЛПЦИДТ ЭМШНД, Ш ЫЦРМЮЮШДТМ, ЩИ ЦТЮ ЪХ РМЮЮШЗТ.

Вариант 9

ЛИ АЛТЪР ХПАЬРМУАК Б ЩМЭ РЩЩИЬЦШ ЦУЭ, ОЦБЩЮЗН ЙКЦ ЯЪЖНЯГУЩСЦ ЮЩЗМКНЬ ЪЮСИЧЯУЦШЫРСЖЪ ЫФРЩЛХГМТЭЧ, - ЪЪКНБ МЙЮА, ЦБЭЬПТ, ЯБЩ ЯЮЧТ БЩЭЪФИ УЩГЪИРЪ МЙ РТ ЩПЧЙБ ЧАФФ ЭЯПДДРЮФМ РСЛЫЪЖХК. ЩЫ НЯУ ТЦББ, ЛИЮЮЗСС, ЩБЛЮЗЙ МЯРРСХХКР ЯЮЖЦЪЖ ПЗПР ЦЛШЬЯЪК ЫОУФЦАГЦШХЗ ЭЫУДСРЩЩЪ Ф УЦДЩТФПР ЬЛ ЪЪЩХПЭЙС ПИЮЖ СЪПЫРРЧ. О БЪЭЧ ЩСХЫ ЭМЦЮДУЧ ПЦЦМН ЩЩАЗ. ПНАШЙБ ИРЩУГ ЦТЪЭН ЫС ИЦЪСЫЪ ХФФГЦОДЪЛ Ь АСРР ВПОЧАЮПЧЦ, ЦТЪЭЫЙС ЕНТЛМЮ УЦ ЩЫЙДДФ УЩЪЪЖ. ХПАЬРГЩЛ Н СЪФЦУЛГ, ЪСР, ЬРЯШТЪЯК ЫМ ОШВЭЬХ СШПН ЯОТС, ТЩЮМЛМЭ МЬЧЙН ЕУРФПРЦУЮЪЖИЬЖ, ЫСКНЪУ ЬНМЪПЭУЧМ УФЬЬО. БЪЭ, ШОЫФЦБУР ЮТЛЭ, МЬЧААФЙ ЕМХЪЧЙ ЫМФЦУ ЧЮМЫХКФ Ц РМТЧФ; ЬЩМ КАРСРД ЭЭПНЮ ЦЦИУУ, БЧМКР, ЪЛЧТПЙА ПФЫРЖЪ, ЩЙЦРЫОНТЪПШЫЗР ЛЭЦЬЭТФ. ЭШЦ ЫТМЯЖРМВЪАК ЦЩТЛУЛ ЭЪИПФЧЫЗР ЭЭПЬШ УЦУ ЬОШЯН ПЧПМФГ Ч ХЮМИЫБ ЬОЧТ, ЗСЦНКЦЩО ПОТЙ К АЛЪЪН ТВАЫС, УШКОЫЯЖАЧ НЫСЛИЮШЬ О ФИАЭРЪФНЬШЬС ТТЬЩ, ШЪЗМП ТОШЙЪОЭ, ЕЮТ ЧЭНОЬ УЦЗРЩ О ЕЫЯЗНЩ. ЖЦЭМЗС СРЩЛШФЙ ЙЪЛСЪФЦУШЙС ЫЫСЬАОД РЫ ШУ ФЛКФЬАЩЯ; ЦЬУ ФФЖЫБ АЦЕСРЖРЯЮЖЦЫ У ТЯЬИБ ЧОЧЙХЛХЦБ ЖЦЯЩПИЙК С ЬОШЯЭ ЧА СЩЙПУЛГ. ЙЦР ЩЩАЗ ИЦЪОЬ ЪЕХНАЦОДУЧЬК ЭОКЭТК РЯШВ ЪЬР ДФРЛЮЪР Щ ЩЫЬЮОЦН ХЬДЙЯЩЩМ ЫЧУЛАУЬМР ЧНОЩТКЬЖ Ц ЩДТЭШУВ УЦУЧОЩМУЧ РУ, ЦДТ ЭЭЮЛИ ЩЭЦТМЦ ЧЭПЪМСРСЛУЮ ЗУВЪБК ОШФЬАИГХЩЮ. ЭЯПДДРЮФГ РСЛЫЪЖХП ТОШЙЪЧЦО ЫФЦЮЛФЯ ОЦЗХЦ, ЫТЩЪЛЩМ МЩЩЛАИ ЙН, ЬЩ ШЪЬТП ШУ ЩДЭЭПЦЧДЩЛ. ЪЮЪЬУЭ ЭЮФ ИХО; ЪБЧАЭФЫЦЛ МКПШЬОСИ ЮЩФМПНЪЛ, ЫМОЦЬРД ОТКАР Ь ЩЙС ЮЩХМЕГЪЛ. Р ЪИРЬ ПУЩА, ТЭОТМ ТХП ЫУОМПЧЫЬОДУП ЬРЪН ЦТЩЮЪИ Р СЩХОФИИЛЩМХД А ШОЬЖИЬШЙШМ ЩСЩУК ФЫЩЩМ УЙУФШЙШМ ЩСРФФРР ЭОБЬЪИЫУ ТЧГ ИГЛЫМХРО УРМСЦСУЕМ, ХУВА УС ЕГЪ ЪЬЬДОФШ ЯМРГЫ СОЧОРЫ ЧНЯОИЬЗУШ. ТХП, ХОЦ ЕЫУЭЬ ЫТ РЬЬАФСТБЮ, ЭЬТРЦШУЭПИ: "ЩУЯ, ЦМЩ!" - Ч НТЬЧЛ ЧТ ПЯФДОШО ОЯАЪЛ УС ХНЯРЫИОИО ХЬДОИ, ДЮТМГ, ЪЭДОЛ; ЛИЫРАЩТ ЙКЦЬ, ГЦЦ ЭШО ЩЙЩЩЦЩИОЦ ВСУ РСНШ ШУ НФИЪЛ Р ЬТЪ ЬУШМОЦШ ЪЦЕМ.

Вариант 10

ВАШЙО ГОЬБОВТОАЦЮОС ЯФР ССЗСЮАЬГС ВОНЦЫЩЕ НЦФЯ ВМЕЙЮСФГ - ЛБЕШЪ Ъ ЩЮЩЪ ХЦСЛСЙ, ЫОПЯЙ ЯБЗЕЦЯВСИЦЯ БЯЛЪС РММШДСЦЫФССИ КЧ ХОШЫХ. ГОПЯЙ УСК ЬЧЬЬДОЗ ХОЬЙМД УЭАСУАЧГ МБАШЗЙГИЦГ, ЭЩЛЪМЧЕЫ Ф ЬЧФОЭЖЧУЫ. ЦНЧ ЮЕ ФЗОЬ СОЙОФО ЫЛСПТМ, НЧГ ОЮКЩСВЧЪФВЯ Ц ЕЧЭУ-ЩГКДДИ ГР ГООЫЩЩЦСД. ЭЩЛЪМЧЕЫ Ф ЬЧФОЭЖЧУЫ ЪНШБАОЖИЬИЭЧ ЦС КЪИНЩЦФГ, ЫЯ ЕЭНЕ ТРМЖСВЬ ЯТСГЬ ФЖС АРФЮЧГООЖИГЬ РАЫЦЙ ЧЩНЦЙ УЫПЩТЪТЦМХ, Ф КЧЬУГЫФЩ ЗМ НЧ У ГЪЯ ЦЯВЗА ЪСПЪЮС, С ИЩЙМХА Ф ИЙ ВЮЬНЬЫ. ВЭЪ ЛСТМЮЙ ОТМ НИЮУЧЫЪН ВШАЪГЕ ВАФММ ЮЫКЯРЪЗ; ЛСРФЖЙ ВЕНА УСШЯ Г ЦЯЧСЭЙЬА О КЧЬЕ. ЦЫПХЫХ НЙКИЧ ВЙ ВОНЙЗ ЭЕДЙУ, У КЪНЧБОШ ИЙЖОРГФССИ ЙНЮА ЬОКСШЦЫ С ААЬЫ ЧЮУГ. ЬЧФОЭЖЧУЫ ЪМЧТЕЩИЧ ТЫЧГ КЦРСБФЩВЗ Г ЙЫКЯЛЙГНЗ: ЯФР ТЪЮЧ ИТЪЬД ЮЕ ФВЦЯСФНЕ ВАЫЙМЯВ, ЪИС ВКФЯЙЬИ ФР, ЛЦШМЖС ЮА ЫЫФЫИ Ф ИОВЛФ ИЙ АЛСТЙЖ, ОЭЙКЦНЩЙ УЯГРЫ КМЛМ ЮЩРЗИ. НЧФДМ ЙЦЩ, ЗММЬИИО УЙБООЫЩМ ПЪ ЕЧЬЕЩГ, КЦСЭНЩСШЩЙ ЩСЗНЛДШГФЭЙЬИ ЭЭЧЩМФ ИЧФАШГ ФДЖФ. ЕЙЫ ТЪЖЕЫО УЫЛШДЗЭЙЬИ О МЫЯРЪИО ЖУЮЙЩ, ГОЮТЙВ СОЙЩЯЧМЖС В БЪЖЕЙОХ ЯЧБОПГ С, АРФЬФШЗФЭБЩСИ Е ЮСТС, ЭДВТЬЙОЮНЪД ШЯОЫЛИГНСА НБУПГЮ, ВТМИЧУИЧГЪН ПСЛОХ ОЦИЙЭИ О ЛИХ И ОЙ ЛЦСИ ЛЧГ НМТСЮАЧГ ШЦТИ ЕЙЮТ. БЙРРИЩ РЙГЫ, ЦЫУЯЙ-ЩГКДДИ МЫСРЗД УЯЗМЕ-ШЯССЖИЮИЩ, ЯЧЬГЪ ГЮ ВЛЯУЙЬ, ПЪЯШЦРДГЪН ОНАСЭИ ЬОУСМФ, КЧГОШ ЛДХАЧ КЩЦГЪЛЕЫО

Ф ЮЧУОЬГФ, ЯБЬЫВСЯЭЧ У ВВЪАТ ЧЕЩА: "ПЩНЦЙ! ЫЯ, ЧЮЙ ШЯЮЮ УУЯЛЛЛД, ХОЧБЦЯ БЗНЕ ЯЧСИЕ БАУОХЮОС; ЭДЮЕЭГ СЭ СМЖЙ Щ ЧЮЙ-ЦЩБЯЯЕ ГАЦЙМЯ, ЧЮЙ Ь ЮАЭ АЪГЬ!" Ф СОЬАЛ ЗСВКМ ЭЙБЕЩГУЯВ ОЫФЩЛММЕ У МСУЧЫ. ПЪЛИХОГИДЪ КЯМ ЪСЛМ, ИОВКЪЖЕЫО ЫЫФРНФС, Й ЩНЪЮНС И ЭЭИШАЩИЙР КЯЛСЗА ЫЙХЦЩМЖСВЬ ОЗОВТС. КЧХКЬАШЩВДГЪН ТМЕСЭ ЗМКЙВОШ ЮЩСМШЫЫЩКФ, ЛСГОЬЦ, ЭЩЛЪМЧЕЫ Ф ЬЧФОЭЖЧУЫ ЪКИГЬ ЫЛЧХОЧБЙЬИ ЫОЫН. ЧСЗ НСЛСА, ЧХНМЕЧ ЧЕ, ДЖС ЯНФ, НОЭ БЪЖОЦ УШАЦНШМЖЙВЬ ЮЙФАА ФР. ЛВЕ ЫЙАГИ ЬЫРТРЪЯСЬИЭЧ ШЯ ДЪЗЙЭ, И ЪМЫСВМЖСВЬ ЮА, УЯТЪЛДЦ ИШАФЩ РЪЯСГЕЧЧЪЫИС ЮЦЦЗРЫ НСЛСА НБУПГЮ.

Вариант 11

ЖШЮТЮЙЭ ЯРКДШ ИЙ ЦЮДЧРА ЧГЬУЦЭГЛТВП ЦТ ЗОГВУ, ОЫНЧВЛШ ТЪ ИО ЮЮЦ ФНВМЭПЧЙЯЧ ЦАЗПВ. ЬЫЦГЪЫН СЙХ УЛЮ СХВОЯМЭТТ ИОУЮЮАЕЙО ГВГТТИСЧ, ЪУОХА ЧУЛЭСЫЭОЯЭБ ХЯЛЧЪЫЫХЙ Э ЪДРГМЪО Л ЮРЮТЭЙЪГШЫ. ТЪ ЬДЭ ЯБОЭЦЫ ГЮЮТЩЙЗ. ЮРЮЙЬЧУЪЩ, БХЯЛДЫ Ш ХЯЮЙУЪЩ ЗФЫИЫАЭ Д ТЧЙБЬЮЯ, УЫРЧШШЯ СН КЧЦЭТЦИД УФХГЩА ЮФТЧ, ФЯШ ЭОГМ ЫЛЩЫФЧТУС РЙФЕСОРХ Г ПЧЫЕЯЩГ ЯФХЕДЩГ С ЬАУХЪЦХЪ ЯБПАЗОГПЙДЩГ. ЧЯ СОП АНЛЧАЩИТИ ЦТ ФЖЕЫЭДЗ БЕТШЬСЬРИ, ИЫ КЧЭЮХМЪЦ УВГЦПИР С ГЭЫЛА УОГВЫЗЭЫЦЯЛИ, Х ПЦАЕААТЛ ЙКДЮКОЫЩ ЛФХГЩА. КЧЦ НЕМЩ ПЩАЭЕТЪЙХ ЯРИТСГФАБП СТЬЧЭМЛТТ ЕЩНЫШЫЧЙ ЪА БЭДЩАТЬРЯМ ЬЙ ЧУХЫР ЮНЧВЮАДЩ. М КАЪБЖ СЙХТ СОПХ ИЙФХДЯ ЪЫ ЫТЪЫЩ УА ЪДЮЮЕХЕЙЗ, ШАИТ ЭСДЛИ. ЖИМЧЬРТ ЗЭОБТ Б ВМЭЫХЪФУПЙИЧР ТШФВОБЬЮС М ЯЛОБХМЧЖГХЪ ЫЫХЯЧИЮШ ЪЙШАЦЧЫУ УТЛОЦ ФБРЫЗ. ЦЧБЭТШЧУА РЯЕНЛЧФ Т ЧЖН ЛИЦР ДЦЫЪФЪ БГЙСГ НФЮГД, ЫЬЩТЧЖГ ЭЙН КШГТЧЙТ ЕЫЫЪИ, ЭОЦИШН Ч ЯЧЮГ. ЪД НЗКТАУРХ, Е ЪТЬОР ПЙЩАВУР, ЮНЧСЫЫ ЦЭАЬХЮЮАЪГУТЬЫ ИПЫ ШАУГЙОЫ, ЧЦША СНКЩАВЫЖ СЛЬХЮЦТ, ЧЛДДЛШ ЦНЕПЧ ББПЫЗЧР. ВГЙАЮЧЭМАДМ МЫЧЭУ ОНБНАУБ МФ ИСЗ СОПН МЦТСЩЙЪЫ ЦЪЧШСЙЕЧР ФХЙЭЧЗ Ъ АУЛЩЫФЧТУСН ЛЙЩЭОРХ ГРАСГДУАЦЪПЯМ. ЪЫ ЧЦЭБН ХВ ЦЪЕ АДЭГЪАТУС ОЦФ ГШЧГЖГТ ЯР ФТДЕО ЬЮЪДЧ, ЯОВЦУЖЕГТ ЯРЧ ЗЫЖЧФЮС ОЭОПЬГ Д СНЯШЪБПВ: "ПМО ФЛВАЛ". ИЙ ЦАЖЗЫД ЭЭПЩОН, МЬЭХЫ М ЬЙ ЪДЮГТЪЫХ, ЦЫТ ОЭЫЪАВО, ПЫУЙЦМ, ДЦЫЪЛКРТ ЖПАЩЗ ЭБЗНЗС, ДАЖЕЧЫ, КЕСАЯ Х ИЙЦЯЫХЙ: "ЭСЯЮ - ЭТФЫЯЬРТ УЫНОЗР". ЫЛ ДАЩЦРЭД ЫЯЦАУБ МФ МЙВРШЖ ПЦМЭПЧЯПЫФ ГЪХТФЧ ЧХАБРЪЙО ГЫЖЩЫЭЧЧ ЮЭСЫ ЬЙВРФДЪ Г ХЧФАЯТ НЩЕСО. Ч ПЙЩАВ ДЦЫЪФЪ ФХЙ ЬОБЬШ. ХХТ КЧЬРЪЯПЫФА, ЗЕТ ВЙРСША ИЫЗЙ ЭОФМШ КЧФХДЙШГЫОБТ М СЭЧВ ЗУХЯЙ ЧХЫУЬНЖС БШГЬТМЫФХАСИА УЭШЭМ. ФЫ ЛААБЦНЗС ЯРИТСГФЪБП ИПА ЛЧВГГЪЦО ЮХЮАЪГЯН. ЯБЛНЯС ЦЮЯД ЕЖС ГРЧЯ; Х МУФЮЬА ПАЩЗГЛОХ ЯОВХХ ЖХЯЦН СОПХ ЙНЯШ ЕТШЧУА ВШРЪЦО КЫТУЧГ ЫВГФ ХЧЛДФРХЬХРЪС Т ЪЙШАЦАЩ ЦЧЖА ЮТВ. ХХТ МОЭХАМТ КЧЮХМДШЙЪО ЭУ ЬХЛЧЬЮЯ М ЭЙЛЯЮЯ ЧЮНЬБХ ЦТЭЦ. Ъ ГХХЙЭИЧЫ БЕТЭЙЦН ТДЙ ФЫЪЭЮАГШЫ УВГЕДМ ЮЧВР Ы УЫЯЧКТББ ЮЭЧЧО БОНИАЪТУПНМЕ Е БУРЫЮЧ ЦТБФН. КЩЪ ТЪЗШЪНЧ ЭУ СТА ЪЯШЪЧ ЫИЙ ЬРЪДШЫЪО ХМЙ ЧЛЬЙХ, Ы СН ЭДГЮЭТЦ ЭОВЕЖЬЧА ОЧ ВБФДЫФЪ ЪБЙ-РЯО ЯХВФНЭСЭМАЯТ МЫЧСЮМ ЯЙВЧУБ ЕАЛЕСЭУ М ДАЩЯХЮМ ЪЫ ЪФХЕПЫЗ ЦЧСШ.

Вариант 12

Щ ЙУЧЙЧЙЗТОУ ЬСГКЩ ТС ЯБЩЦЫЪЕ ЖХЯГЛЬПГ ЦБВЕПД ЙЧЖЦХД ЪШУЧМДКБН ЮИКЖ ЯЬННЪ Г НЩУЩЮД ЖНГАИНЕЭЪ Ю ШЕГЪНЙУУНС ЩУБАОДНИЬЬМ. ЕЮХЗЯОВЬДЬ ЙЧАЙИА Щ ЖМЧТЗЕГИПЩЧ ЖЕПЩ ЪАКЧ ААА ЗШЫЕ Н ЩЗЦВВДТМЮД ЯЪ БААЯЧЦЭШИПЯЮП ЖУАЧУЬТЩР ЛЯЧЯЮТЧСЩ Ъ Н ЖХЩЭДОТЯР НЕРЩЦЙЕЦГОЪ ЯМЛСНДДПД ДГ, ЬГА ЮТЗЦГЖЯ ТСЦ ИЧИСЩДДЕЭЪ АЬРСРОИД ХЭЫ ЙУФА, УЙУТН ИЕЛЮА ЭТРЯ БКИХЦЦНЙЗЯЮ ДМ ШШЯЬЙБ, ИДК ДЕЖААЯЧВС Ю ИЕЭНС ГЕФТГЯТСЗ. ЯКЗЦВЙЧТГЬД, ШРЦЦЙТК ЭЪНИА Щ ВКЮУУНБ ИРСФЫДПЩ, ЪАКЧ УЧЗЯЬСФК ЖУШТАЯ ЦУАДМ РЦХБДБЫЪС, ЩКБДЗЦЗМЗ АЬЗИАЙЕП, АВДБЕШНЮЧД ЩЮ ЛЕЙЮЬИЧЧН ЯБИПЯЭШБУ УНФЬ ФЬЧУЕ Н ХЧМЭЕГОНЦ ФБСИЬК; ЫАМЕЬЦ ГЖЧМСДШ, Щ ВГА ЮЗКЭС ЙЬЗВЬДА ФБАНЖКЫД - ЛЬЙСХКЪНИЧНБНЪ ЯБЩЦЫЪЕ ЖХЯГЛЬПГ. ЯК ОКЭ УЗЯЛЦ Ь АЩШЭ ЙЬИЕЭ, ДБГ ШЭЧЙУЭСЧОИД ИЪНВУ ФЕЮЬХЮЧМЕЗ, АЧАЧИЯХКЩ Н ХЧОЬО: ЯЯД ДЕЫАЙЬЫ УНОЬЦЮСЪЙЦР ЯБЭТМЮД ЯЪ БААЯЧЦЭЫГН, ЩЦПРНЭЪ ЛЕЙ БЕЖК Ц ВФКЯСЩ ББИЧБНИЯ, ХСЩЙЕЫУЧОДАЭЪ, НВЕТАЙЬХУЯЧГН АААЗШФТИЯ. ССЭК-ЖУЭТЗК ФБЪНЕКХЪЙЦГГГЫ Б НЖ АЭРКВДЮК ЗВЧ, КБУЮЙДЩЭЩЧ АЕЗЯЭШДУ УТВДАЦ ЦКГЕЙЯДЬ МСЯЫЙНР, ЬЬБ-ЧЯ: БКЪУУАМЯЗЙЪЬ И ЦУАДГ ЙЯЬОЕХЯЮ К ЖУФААЬ Н Я ЯБШУЬОФЕС АВЧРНЫЧ, ЮИПЯЙДЩЭЦЮ ЙЧ ТЯГП, КМЮТЮПНЦ А ГЫУБАЮУК ЬАФЧЙЦЫ Д ЫКГЧЕ ИЗЯЪС, ЩФБАУЬС АЖЧММФЬХЮЩЗ ЭЕРНКДЬ ЙСВКЩЕЮЪЫ, ЖХЯЙДЙЕУКДЬ ЕЕЪФК Н УТВДШП ГОЧЧНР Ю ЪЕШЧОЧЪ Я БМЯКШШЬХЮЩЗ Д ЕЧЛЧГЭЕПЛДМ, ТСЬКДКЗ ФЧЖНУКДМ ЬСКЖК ПЯЖДХ Н ИТЪ; Б ТЩЮ

ЛЗНВАБЫНЮСЪЙЦР Ъ ОЬ, ПЯДКЗАЖ ЩЬЩНХЯЬЦ ЦДЦШШЕ ЮТАЬРЩЭЬ ШРСХКИРЯФБДТМЮ ГЩЕЮЪБГ ЬЩЯКЩТЩЬКЩ ФЯ АНЕЖЦЯЙТС ААМКЬЦЯДЦС. Ы ЯДГ ФБЪНЕКХЪЙЦГГГЫ Я ЧЦ, ЬКЙУБНБ ИРДШЬЙ З ЩЯКИЧБТЙДУЪ ЬКВРЦХДЯ Н ЯДЗЯЬСРОИД ТЭЬЪУБААИЧУАИ ИЗЯЪС ЮЕЮСОЯО Щ БМЯЗМЙББ. ЖЯШБ, БЕЫЪБ ЬЦГО ЛЗКЫВЬИТМЧ АЕРЧЯКИЧЩ Ъ НВШЧУЧ! БЕЫ АЙЯ ЗЯЩЮТЭСРО Я ШВЭЬЭЙСРО ЫШЙЕ! ЙЕ, ШУН! Ы ДК ВЭПЭШ Щ ЭДПКЮ ЕАЕЗЯЭШИЧУЪЫ ЩНХЧОУ ЧЯЯЖЕК ЯУМЧЮЦЯДЬ Ц ВАЭЕГ ЮТУЧРНЯДБУУ. ФНЬ, ЬГА ЮТ ТЩ ФНЙХЦДДЙК ЮТ ЙЬЗВЬКГ ФБАНЖКЫДБ, ЩЦЦ ЪНЖУЬЯБДУ АВДВНИЪЫ: ГШЧЙДДА У ЦЗЯТЮНС ИГБДПБЕЖ, Г ГЧРЯШБДТМЮД Щ ПСВИЧТМ ВПБЕЭЪ, ИЧСМ Ф МЕМЯФЧМ, ЖЦЭЧМ Н ТЭБЫТЯ-ХКВШТНС ЧЧЬТНДАЖ ВБЫНЮХКЙЕЖ Ъ ФВДАЬЬМ.

Вариант 13

ЧЩ ЭГТБОР ЫШУАХУ ЪО ЮЕКСУЯ, ЧНШ ЭОЭЫЭ ЛЖЩ ВЫЛЭВЦЭ ЬГЪЩСБП, ИП ЧУЛНАЬ ХЬШ-ДНШ ЫОДЮЕКТОЕЙ Й ЬЩЪ БОФПЬАХТ, Е ФЩАБЭЙЦЮ ЭГХИКПЩШУЫХ ЪЦГЫЮШН. УДЯЧ ШЯЦЙТЛЕ, ЬЬДЯЫМЦНСЖГП Н ЭШЯАЪМБГРА ФЛШБЦ-НШ ЬЮШСИТФ ШЮНМЫ ЩПМТМЬНО. АН ЭПВУГТ, ИК ЩПШСА Э ЬАУЯМФЩСБ ЮЙМРААХЕК УЩЫ А ЯПФЯЕПГЬРЩПЪЙНЩ ЯЕННЫХЬЦЫ, ЕШЭЬГИД МЖЯЮАБТЦ ЛЕЫН БУЫ ДЫЛШХОЮТНЧУЪЫ ЯЛЭПОЯХ, ЭЕ НЯШРЯК ШОЬСАЬР ЬЧЪЙНЩ ЦЪ ЪГЯ. ШУДЧЙХЗШБ ОЖППЫОВ, МШНУГЕАЧШЬ ФТМАНУЕЪЦЯ, ХОЭ ЬАЬРЮФАЛН, ПЬКТЛПФ, ЦЪ ЧЙЬЩЮОВ ГЧЖУ ВТЛПТЮШШГ, БЛЧАИД ЫЭЬЮХЕ, ЮЩЮЕТКТЛЫБ, СЙЦЛЖАХА ЬЛЫЙИ - ЭЫР ЛЕЫ ЬЕНОШЯ ИПЫОЪСАХЗЫБ Ю ММРАЮИЗ ЗЪЬЮТНШЧ, ШБЯЙЪЖЧ ФШАГРА ВЭГ ХЛЪВТ, ЗПСТЖ ОЖКОЬАЭЫМШЬЬ ОЖШШТЫЪЕШФ Ц КТЛЧЖЪ ЗЭЫФЩЪ ФЭЫЬБО ЫШГ ОЩЪУЕИПОЬ ЪЪЫФЩЪБРЙ. ЗЭЦИ ВЖКПЫБЧЛШНЫОВ ЯПНЦЙ ДЛПТРОДЫУШЬ ЕЭООШЬ ГНМВРРШШГЬЗ Ц ЪНМЬЛРЫЯЧ ЫЧУТЯЧЫК; ТЮМ ШЬЩСБ ЪОРШЬ ФЫЖЖГЬШ ХМФЮЯДЯЭШ УЩЫ, ШОБГУ ДЧЫСЛАП, ЮЙМЬУЯ ЪА ТЧУЕЙ ИТХОЭЫЮШ УЯЭАМЫЭРУ. ЪОРШЬ ЦЫЭШЫЦЕЙ НКХ, ЕЕЫЬЕ ШУ ФИЖШ ШЦ ДШГВХЬЯ АЗЧЩ, ЫЫ ЮЖТГШБЩ МЦРЖАЫ, ТЬЩПО ПЙ МЬУЯ ОЦХЛ АУ ЩАХЩЕП, ЧЙЬЩЮЖЛ ЖИМНЕ УАЧДЦАИ. Э ЗЭЬЯ ЪЫОЩПАЫ ЙЬПОЕЙ МЩЫОХТЯХУРБЮНЖ ЩХАНТПШЫОЩ ЮШЬЭБСЫЦ. ЩЫЫ ХЗПЙА БЮЙЛРЫАИД ОЛЮ ЪНМЬЛРЮМНЖ ЬЪШМНЖЬН Ы ЮЖЭГОЕЙ ШЬУГ ФТМАНУЕЪЦЯ ХЮУЮЫМУД. ХЫМФЦЦЙНИТК, ХУСОВЛУЯИА ЫЧУИЫЗ: "КА, ЭШЭАЫЭОАЙНП! ШУ ДЯЦОШЬ ЮХ ЭКЧ АУЧ МЦРЖЫЯЧ!" - ЛЖРУЛН ТЧ ЕУЮНШ ЦБКЕАИ ШОЦЭЫОЩМ. Х ПЦЫГУЯ ЧЖКЬЯШ ЫИТ ЪЬВНЯКЙАДМ ЙБРЫП ЭАОХЬ ЫШГ, ХЮЕЛТ МФЛХУЯЧ, ЧУШБРЯК. ЩАЕАЯК ЩЫЫ ЮЙМРЮЛТИЧЩ РОЯАЫШУАИ НПЧ, ЕЕЫ ИКТЙХНЩЬ Н ЛЕЫЗ ШМЗШЮНМР ОГХМЬЩШГННКЧЦ; ХЬЛШВУЯ, ЫИТ ЬЕЫЯЫИЭЯТ АТПШЙЯХ Г МЩЯВХНКШЫОЩГ ХЙТПЩГ. ШШЦ ЮЛЬЙЭ ЭБЯЙХХЬХННЖ ЩП ЮХНПЫОЕАЛП; АРУШЪЬ МБЮРЫЪУЫУ, ЬОВХЦАН Г НЫУКН Г НЩРБЭЪЬ Ь ЭГТВЪРЫЫТЗ Т ЩЯЕЭЙЧЫОЩГ ФЩЦЭЫМЬКЪЫ ЫЬ К. Л. ЬГШЙМР.

Вариант 14:

Й ЯБЭТТКО АЛ ТЗХШЛУТМ ЩЮЪУККШЬЫШЖ ЧТВУШПЛЙ ЭШЧФОХМЭФ ЩОФЮГФБЕ Ы ИЫСХЕЪЮЯ. ЮТЛХХГ ЗЕЛ ЫЮХЛЪШПЭАБУ НПЬШЬ М ПШЫАФЦ СЦЛДСП ВЫХЦФ ЗТШУБ ЧХОМР. ШЯП С ОТУКААЬШЮЛЬНПУБ ИШЗЪРДШК, С ЬЮЦФ ЫЧКБЕСТВШУБ ИЪЕЦХАО, М КШВБЦШЕ ЪГДЧФИУ ЦЫИПТ ЧР ЗЩ-ЮУ, ЭЦШ ЮТЛХХГ ЦКЗЦХГОХ ВЫО ДИШЮ РШЪУЖ И ЧШЭЖФОНЮ, АО М ККЪБТ ЫЛЭЗУЛ, ЧЕ ОХЮЖХ ИЫЪЮДБЕЧШТ. ФЧ ПШЫБМТЛ МБЕЖМАЬМ Х ЧПМЖ ЗУЧШВ, ШСШККТЖ Т ЧИК, БЕВП ШШЧЧЛЯ ИШ ВЫХЯ О ЛЫЬМ ВВЙНЕЬ ЭЖРДШХ ХФЫКЪХДЛЧЬП. ЮА ХШЛШЦЫС ЫЕЛХ Х ШПЧПЭЫЛ ОЕЫПЕО ХЕЬ ББЧЬАМШЕВ ФАЩШЕЖХ ИС ЯТШТДПБТШТ ТЕБТЭ, Т УРХ РШШ БЕЫБ ШКК МХГУШ И ЧХБШЪАСШЯФ, ФАФ БЖКЖБК, ЯБШШМЭ ЗЕФ ЫКШАШЛ БИЧЮХУТК ЩЮЬЖЛУОХЕ НКГХПАЩЬЬ М ИХЛУЦКАДРЭЮ ЫТБЛНО ЧРКЖХЬЧШЭЖ, ЧЕРХЮО ЧЕЦХЙ ЦПШТВДЕ ЩЕЪХЯЛЧИЬМ ДИШЕ ЫЫБИШ. НТ Т ЭЖФОЦ БЮЩБАП ЭШ ЩМЕХШКОМАХ ЮА ЧМОТЕ ЫНОЕЪЦШР, Т ЕЫЫЫ ЬПНК ЭУ РКРЬЮЗЛХЬ ЫЫЫЮФОЦ ЯБКЧИЦРЮЖЫЬ ЩАБШТВ ШСОРЧОМХАУШГШ, ЮА УП ПЪШФЖМЛЙЫ АО ШДЧЮЬ РШППЩЭО, ЧО ЭЬШУЖШКЫ ЕФХЬФЮ ЭФХИБХДШМО, Т ЕБШЙ ОЫВУИКЛЫП ЫУШГОР АЛЫКШЫПРШ ГШЫБКЧЫЦ, ЭБ, ФОНКЪБ МП, ПЪШХБФАХ Ъ РШШМЭ. РЭРЭРКВАФЫТЖ ХЦФ ЩРШБЕОЪАХРДВ ОО ЬЮЦФ, БТШ ЮА ХШЛШЦЫС АЕХЮХЖЬЬ РХАЩ ЫВШО Х ЧЭТФШ АЛ ЛОХХШ КМУЯ АУН, К ЧЬЮФБ ФАФ-ЫЗЭДЖ ЭШ ХШЦПЫБИКТЖ ЫЫЮЧИУ АУН, ШН ЧШЭФНДК ЭШ РХАХ ЯШЦАУ ЛЮЮЛП ООЭБП ХОРХКРТ В ЫТБП ЫУЩ; ТВЦШЧПЬ, Х ИШСФАШЧЧЫУ ФШУЖ ЭЬЮ ВЦКВТЫБ УП ТКЪ ДШЪОНЮ ЫЧЩОХЭТСШСЖ, ЯБШШМЭ ЗЕФ ВИХЫШЦ МЫЩШХЖХ ТШУЧЖ ОВП СЖШЕЛФШ ВОМА Т ЮЧУЭ БЭВОСФУ ЬЬЫУЧОУ ТБКФИ, ФЮЕФЪУИ, ЮЧУККШ ЦШ, ФЧ ВЫХЦКК БЪРАОХ. ПТЫ БУ МОМБШ УП ТКЪ, ЭЖФ АЧУЮОБАЧША, РШТШАОП ЬОЬЗУЧ ЩОЫЫШ ФЛЕОР ЪЖЩИЪРШШ ОВПАП УК КЪОКФФ И ЧРГЛСЫМРШШЫЯ ШФЫУ. ЧАЩАБШТВ, ШЭ, ЭЖФ НПЬШЬ, ЩИХ ТДЛНДК ТЧФЯНШТШУЧО, ТЫЫ Ч ЫАЩЮЩУТКШЬ ЦФЮМКЭБТ, ТЛТ Б ДШШЛЙАБТ ФУЧЖБТ, ЬОРХ АЛЦЦПЬ Ы ЗШЛЖИЫТ ЩЬЙЭЫЬПЮ. ЬРЭФМ БЕЫ ИЖЪАФВШЦ ЛЛКУБЦШДЧЮЦФ ВИХЫШЦК, КШВБЦЕЙ ЧРЭФЧЕА СОС ЩРТТШКПН М ЗГЛСВЕЗУПЧО СРЕЦЭДЧШЕЛХЬЧЮШ

ХШЛШЦШУТЕ. ЯЮЕЕ ШН ЛЛЮ ЪХЕНЬУШТК Т ЭШТПЦ, ШФАЖФО Р ЯБЧЬУЩЪЫ ХТРШУБИК ВШЧФЩОИХШ Х УПМ БВБ-ШШ ПШЕБМПЕ ЧР ГЛМНШБЕВ.

Вариант 15:

Ш ДЪМСЙЩЕ ЗМЕДЦУЙ ГЯЬМ, ЗЖЯЕЧ ЙЮ НТ СОЩЯЩЧРЧСЦЙЪ Н ЫМШФЖВД, ЪЧОЮГУ ЦНХЕПЙ ЯЖЖСНЪЭЦТУЖ, НС ЮЬДПМТИ ИЩ ТЛ СОПЙ Щ ТУСОШО ЮК ЮТЫНЫГБЬЖ. ВРЛДИ ЩФ СЮЫЬ ПЛС ВЦЙАЕШФЫХ О ХЗРЧЕХ ЙХТЩКО РЙЭЕ; Н КЛМВСЪ РКО ЫЛЯНТХШЧЙ РЗЦМНФА ЮКУОЪЛМЮНЧХЕ: ЫАБКП ЦОРХЦМПХМ ЪМГЕШХВФЖСЦЗ САЬАГЕ; ПЙЕЬСМ УЭЙОЬГЬНЬГ; ВЗКБАОФУЧ, МЯИШЪВДГВБ, ОХСЫЙХНШ Й МЯИХНЫМ И ЫЙТКСЗЛ ОЭЦХА ЦО ЧАВЧШПЦС. ЕСПЩЙ ЖС ЬМР ЮНАЭ Г УСРШТС ГШШЧТЕЩГЦ ПЩЙАЧАУЕ, ХХГРЫ ЯТ ЮОНМЖ, ИЧЩ ДТЪ ЬМР ЬХБЭНУКШФЫХ АФУ ШХС! ЫЛЩ ВЭХМ ЩАЯЖЖСНЪЭЦТШХМ УЛЦРУАЕ, ЦЫШЕЦХСИ АЭШ, НШЕ ЫАБКНХРЪНЩРЩШЬ Я ИЦИЩ Й ГЧЫШЕА; ХН ГОУЦЭЙООЫЬ, ЬЭХ ЕРЭС СЩК СЮЙРЧЗ; ФО ЬАЙНЦШЯ ОЙ ИЧЩ ИЫ ЮЙ ЮН ЬЩАЧЙ ЯЛУЛАЮЧ ЦИЩ ЙОУЭБЕДМНФЪ У ПЛЧЕЮО, УКЬГ ДЬЙЧЕ, ХЗК О ЖЩЪЩЧАРЕЦ. ЬЫМЗ РЭЦ СУФУЮЦ ЮУЬ ЛЕХМГЗУЩЕЧЧЮУ НВШСЖ. ЯТ МВЛ О ЗДТППРС, УЩЧЩУ ЗЪЖЯЧЩУ, С НЙЬБГПМ ЭНЯДВПМ ОЙБУЭФИЦЙЭ; ТЛ ФЕШ ЬМРУ ОАШУЦЗЖМ ПМИГЕЦХНЗ; КБН МХКЯ УАЕОЗ. ПЪ УЬДЪМ С ЫЖПСЛНЕШ ЗЯЛШХ БЗЖЯ МЛСЛКТЩЧЗ, ЮТЪ ЙЮ ЦВПТМАГЦК Й РМИФК ЬЩАЮМЫУОХ СЪЭЦЧШПКМ. КЯ ЗЬММЯ ВССРЩНЪ ЬМРЩ, ЮТЪ ЙЮ КАЗЛ ЦОХЕ-ШПБЯЯН Ц НПЗФНЯС. ЩФ ПЪЮЬДПМЛ ЩЫ ЯЖР ШТЪЛЯТЖ, ОАЦЛЩЬЛТ КЯТЦХЮ: "ЦОРЫУЕФ!" - ШЕЧ Г ДКАЗЛ. НАХТЖР КЪЭСРРЙ ЧЯНН ТР ШОДАЬ Ц ЮУА. ЪИ ЮК ТФАЧ, ЕСП У ЦОРОЭЕЭГ О ЮЫЫУЧ ШТЬЫЮТЩУ ПЬЙЩЦГМСЮЭЩН. ХЗК ТА ЭУСФО, О МССЩУ ДСЖЦ, ЬЭХБЗ ИЯЦ, ХХТЪЛМО РАЕ ОТЦХЛ ИЫЧ О ЮКОХ НМ ЖЩЫР, ФЕ ШЙФ КТЛИЮЧ Щ ЪЩЛИЮЧ, - ТАЦ Й МЯИХНЫМ! ОЩ КЯЖРНАЧ ВС ПЛЧЕЮЙП, ПЩЩОЬЫР, П ЬЮАЭНЩГ, ЪЧОСРСРЛ ФЕРЫЬКХХ И ЪМГЕШХВФЖСЦЗ ЦЕЬАХ ПЛОАЩМЫНЧ ШОНЙБУЧ.

3. СОДЕРЖАНИЕ ОТЧЁТА ПО ЛАБОРАТОРНОЙ РАБОТЕ

После выполнения лабораторной работы и расшифровки всего сообщения, необходимо подготовить отчёт, включающий в себя:

- титульный лист;
- задание к лабораторной работе (согласно вашему варианту);
- подробное описание разработанной Вами программы, включая краткое руководство пользователя (криптоаналитика) по её использованию;
- подробное и поэтапное описание процесса дешифрации, проделанной вами для взлома зашифрованного текста и получения секретного ключа;
- листинг составленной программы, реализующей алгоритмы (шрифт `Courier New`, 10 кегель);
- результат работы программы (копию экрана с работающей программой, расшифрованным сообщением и секретным ключом);
- заключение, содержащее выводы о полученных лично Вами результатах, в ходе выполнения лабораторной работы (приобретённые знания, навыки, умения и т.п.).

Отчёт должен быть подготовлен в текстовом редакторе, согласно действующему стандарту организации на оформление студенческих работ.