

**Орудия Победы**

**ПРАКТИКО-ОРИЕНТИРОВАННОЕ ЗАДАНИЕ**

**Шифр Рамзая**

Шифр Рихарда Зорге (руководителя японской резидентуры ГРУ «Рамзай») о котором здесь пойдёт речь, нужно рассматривать как типовой образец действующих шифросистем всех советских спецслужб, а не приписывать его изобретение самому Зорге или искать в нём некую уникальность. Свои телеграммы в Москву Зорге для конспирации составлял преимущественно на английском языке. Поэтому в качестве ключа для построения квадратного шифра было выбрано слово “SUBWAY”, что переводится как «подземный ход».



В конце алфавита в таблице добавлено два знака. Это точка (.) и знак индикатора (/) – для обозначения разделителя слов или перехода на цифровой текст. Подробнее об этом ниже.

Однако таблица в подобном виде использовалась только для придания вошедшим в нее символам новых цифровых обозначений.

Известно, что наиболее часто встречаемые в английской речи восемь букв можно представить в виде анаграммы ASINTOER (фраза «a sin to err» («грех в заблуждении») без последней буквы). Её-то и использовал Зорге в качестве второго шага построения своего шифра. Для этого он нумеровал входящие в анаграмму буквы в своей табличке по порядку сверху вниз и получал новую таблицу:



Конечной целью разведчиков являлось составление следующего квадратного шифра:



Понять систему его построения нетрудно. В верхней строке мы видим наиболее встречаемые в английском языке буквы, которым даны цифровые обозначения от 0 до 7. В две оставшиеся строки выписаны по порядку остальные буквы из таблицы “SUBWAY” (то же сверху вниз). Они получают обозначения в виде двоичных чисел от 80 до 99. Как видно, в верхней строке конечные клетки под номерами 8 и 9 пустые. Эти цифры становятся номерами строк в ключевой таблице. Таким образом, здесь мы имеем воплощение идеи так называемого пропорционального шифра, позволяющее резко уменьшить количество входящих в шифрограмму знаков. В зависимости от размера текста это сокращение доходило до 30%. А это было очень важно для облегчения самого процесса шифровки, затруднения возможной дешифровки противником и уменьшения времени передачи радиограмм. Отделение же в тексте однозначных знаков от двузначных (конечно, при знании кодовой таблицы) не представляет никаких трудностей. Это была великолепная идея неизвестного нам советского криптолога, нашедшая затем широкое распространение в мировой криптографии.

Предположим, нужно зашифровать следующую телеграмму на немецком языке: «DAL. DER SOWJETISCHE FERNE OSTEN KANN ALS SICHER VOR EINEM ANGRIFF JAPANS ERACHTET WERDEN. RAMSAY» [DAL. Советский Дальний Восток может не опасаться нападения Японии. Рамзай]. Каждая радиограмма разведчиков начиналась их «обратным адресом»: DAL. Это были начальные буквы географического названия Дальний Восток. Заменяя буквы, знаки препинания и добавляя разделитель согласно квадратному шифру Зорге, получим:



Имея в виду, что шифротекст разведчики разбивали на 5-значные группы, последние цифры криптограммы или дополняли до полной пятёрки нулями, или просто удаляли.

Полученная первоначальная шифровка текста далее перекодировалась методом наложения на него бесконечной одноразовой цифровой гаммы по модулю 10. Способ её получения мог быть разным, начиная от использования так называемых одноразовых шифровальных блокнотов до преобразования букв определенного книжного текста в цифры.

*(Источник:* [*https://nightquests.ru/knowledgebases/shifr-ramzaya/*](https://nightquests.ru/knowledgebases/shifr-ramzaya/)*).*

**Задание.** Используя шифр Рамзая, создайте первоначальную шифровку для фразы «**Победа будет за нами**».