Конкурс на разработку ручного шифра

Условия

1. Ключ, открытый текст и шифртекст являются словами в русском алфавите.
2. Допускается замена символов алфавита числами. При этом должна использоваться следующая кодовая таблица:

А = 0	К = 11	Х = 22
Б = 1	Л = 12	Ц = 23
В = 2	М = 13	Ч = 24
Г = 3	Н = 14	Ш = 25
Д = 4	О = 15	Щ = 26
Е = 5	П = 16	Ъ = 27
Ё = 6	Р = 17	Ы = 28
Ж = 7	С = 18	Ь = 29
З = 8	Т = 19	Э = 30
И = 9	У = 20	Ю = 31
Й = 10	Ф = 21	Я = 32

3. Ключом может быть произвольное непустое слово.
4. Шифр должен противостоять атакам при выбираемом открытом тексте.
5. Зашифрование и расшифрование можно выполнить с помощью карандаша и бумаги, без применения вычислительной техники. Для ускорения шифрования разрешается использовать простые доступные в быту предметы: карты, лото, домино и пр.

Пример: шифр `Terminal`

Функция `terminal`

Символу $\alpha \in A$ поставим в соответствие число $\texttt{terminal}(\alpha)$ — количество концевых элементов (терминалов) в начертании символа. При подсчете терминалов используется заглавное начертание и шрифт без засечек (см. предыдущую таблицу). Точки над Ё не содержат терминалов, черточка над Й содержат два терминала. Примеры: $\texttt{terminal}(\text{Ж}) = 6$, $\texttt{terminal}(\text{Й}) = 4$, $\texttt{terminal}(\text{О}) = 0$, $\texttt{terminal}(\text{Ы}) = 3$, $\texttt{terminal}(\text{Щ}) = 4$.

Зашифрование

Зашифрование слова $X = x_1 \dots x_n$ на ключе $\theta = \theta_0 \dots \theta_{l-1}$ выполняется по следующему алгоритму:

1. $x_0 \xleftarrow{R} A$.
2. $j \leftarrow 0$.
3. Для $i = 0, \dots, n$:
   (1) $y_i \leftarrow (x_i + \theta_j) \bmod 33$;
   (2) $\theta_j \leftarrow (2x_i + y_i) \bmod 33$;
   (3) $j \leftarrow (j + \texttt{terminal}(x_i) + \texttt{terminal}(y_i) + 1) \bmod l$.
4. $Y \leftarrow y_0 y_1 \dots y_n$.
5. Возвратить Y.

Упражнения

1. Выписать алгоритм расшифрования.
2. Разработать атаку на `Terminal` по определению ключа θ. Разрешается выбирать открытые тексты X и наблюдать Y. Символы x_0, использованные при зашифровании, неизвестны.