**Криптограмма**

*Криптограмма* – это довольно распространенный вариант головоломки из слов, которая имеет такую особенность: чем она длиннее, тем легче ее расшифровать. Коды появились еще в глубокой древности в виде криптограмм (по-гречески ‑ тайнопись). У древних иудеев существовал свой метод шифрования священных текстов (*атбаш*). Шифровали *методом замены*: вместо первой буквы алфавита писалась последняя буква, вместо второй - предпоследняя и так далее. С начала эпохи Возрождения начала возрождаться и *криптография* ‑ наука о методах обеспечения конфиденциальности информации. В качестве ключа в шифрующих таблицах используются: а) размер таблицы; b) слово или фраза, задающие перестановку; c) особенности структуры таблицы.

Одним из самых простых табличных шифров перестановки является *простая перестановка*, для которой ключом служит размер таблицы. Например, текст записывается в таблицу поочередно по столбцам. После заполнения таблицы текстом сообщения по столбцам для формирования шифртекста считывают содержимое таблицы по строкам.

Немного надежнее метод *одиночной перестановки* по ключу. Этот метод отличается от предыдущего тем, что столбцы таблицы переставляются по ключевому слову, фразе или набору чисел длиной в строку таблицы.

Метод, когда повторно шифруется сообщение, которое уже прошло шифрование, называется *двойной перестановкой*. В случае двойной перестановки столбцов и строк таблицы перестановки определяются отдельно для столбцов и отдельно для строк. Сначала в таблицу записывается текст сообщения, а потом поочередно переставляются столбцы, а затем строки. При расшифровании порядок перестановок должен быть обратным.

В средние века для шифрования перестановкой применялись и *магические квадраты* ‑ это квадратные таблицы с вписанными в их клетки последовательными натуральными числами, начиная от 1, которые дают в сумме по каждому столбцу, каждой строке и каждой диагонали одно и то же число. Шифруемый текст вписывали в магические квадраты в соответствии с нумерацией их клеток. Если затем выписать содержимое такой таблицы по строкам, то получится шифртекст, сформированный, благодаря перестановке букв исходного сообщения.