Кр💀птография

Разминка

> Расшифруйте **шпдж{лдхиофиыист}**
> Найдите сдвиг и расшифруйте **djye{clapwnrgml}**
> Зашифруйте фразу «не хочу быть программистом», используя ключ «кодинг»

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	.	,	?

Расшифруйте слово 15 24 14 26 34 14 13 34 33
ПНЕОИЗСЕДТИУППЕЛРЕЕ

Компьютерные способы шифрования

XOR (исключающее ИЛИ)

Это логическая операция, которая широко используется в криптографии для создания сложных шифровок. В отличие от обычного шифрования, при котором каждый символ шифруется по аналогии с сдвигом (например, с помощью ключа), XOR работает так:

- Если два бита одинаковы, результат будет **0**.

- Если два бита разные, результат будет **1**.

Основные особенности XOR:

- Это операция, где тот же самый ключ используется и для шифрования, и для дешифрования (симметричный)
- Применяется в симметричных шифрах и алгоритмах, таких как **RC4**, и в системах на базе **шифрования потока**

Пример (XOR-шифрование):

```
01101000 01100101 01101100 01101100 01101111 00100000 01101001 01101101 00100000
01110101 01110011 01101001 01101110 01100111 00100000 01101101 01100001 01111000
00100000 01101101 01100101 01110011 01110011 01100101 01101110 01100111 01100101
01110010
```

Ключ пусть будет **232**:
`11101000`

Применяя последовательно на каждом байте:

```
01101000
11101000
--------
10000000
```

Результат:

```
11000010 10000000 11000010 10001101 11000010 10000100 11000010 10000100 11000010
10000111 11000011 10001000 11000010 10000001 11000010 10000101 11000011 10001000
11000010 10011101 11000010 10011011 11000010 10000001 11000010 10000110 11000010
10001111 11000011 10001000 11000010 10000101 11000010 10001001 11000010 10010000
11000011 10001000 11000010 10000101 11000010 10001101 11000010 10011011 11000010
10011011 11000010 10001101 11000010 10000110 11000010 10001111 11000010 10001101
11000010 10011010
```

Как понять, что перед нами XOR?

- Обычно XOR используется для **шифрования одного символа** или **небольших блоков** данных. Если ты видишь, что текст выглядит как случайный набор символов, и ты знаешь, что это побитовая операция, скорее всего, это XOR

- Кроме того, если видно, что зашифрованное сообщение и ключ одинаковой длины -- это тоже может быть признаком XOR

Практика:

1. Побалуйтесь с XOR. Зашифруйте сообщение, передайте соседу, а он пусть попробует расшифровать. Сделайте выводы
2. Попробуйте сделать XOR несколько раз. И передайте другу на расшифровку. Посмотрим, что из этого выйдет ;)
3. На листке с места преступления злоумышленник оставил записку: "Способны ли вы найти меня? `cfd8caf7eebce0ffe4bcbfd3e2b8efe4bde2b8bff8fff5edd3ffd3e1b8e0bcebbcf1`". На экспертизе выявили, что невидимыми чернилами написано 3 буквы: "**XOR**". Сможешь ли ты разгадать загадку?

Перестановки (Transposition Ciphers)

Символы текста только изменяют свои позиции. В отличие от подстановки, в перестановке используется тот же самый набор символов, просто они перемещаются по тексту

Как понять, что это перестановка?

- Перестановка часто делает текст трудным для анализа по частоте букв. Однако, если заметно, что набор символов остался тот же, а структура текста изменена, скорее всего, это перестановка (если есть часть исходного текста)

> **12.** Старшеклассница Таня, увлекающаяся криптографией, решила рассказать своей подруге Ангелине о переживаниях насчёт собственного будущего. Но чтобы не загружать подругу своими проблемами и не расстраивать её, она решила сделать это в более интересной форме, а именно с помощью зашифрованного послания. Известно, что для этого Таня использовала таблицу, но сколько в ней было строк и столбцов, неизвестно (число столбцов > 1, число строк > 1). Девочка записала сообщение последовательно, начиная с левой верхней ячейки и заполняя каждую строку слева направо. Также известно, что длина зашифрованного послания при делении на число столбцов даёт остаток, равный 3 (то есть в последней строке Таниной таблицы записаны последние 3 символа её сообщения). Затем Таня выписала последовательно содержимое всех столбцов, начиная с левой верхней ячейки и выписывая каждый столбец сверху вниз.
>
> Зашифрованное послание: **ПНЕОИЗСЕДТИУППЕЛРЕЕ**.
>
> Помогите Ангелине расшифровать послание, чтобы понять, что беспокоит Таню. В ответ запишите без пробелов полученный текст, число строк таблицы, которую использовала Таня для зашифрования и число её столбцов.

В последней строке - 3 символа
Ищем: $19 \% X = 3$
Таких числа 2: 4 и 8

Пробуем 8 столбцов и 3 строки:
ПНЕОИЗСЕДТИУППЕЛРЕЕ

П
НЕОИЗСЕДТИУППЕЛРЕЕ

П
Н
ЕОИЗСЕДТИУППЕЛРЕЕ

ПОС
НИЕ
ЕЗДТИУППЕЛРЕЕ

ПОСТУПЕЛРЕЕ
НИЕИП
ЕЗД

ПОСТУПЛЕ
НИЕИПЕРЕ
ЕЗД

11. Для шифрования используется таблица, в которой самая верхняя строка содержит буквы русского алфавита, расположенные в случайном порядке, самый левый столбец содержит номера строк. Остальные ячейки таблицы содержат двузначные числа, причём в столбце могут повторяться числа, а в строке нет. При шифровании строки таблицы просматриваются последовательно, начиная со строки под номером 1.

	А	В	У	Д	Л	Р	Й	Г	Е	О	Т	И	М	С	…
1	13	78	65	31	23	98	45	37	56	15	55	81	11	10	…
2	57	56	37	45	74	82	90	81	76	49	52	92	15	16	…
3	31	82	57	24	68	98	49	42	97	12	63	64	17	18	…
4	44	12	36	11	49	18	10	99	53	57	61	98	21	22	…
5	63	71	12	33	31	27	49	81	16	77	51	83	19	20	…
6	17	15	57	41	82	97	31	16	49	44	21	92	23	24	…
7	11	37	49	16	31	61	18	97	36	15	82	19	25	26	…
…	…	…	…	…	…	…	…	…	…	…	…	…			…

Известно, что таблица позволяет зашифровать одно слово несколькими способами, но для каждого получившегося шифра выполняются следующие условия:

- В начале шифртекста идёт начальная группа цифр, длина которой не превышает длину шифруемого слова, причём среди цифр этой начальной группы не может встретиться 0.
- Затем идут двузначные числа (число двузначных чисел совпадает с длиной шифруемого слова, то есть каждая буква слова шифруется одним двузначным числом).

Также известно, что зашифровано слово из 7 букв, имеющее отношение к программному обеспечению, и полученный шифр выглядит так:

121111 31 82 57 49 12 16 97

Какое слово было зашифровано?

121111 - Последовательно суммируем?

1 -> 31 = Д

2 -> 82 = Р

2 -> 57 = А

3 -> 49 = Й

4 -> 12 = В

5 -> 16 = Е

6 -> 97 = Р

Бинарные сдвиги

Сдвиг влево (оператор `<<`) — это операция, при которой все биты числа сдвигаются на заданное количество позиций влево, а справа добавляются нули

Допустим, у нас есть число **7** (`00000111`)
После сдвига влево на 2, оно стало (`00011100`) = 28

Вправо такая же логика, но мы делим на 2, а не умножаем

ПОСЕДТИУППЕЛРЕЕ
НИ
ЕЗ

Практика:
Вы оказались в далеком будущем, людей не осталось. Теперь есть только роботы. И вот к вам подошел робот Тимофей и сказал:

```
11100100 110101100 11100000 101010000 11100000 101010100 11100100 110001100
11100000 101000100 1100100000 11100100 110111100 11100000 101110100 11100000
101001100 11100000 101011000 11100000 101101000 11100000 101110100 11100000
101001000 1100100000 11100000 101101000 1100100000 11100000 101011000 11100100
110111100 11100000 101001000 11100000 101100000 11100100 110110100 1100100000
11100100 110110000 11100000 101011000 11100100 110101000 11100000 101011000
```

Расшифруйте, что он хочет от вас

Алгоритмы криптоанализа

> ⓘ **Info**
>
> **Криптоанализ** — это искусство и наука расшифровки зашифрованных сообщений *без знания ключа*. Он включает в себя использование различных методов для выявления слабых мест в криптографических алгоритмах и попытки извлечь скрытую информацию

Грубо говоря, криптоанализ — это искусство взлома шифров, где задача — найти способ расшифровать текст, **не зная ключа**

Частотный анализ

Частотный анализ — это один из самых старых и наиболее популярных методов криптоанализа, применяемых к шифрам подстановки, таким как шифр Цезаря или шифр Виженера. Этот метод основывается на анализе частоты появления символов в

зашифрованном тексте:

$$\mathrm{Freq}_x = \frac{Q_x}{Q_{\mathrm{all}}},$$

где Freq_x — частотность слова x,
Q_x — количество употреблений слова x,
Q_{all} — количество употреблений всех слов.

Также необходимо найти закономерности в шифротексте и попытаться расшифровать его с помощью анализа структуры текста

Идея довольно простая:

- В любом языке буквы встречаются с разной частотой. Например, в русском языке *наиболее часто* встречаются буквы **о**, **и**, **е**, **а** и так далее
- Задача криптоанализа заключается в том, чтобы определить, какие символы в *шифротексте* соответствуют наиболее часто встречающимся буквам в языке

Вот статистика с Wiki для русского языка:

буква	ранг	употреблений	частотность	
а	3	40487008	8,01%	
б	21	8051767	1,59%	
в	9	22930719	4,54%	
г	19	8564640	1,70%	
д	13	15052118	2,98%	
е	2	42691213	8,45%	
ё	33	184928	0,04%	
ж	25	4746916	0,94%	
з	20	8329904	1,65%	
и	4	37153142	7,35%	
й	23	6106262	1,21%	
к	11	17653469	3,49%	
л	10	22230174	4,40%	

буква	ранг	употреблений	частотность	
м	12	16203060	3,21%	
н	5	33838881	6,70%	
о	1	55414481	10,97%	
п	14	14201572	2,81%	
р	8	23916825	4,73%	
с	7	27627040	5,47%	
т	6	31620970	6,26%	
у	15	13245712	2,62%	
ф	31	1335747	0,26%	
х	24	4904176	0,97%	
ц	28	2438807	0,48%	
ч	22	7300193	1,44%	
ш	26	3678738	0,73%	
щ	29	1822476	0,36%	
ъ	32	185452	0,04%	
ы	17	9595941	1,90%	
ь	18	8784613	1,74%	
э	30	1610107	0,32%	
ю	27	3220715	0,64%	
я	16	10139085		

Я собрал свою статистику, проанализировав статьи из вики на частотность. Sample вышел небольшим - всего 10к строк. Вот результаты (*справа - моя, слева - вики*):

о – 10.97%	о: 33393 (10.24%)
е – 8.52%	и: 27708 (8.50%)
а – 8.01%	а: 27325 (8.38%)
и – 7.34%	е: 24497 (7.51%)
н – 6.71%	с: 22969 (7.04%)
т – 6.28%	н: 21996 (6.74%)
с – 5.52%	р: 19947 (6.12%)
р – 5.32%	т: 17166 (5.26%)
в – 4.58%	в: 14965 (4.59%)
л – 4.02	л: 12410 (3.81%)
к – 3.49%	к: 12128 (3.72%)
м – 3.27%	д: 9465 (2.90%)
д – 3.03%	я: 8873 (2.72%)
п – 2.81%	м: 8579 (2.63%)
у – 2.62%	п: 7572 (2.32%)
я – 2.03%	у: 7297 (2.24%)
ы – 1.93%	г: 6562 (2.01%)
ь – 1.85%	ы: 6252 (1.92%)
г – 1.77%	з: 4962 (1.52%)
з – 1.62%	й: 4860 (1.49%)
ч – 1.47	б: 4458 (1.37%)
й – 1.22%	ь: 3937 (1.21%)
х – 0.99%	ч: 3586 (1.10%)
ж – 0.94%	х: 3482 (1.07%)
ш – 0.89%	ж: 2053 (0.63%)
ю – 0.55%	ц: 2038 (0.62%)
ц – 0.48%	ф: 1797 (0.55%)
э – 0.36%	ю: 1720 (0.53%)
ф – 0.23%	ш: 1420 (0.44%)
ё – 0.09%	щ: 1269 (0.39%)
	э: 712 (0.22%)
	ё: 585 (0.18%)
	ъ: 162 (0.05%)

Разница достигается из-за:

1. Размера семпла
2. Контекста

> **Important**
>
> Важно отметить, что текст, который мы пытаемся расшифровать криптоанализом, должен быть достаточно длинным, чтобы найти осмысленность в словах и определить замены

Если мы возьмем, к примеру, такой текст:

```
Мэие Кщьфеу — гшэв эь ёфбпй шещцвэй э эьцщёжвпй бщжгшгц мэиегцфвэу, вфьцфввпю ц лщёжр еэбёягчг дгаягцгшкф Таэу Кщьфеу, ягжгепю эёдгарьгцфа щчг шау ьфнэжп цгщввгю дщещдэёяэ. Сжгж мэие гжвгёэжёу я жэдз бгвгфаифцэжвпй дгшёжфвгцглвпй мэиегц э ефхгжфщж дг деэвкэдз ёшцэчф хзяц фаифцэжф вф иэяёэегцфввгщ лэёаг дгьэкэю. Вфдеэбще, деэ ёшцэчщ вф 3 хзяцф «A» дещцефнфщжёу ц «D», «B» — ц «E», э жфя шфащщ. Вщёбгжеу вф дегёжгжз, ц фвжэлвпщ цещбщвф сжгж бщжгш гхщёдщлэцфа шгёжфжглвзт ягвиэшщвкэфарвгёжр, жфя яфя хгармэвёжцг дегжэцвэягц вщ збщаэ лэжфжр шфыщ гжяепжпщ жщяёжп. Ёщчгшву мэие Кщьфеу вщ ёлэжфщжёу вфшщывпб эь-ьф ащчягёжэ щчг цьагбф (вфдеэбще, бщжгшгб лфёжгжвгчг фвфаэьф эаэ дщещхгеф цёщй цгьбгывпй ёшцэчгц), вг гв гёжфщжёу цфывпб злщхвпб эвёжезбщвжгб ц яеэджгчефиээ. Щчг деэбщвутж шау гхоуёвщвэу хфьгцпй деэвкэдгц мэиегцфвэу, ф жфяыщ ц чгагцгагбяфй, яцщёжфй э дегёжпй дегчефббфй шау ягшэегцфвэу ёггхнщвэю. Яегбщ жгчг, бгшэиэяфкээ мэиеф Кщьфеу ащчаэ ц гёвгцз хгащщ ёагывпй фачгеэжбгц, жфяэй яфя ROT13, ягжгепю эёдгарьзщжёу шау лфёжэлвгчг ёяепжэу жщяёжф ц эвжщевщжщ (вфдеэбще, ёдгюащегц эаэ гжцщжгц вф ьфшфвэу).
```

И попробуем провести частотный анализ, получим следующее:

Если попробуем анализировать классический **русский алфавит**:

Шаги для расшифровки простой подмены:

- Мы знаем, что в русском языке буква **о** встречается чаще всего
- Пытаемся найти буквы в шифрованном сообщении, которые наиболее часто повторяются (например, в нашем случае это будет **к** и **г**)
- Предполагаем, что эти символы могут быть заменой для **о** и **и** в оригинальном тексте
- Сдвигаем буквы шифрованного текста на нужное количество позиций, чтобы получить читаемый текст

Я сидел 2 часа, в итоге получилось что-то типо:

```
Мибр Кегаря — опис иг вадуз претсиз и игтевнсуз денопот жибротасия, сагтассуц т
йевнф ридвлоыо моклотопха Ткия Кегаря, лонoруц ивмокфготак еыо пкя гащину тоессоц
меремивли. Снон жибр онсовинвя л нимь досоакбатинсуз мопвнасотойсуз жиброт и
рачонаен мо мрисхимь вптиыа чьлт акбатина са билвиротассое йивко могихиц. Вамридер,
мри вптиые са 3 чьлта «А» мретращаенвя т «D», «В» — т «Е», и нал пакее. Вевдонря са
мровнонь, т аснийсуе тредеса энон деноп очевмейитак повнанойсьш лосбипесхиакфсовнф,
нал лал чокфжисвнто мронитсилот се ьдеки йинанф паюе онлруную нелвну. Ёеыопся жибр
```

```
Кегаря се вйинаенвя сапеюсуд иг-га кеыловни еыо тгкода (самридер, денопод
йавнонсоыо асакига ики меречора твез тогдоюсуз вптиыот), со ос овнаенвя таюсуд
ьйечсуд исвнрьдеснод т лримноырабии. Щыо мридесяшн пкя очёявсесия чаготуз мрисхимот
жибротасия, а налюе т ыокотокодлаз, лтевназ и мровнуз мроыраддаз пкя лопиротасия
воочщесиц. Яроде ноыо, допибилахии жибра Кегаря кеыки т овсоть чокее вкоюсуз
акыориндот, нализ лал , лоноруц ивмокфгьенвя пкя йавнийсоыо влруния нелвна т
иснерсене (самридер, вмоцкерот ики онтенот са гапасия).
```

> Магии не существует o_o. Я разочарован

Придется доработать ручками. Из совсем нечитаемого, мы получили +- что-то осмысленное. Если прям ~~совсем делать нечего~~ вдаться в анализ, можно заметить `Мибр Кегаря`. Предположим там зашифровано `Шифр Цезаря` - тогда меняем остальные буквы во всем тексте

М => Ш
Б => Ш
К => Ц
...

Можно найти слова:

- иЗ - з тоже валидна
- Юция цеЗаря ==> Юлия Цезаря? (Тк мы уверены в буквах и, я, а следующее слово - Цезаря) ==> **Ц = Л**
- буква Т встречается довольно часто, особенно в единичном экземпляре. *Буква-Предлог*?
- Шри вптиые ==> При ... ? Тогда **Ш = П**

```
ШиФр ЦеЗаря — опис иЗ вадуз претсиз и иЗтевнсуз денопот жиФротасия, саЗтассуЛ т
йевнф ридвлоыо ПоЛлотопха ЮЛия ЛеЗаря, лонорУЛ ивПоЛфЗотаЛ еыо пЛя Защину тоессоЛ
ПереПивли. Снон жиФр онсовинвя л ниПь досоаЛФатинсуз Попвнасотойсуз жиФрот и
рачонаен По ПрисхиПь вптиыа чьлт аЛФатина са Филвиротассое йивЛо ПоЗихиЛ. ВаПридер,
При вптиые са З чьлта «А» Претращаенвя т «D», «В» — т «Е», и нал паЛее. Вевдонря са
Провнонь, т аснийсуе тредеса энон деноп очевПейитаЛ повнанойсьП лосФипесхиаЛфсовнф,
нал лал чоЛфжисвнто Пронитсилот се ьдеЛи йинанф паюе онлруную нелвну. Ёеыопся жиФр
ЦеЗаря се вйинаенвя сапеюсуд иЗ-За Леыловни еыо тЗЛода (саПридер, денопод
йавнонсоыо асаЛиЗа иЛи Перечора твез тоЗдоюсуз вптиыот), со ос овнаенвя таюсуд
ьйечсуд исвнрьдеснод т лриПноыраФии. Щыо ПридесяПн пЛя очёявсесия чаЗотуз ПрисхиПот
жиФротасия, а налюе т ыоЛотоЛодлаз, лтевназ и Провнуз Проыраддаз пЛя лопиротасия
воочщесиЛ. Яроде ноыо, допиФилахии жиФра ЛеЗаря ЛеыЛи т овсоть чоЛее вЛоюсуз
```

```
аЛыориндот, нализ лал , лонорул ивПоЛфЗьенвя пЛя йавнийсоыо влруния нелвна т
иснерсене (саПридер, вПоЛЛерот иЛи онтенот са Запасия).
```

- лриПноыраФии ==> криптографии? Л = П, Н = Т, Ы = Г
- пЛя ==> для? П = Д

```
ШиФр ЦеЗаря — оДис иЗ вадуз ДреВсиз и иЗВевТсуз деТоДоВ жиФроВасия, саЗВассуЛ В
йевТф ридвлоГо ПоЛлоВоДха ЮЛия ЛеЗаря, лоТоруЛ ивПоЛфЗоВаЛ еГо ДЛя ЗащиТу ВоессоЛ
ПереПивли. СТоТ жиФр оТсовиТвя л ТиПь досоаЛФаВиТсуз ПоДвТасоВойсуз жиФроВ и
рачоТаеТ По ПрисхиПь вДВиГа чьлВ аЛФаВиТа са ФилвироВассое йивЛо ПоЗихиЛ. ВаПридер,
При вДВиГе са З чьлВа «А» ПреВращаеТвя В «D», «В» — В «Е», и Тал ДаЛее. ВевдоТря са
ПровТоТь, В асТийсуе Вредеса эТоТ деТоД очевПейиВаЛ ДовТаТойсьП лосФиДесхиаЛфсовТф,
Тал лал чоЛфжисвТВо ПроТиВсилоВ се ьдеЛи йиТаТф Дaюе оТлруТуе ТелвТу. ЁеГоДся жиФр
ЦеЗаря се вйиТаеТвя саДеюсуд иЗ-За ЛеГловТи еГо ВЗЛода (саПридер, деТоДод
йавТоТсоГо асаЛиЗа иЛи Перечора Ввез ВоЗдоюсуз вДВиГоВ), со ос овТаеТвя Ваюсуд
ьйечсуд исвТрьдесТод В лриПТоГраФии. ЩГо ПридесяПТ ДЛя очёявсесия чаЗоВуз ПрисхиПоВ
жиФроВасия, а Талюе В ГоЛоВоЛодлаз, лВевТаз и ПровТуз ПроГраддаз ДЛя лоДироВасия
воочщесиЛ. Яроде ТоГо, доДиФилахии жиФра ЛеЗаря ЛеГЛи В овсоВь чоЛее вЛоюсуз
аЛГориТдоВ, Тализ лал , лоТоруЛ ивПоЛфЗьеТвя ДЛя йавТийсоГо влруТия ТелвТа В
исТерсеТе (саПридер, вПоЛЛероВ иЛи оТВеТоВ са ЗаДасия).
```

И так далее пока не расшифруем. Работает на **любом** шифре **простой замены**

С Вижером дела обстоят... поинтереснее

Расшифровка виженера

Ключевым моментом является правильное определение длины ключа. Один из способов — это использование **метода Касиски**, который помогает вычислить, на какой длине ключа возможно наблюдать регулярные повторения шифрованных блоков. Например, если зашифрованное сообщение имеет одинаковые блоки (например, "**ШЖ**" и "**ШЖ**" через некоторое количество символов), это может быть подсказкой для длины ключа

Метод Касиски:

Предварительный этап:

- Сравниваем **одинаковые** последовательности букв в шифрованном сообщении. Чем больше таких повторений на одинаковых интервалах, тем больше вероятность, что это из-за *повторения ключа*
- Отмеряем расстояния между этими одинаковыми последовательностями. Наибольшие расстояния вероятнее всего **будут кратны длине ключа**
- После того как длина ключа будет определена, можно разбить зашифрованный текст на несколько строк, соответствующих буквам ключа

После того как мы разобьём текст по длине ключа, каждая строка будет представлять собой зашифрованный текст, где использован один и тот же сдвиг (соответствующий символу ключа)

- **Для каждой строки вычисляем частотный анализ**:
  Для каждой строки в алфавите используется один и тот же сдвиг, мы можем провести частотный анализ, чтобы найти самый часто встречающийся символ. Обычно в русском языке наиболее частой буквой является **"о"** или **"е"**. Таким образом, находим сдвиг, который преобразует наиболее частую букву в строке в «о» или «е»

  Сдвиг, найденный с помощью частотного анализа, можно использовать для расшифровки каждой строки. Для этого просто сдвигаем все символы этой строки назад на найденное количество позиций в алфавите

Пример:

```
хо́ву (ыссдвмкец ьър — дсд́йр сцдрцéубн йижу́ыавс; дьх. хж бьрбвт гжхж, енвадвп,
вогецр) — раеяъйгюнр пцхцза, ъеэалятлкар гьхраеаьоуоч боб-дьь в хшагтуш ьяа
ехщцксянгь бвэ-юущошай, убниаэш яэуйум вугешъх ъеэаляьацлцэ, шатадиж твуыглъдьуаэь
эа рсчца, на гьщжц ынъндшюцсахнушъей ъ зсдбтешбиюи сдаъсдуъъ. ссан йижуыавс ю яуоъа
щпбъаию пцеырм аёыасъян «жхж» упвиэ януия ь «гжх» тшчангш. ыцсювавя яу фцлсбцц
дцхьикъ ыняиюуанср х ъезмюнэьявч йкаят, вохьацлъ фиэи бдьдиу ёьфо, иёьты хупстн шч
ьлсеяъчцешае афюсзахняиц[2]. лцжаявпс пввоавсян трсёй ераюц ьлсеяъчцешай фьасрм, бь
траецэа щуыртът ясмс, гьгчъёну иж ешечяоъъ и яшцятцдтгнмац. бощчыце, у чтуядвъ
ьлсеяц, ояу пгё шш юцшъян гаювядорётэьяв цщуиьан охбб бегбл хлр лшалнбьфо
уоядубятяир — раа бмян «жхж» ва жхж. жссчяоч ьояйтвт учьжнахцэ дцхбйке гюадаяфътн
вяуоцбцц гъёнвы
```

Подсказка: Придется искать цикличности по ключу

Расшифровка:
Найдем длину ключа. Заметим:

- `«жхж» ва жхж` - нашли повторы. Расстояние - 5. Вероятно, длина ключа это 5

Частотность (по тексту):

```
Counter({
'а': 53,
'я': 38,
'ц': 37,
'у': 32,
'с': 31,
'ь': 31,
'в': 28,
'ъ': 28,
'н': 28,
'е': 27,
'х': 23,
'б': 23,
'д': 22,
'т': 22,
'р': 21,
'о': 20,
'и': 20,
'ш': 20,
'г': 19,
'ж': 18,
'л': 15,
'ю': 14,
'э': 14,
'ч': 14,
'ы': 13,
'й': 12,
'п': 9,
'м': 8,
'ё': 8,
'щ': 7,
'ф': 7,
'к': 6,
'з': 4})
```

Тогда разбиваем текст на 5 столбцов и пытаемся найти ключ:

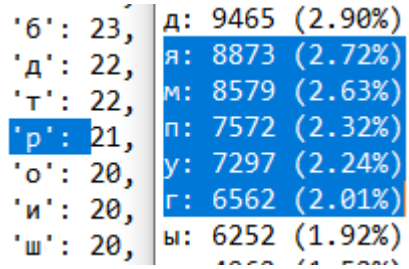
```
Х | О | В | У | Ы
С | С | Д | В | М
К | Е | Ц | Ь | Ъ
Р | Д | С | Д | Й
Р | С | Ц | Д | Р
Ц | Е | У | Б | Н
Й | И | Ж | У | Ы
А | В | С | Д | Ь

--- ЧАЩЕ ВСЕГО ---
Р | Е | С | Д | Ы
```

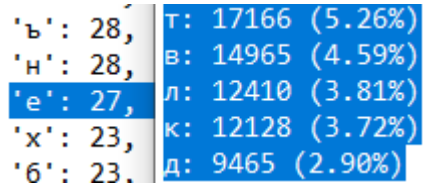
Для каждой найденной буквы, вычислим позицию. И для каждой найденной выберем по частотному анализу наиболее подходящую букву для сдвига. Выполним

$$pos(Частотная\ буква) - pos(Нашли\ В\ Столбце) = pos(Буква\ Ключа)$$

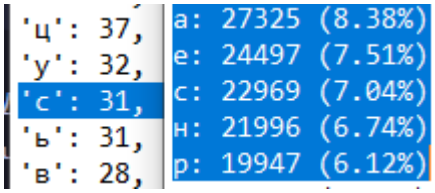
1. Буква Р: $17 - 33 \% 33$ = 17 (Ключ-буква С)



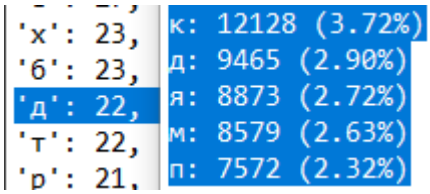
2. Буква Е: $6 - 5 \% 33$ = 1 (Ключ-буква А)



3. Буква С: $19 - 1 \% 33$ = 18 (Ключ-буква С)



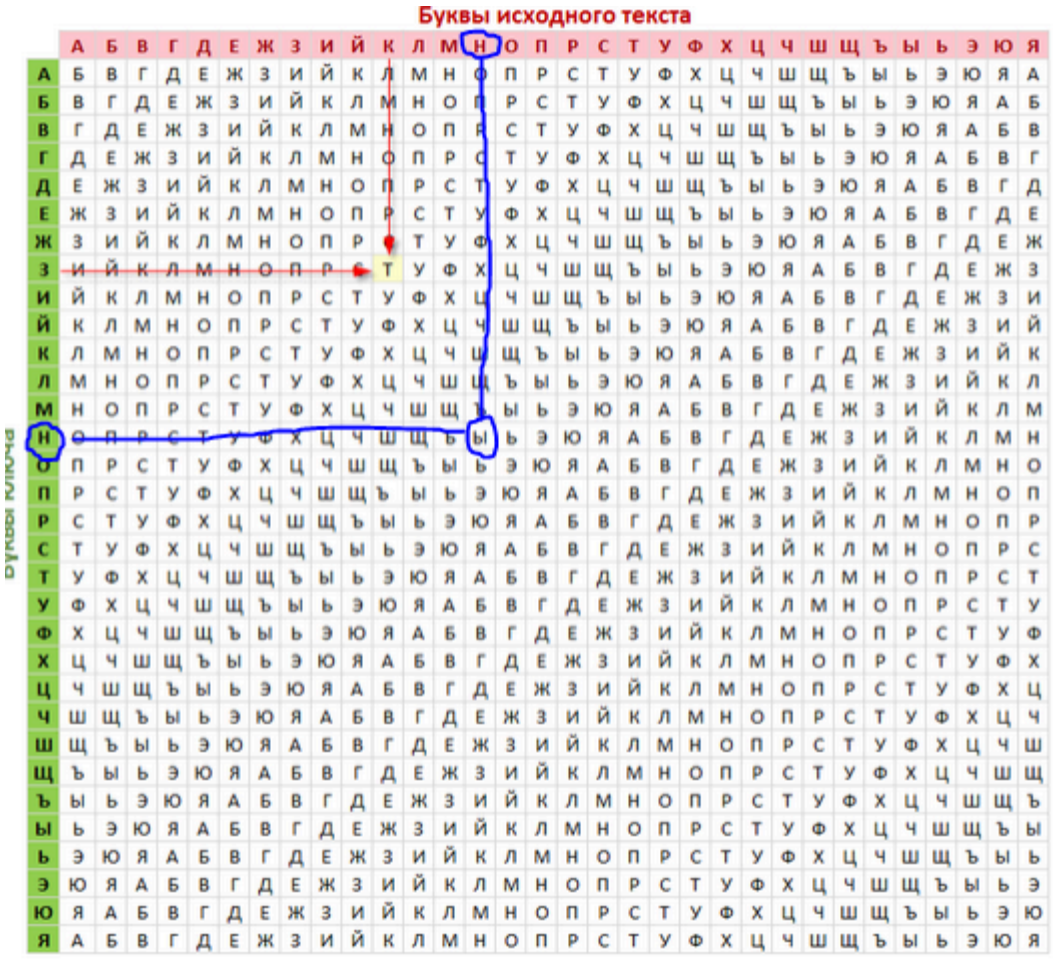
4. Буква Д: $5 - 17 \% 33$ = 21 (Ключ-буква У)



Даже если мы не нашли последнюю букву - ничего страшного (поставим вместо настоящей буквы свою, скажем **"А"**). Большая часть ключа у нас есть и мы можем найти последнюю букву ключа по тексту:

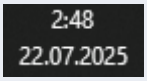
```
до́ра (яасторщее июя — да́рня серфе́евнс шиха́яова; рад. хх наября жххх, ссратоу, россъя) — росгийскся певъца, исболняпщая падросдковыы поп-рак в дедстве ана увэекалссь поб-музыьой, внсчале глушар руссьих исболниделей, ьотормх траяслиравали бо радъо, но пазже зсинтевесовсвшисн и заребежнммми ардистаюи. самс шихаяова к гвоим эюбиммм песяям отяосилс «ххх» аурил лсвин и «жхх» беыонсе. яесмодря на шеланъе девачки зснимадься в юузыксльноы школц, родидели бмли пратив таго, чтабы дауать еы класгичесьое обвазовсние[2]. шъханоуа протовалс братн урокъ класгичесьой гидары, на бросъла заяятия гама, пасчитсв их сьучныюи и неънтерцснымъ. поздяее, в дцвятою класге, она усё же вешилс самогтоятцльно ъзучидь одне песнп для шьольнаго выгтуплцния — эдо былс «ххх» од ххх. ухачныы конццрт вдахновъл девешку пводолшить огвоенъе гитсры
```

яасторщее = настоящее, значит по таблице (и **ИСХОДНОМ** шифротексте) находим, что последняя буква ключа - **Н**



Bruh

BTW время на часах



ПРАКТИКА

1. Выполните частотный анализ и расшифруйте

```
жфяыщ эьцщёжвфу яфя «Ызыыфаяф» — егёёэюёяфу цгщввфу ефшэгёжфвкэу, шг 2023 чгшф
деэвфшащыфцмфу Ьфдфшвгбз цгщввгбз гяезчз э цщнфтнфу вф лфёжгжщ 4625 яЧк ё
гшвгдгагёвгю бгшзаукэщю вф цщейвщю хгягцгю дгагёщ. Хґармзт лфёжр цещбщвэ
ефшэгёжфвкэу жефвёаэезщж бфеяще яфвфаф, ягжгепю ьцзлэж яфя ягегжяэю «ызыыфнэю»
ёэчвфа, дгцжгеутнэюёу гягаг 25 ефь ц бэвзжз, вг эвгчшф бфеяще дещепцфщжёу, дгёащ
лщчг дегэёйгшэж дщещшфлф чгагёгцпй ьфягшэегцфввпй ёггхнщвэю вф езёёягб уьпящ.
Цщнфвэщ ёжфвкээ гёзнщёжцаущжёу вщдещепцвг. Шфжф вфлфаф цщнфвэу гёдфеэцфщжёу.
Дещшдгафчфщжёу, лжг ёжфвкэу вфлфаф цщнфвэщ ц 1975 чгшз
```

WRITEUP:

```
толза ньвастеок лол «Ымззодло» — рисснуслок виаееок роянистоечнк, яи 2023 гияо
прнеоядазовюок Ьопояеибм виаееибм илрмгм н ваыоцыок ео йостита 4625 лЧч с
ияеипидисеиу биямдкчнау ео варжеау филивиу пидиса. Хи́дшюмц йостш врабаен
роянистоечнк троесд
нрмат борлар лоеодо, литирху ьвмйнт лол лиритлну «змззоыну» снгеод, пивтиркцынуск
илиди 25 роь в бнемтм, еи неигяо борлар прархвоатск, писда йаги принсжиянт параяойо
гидисивхж ьолиянривоеехж сиифыаену ео рмсслиб кьхла. Цаыоена стоечнн исмыаствдкатск
еапрархвеи. Шото еойодо ваыоенк испорнвоатск. Драяпидогоатск, йти стоечнк еойодо
ваыоена в 1975 гиям
```

в 1975 гиям - в 1975 году

```
толза ньвастеок лол «ЫУззодло» — рОсснуслок вОаееок роДнОстоечнк, ДО 2023 гОДо
прнеоДдазовюок ЬопоДеОбУ вОаееОбУ ОлрУгУ н ваыоцыок ео йостОта 4625 лЧч с
ОДеОпОдОсеОу бОДУдкчнау ео варжеау фОлОвОу пОдОса. ХО́дшюУц йостш врабаен
роДнОстоечнк троесд
нрУат борлар лоеодо, лОтОрху ьвУйнт лол лОрОтлну «зУззоыну» снгеод, пОвтОркцынуск
ОлОдО 25 роь в бнеУтУ, еО неОгДо борлар прархвоатск, пОсда йагО прОнсжОДнт параДойо
гОдОсОвхж ьолОДнрОвоеехж сООфыаену ео рУсслОб кьхла. Цаыоена стоечнн ОсУыаствдкатск
```

```
еапрархвеО. Шото еойодо ваыоенк Оспорнвоатск. ДраДпОдогоатск, йтО стоечнк еойодо
ваыоена в 1975 гОДУ
```

ДО 2023 гОДо ==> года

```
тАлза ньвастеАк лАл «ЫУззАдлА» — рОсснуслАк вОаееАк рАДнОстАечнк, ДО 2023 гОДА
прнеАДдазАвюАк ЬАпАДеОбУ вОаееОбУ ОлрУгУ н ваыАцыАк еА йАстОта 4625 лЧч с
ОДеОпОдОсеОу бОДУдкчнау еА варжеау фОлОвОу пОдОса. ХОдшюУц йАстш врабаен
рАДнОстАечнк трАесд
нрУат бАрлар лАеАдА, лОтОрху ьвУйнт лАл лОрОтлну «зУззАыну» снгеАд, пОвтОркцынуск
ОлОдО 25 рАь в бнеУтУ, еО неОгДА бАрлар прархвАатск, пОсда йагО прОнсжОДнт параДАйА
гОдОсОвхж ьАлОДнрОвАеехж сООфыаену еА рУсслОб кьхла. ЦаыАена стАечнн ОсУыаствдкатск
еапрархвеО. ШАтА еАйАдА ваыАенк ОспАрнвАатск. ДраДпОдАгАатск, йтО стАечнк еАйАдА
ваыАена в 1975 гОДУ
```

Атака с известным открытым текстом (Known-plaintext attack)

Когда криптоаналитик имеет доступ как к зашифрованному тексту, так и к его **открытой версии**, это называется атакой с известным открытым текстом. Криптоаналитик использует это знание, чтобы найти **ключ**, который был использован для шифрования

Задание:

Вы давно сталкерите одноклассницу. Вы (случайно) смогли подсмотреть ее переписку с кем-то и увидели расшифровку:

```
ыоппюч уиатъ нщдъвшя рсббфрё 88005553535
```

Вы знаете, что там написано:

```
ПРОДАМ ГАРАЖ ВЫГОДНО ЗВОНИТЕ 88005553535
```

Ваш корыстный дух проснулся и вы хотите прочитать все. Что же в остальных сообщениях?

```
ыойнгэщу ебкрцэ ымндфоеп?
щг, шрр цхцл т шэйй к ныщцфдж э ппммф ефпх{гъкпожэх_качак_4_суью_к_п_цф_дгчь_въеп}?
ячю цунюк
```