

Шифры перестановки

Занятие 2 (лекция)

§ 1. Основная часть

Простейшие шифры

Напомним, что среди всех шифров можно выделить два больших класса: *шифры замены* и *шифры перестановки*. На прошлом занятии мы подробно рассмотрели шифры замены. На данном занятии перейдем к рассмотрению так называемых шифров перестановки.

Шифр, преобразования которого изменяют только порядок следования символов исходного текста, но не изменяют их самих, называется *шифром перестановки*.

Понятие шифра перестановки

Каждое преобразование шифра перестановки, предназначенное для зашифрования сообщения длиной n символов, можно задать с помощью следующей таблицы.

$$\begin{array}{cccc} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{array}$$

где i_1 - номер места шифртекста, на которое перемещается первая буква исходного сообщения при выбранном преобразовании, i_2 - номер места для второй буквы и т. д. В верхней строке таблицы выписаны по порядку числа от 1 до n , а в нижней - те же числа, но в произвольном порядке. Такая таблица называется *подстановкой степени n* . Зная подстановку, задающую преобразование, можно осуществить как зашифрование, так и расшифрование текста.

Таким образом, подстановка является ключом шифра перестановки, при этом легко видеть, что число всех возможных шифров перестановок для текста заданной длины равно в точности числу ключей, или таблиц указанного вида (см. задачу № 1).

Например, если для преобразования используется подстановка

1 2 3 4 5 6
5 2 3 1 4 6

и в соответствии с ней зашифровывается слово МОСКВА, то получится КОСВМА.

1	2	3	4	5	6
М	О	С	К	В	А
К	О	С	В	М	А

Зададимся вопросом расшифрования шифра перестановки. Для этого также используется таблица – подстановка. Пусть на том же ключе, что и в предыдущем примере, зашифровано некоторое слово и получен шифртекст: НЧЕИУК. Покажем, как его нужно расшифровать.

Для этого составим подстановку (таблицу) «обратную» к нашему ключу, а именно, поменяем местами первую и вторую строки исходной таблицы и затем упорядочим столбцы по возрастанию номеров в первой строке.

1 2 3 4 5 6
4 2 3 5 1 6

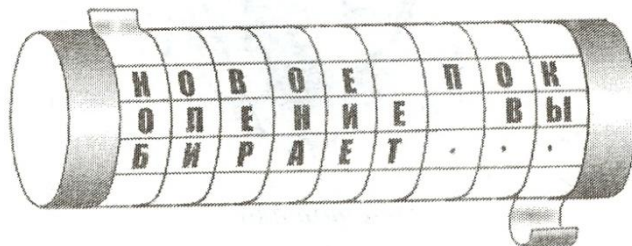
Термин «обратная» употреблен не зря, поскольку полученная таким образом таблица (подстановка) является ключом расшифрования. Действительно, если исходная таблица нам «говорила», что k -ую букву надо поставить на место i_k , то полученная же нам «говорит» обратное, то есть i_k -ую букву надо поставить на место с номером k .

И таким образом, применив преобразование перестановки используя ключ расшифрования, мы получим открытый текст.

1	2	3	4	5	6
Н	Ч	Е	И	У	К
У	Ч	Е	Н	И	К

Примеры шифров перестановки

1. **Шифр Сцитало.** Еще в V-IV вв до н.э. греки применяли специальное шифрующее устройство. Оно состояло из двух палок одинаковой длины и толщины. Одну оставляли себе, другую отдавали отъезжающему. Эти палки называли *сциталами* (*скиталами*). Когда правителям нужно было сообщить какую-нибудь важную тайну, они вырезали длинную и узкую, вроде ремня, полосу папируса, наматывали ее на свою сциталу, не оставляя на ней никакого промежутка, так чтобы вся поверхность палки была охвачена этой полосой. Затем оставляя папирус на сцитале в том виде, как он есть, писали на нем все что нужно, а написав, снимали полосу и отправляли адресату без палки. А так как буквы на этой полоске разбросаны в беспорядке, то прочитать написанное адресат мог, только взяв свою сциталу и намотав на нее без пропусков полосу.



Отметим, что при использовании шифра Сцитало первая буква открытого текста переходит в первую букву шифртекста, дальше из открытого текста выбирается через определенное и постоянное число букв вторая буква шифрсообщения и т. д., пока не достигается конец сообщения. Затем в качестве следующей буквы шифртекста выбирается вторая буква открытого текста и процедура продолжается, пока не будут переставлены все буквы сообщения.

2. **Шифр маршрутной перестановки.** Широкое распространение получили шифры перестановки, использующие некоторую

геометрическую фигуру. Преобразования из этого шифра состоят в том, что в некоторую фигуру, обычно прямоугольник, исходный текст вписывается по ходу одного «маршрута», а затем по ходу другого выписывается с нее. Такой шифр называют маршрутной перестановкой. Например, можно вписывать исходное сообщение в прямоугольную таблицу, выбрав такой маршрут: по горизонтали, начиная с левого верхнего угла поочередно слева направо и справа налево. Выписывать же сообщение будем по другому маршруту: по вертикали, начиная с верхнего правого угла и двигаясь поочередно сверху вниз и снизу вверх.

Зашифруем, например, фразу:

ПРИМЕР МАРШРУТНОЙ ПЕРЕСТАНОВКИ

используя прямоугольник размера 4×7 :

П	Р	И	М	Е	Р	М
Н	Т	У	Р	Ш	Р	А
О	Й	П	Е	Р	Е	С
И	К	В	О	Н	А	Т

Зашифрованная фраза выглядит так:

МАСТАЕРРЕШРНОЕРМИУПВКЙТРПНОИ

Теоретически маршруты могут быть значительно более изощренными, например обход конем шахматной доски таким образом, чтобы в каждой клетке побывать один раз. Один из таких замкнутых маршрутов был найден знаменитым математиком Леонардом Эйлером в 1759 г.

3. **Шифр вертикальной перестановки.** Также хорошо известна разновидность шифра маршрутной перестановки - шифр вертикальной перестановки. Для построения этих шифров используется прямоугольник с m столбцами, в который сообщение вписывается обычным способом (по строкам слева направо). Затем задается ключ, то есть выбирается некоторая подстановка степени m . Выписываются

буквы по вертикали, а столбцы при этом берутся в порядке, определяемом этим ключом.

Пусть, например, этот ключ такой:

$$\begin{matrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 4 & 1 & 7 & 2 & 6 & 3 \end{matrix}$$

и с его помощью надо зашифровать сообщение:

ВОТ ПРИМЕР ШИФРА ВЕРТИКАЛЬНОЙ ПЕРЕСТАНОВКИ

Впишем сообщение в прямоугольник, столбцы которого пронумерованы в соответствии с ключом.

5	1	4	7	2	6	3
В	О	Т	П	Р	И	М
Е	Р	Ш	И	Ф	Р	А
В	Е	Р	Т	И	К	А
Л	Ь	Н	О	Й	П	Е
Р	Е	С	Т	А	Н	О
В	К	И	-	-	-	-

Теперь, выбирая столбцы в порядке, заданном ключом, и выписывая последовательно буквы каждого из них сверху вниз, получаем такую криптограмму:

ОРЕЪЕКРФИЙА-МАОЕО-ТШРНСИВЕВЛРВИРКПН-ПИТОТ-

§ 2. Решение задач

Задача № 1

Известно, что ключом шифра перестановки является таблица – подстановка степени n , где n – длина текста. Найдите число всех возможных ключей шифра перестановки для текста длины n .

Решение:

Ключом шифра перестановки является таблица вида:

$$\begin{matrix} 1 & 2 & \dots & n \\ i_1 & i_2 & \dots & i_n \end{matrix}$$

Число ключей равно числу различных наборов i_1, i_2, \dots, i_n , являющихся перестановками чисел $\{1, 2, \dots, n\}$. Посчитаем сколькими способами можно выбрать набор i_1, i_2, \dots, i_n .

- значение i_1 можно выбрать n способами, то есть сделать любым из $\{1, 2, \dots, n\}$;
- значение i_2 можно выбрать $n-1$ способом, поскольку оно может быть любым из $\{1, 2, \dots, n\}$, но не может совпадать с i_1 , которое уже выбрано;
- значение i_3 можно выбрать $n-2$ способом, поскольку оно может быть любым из $\{1, 2, \dots, n\}$, но не может совпадать с i_1 и i_2 , которые уже выбраны;
- ...
- значение i_n можно выбрать 1 способом, поскольку оно определяется однозначно по уже выбранным $n-1$ значениям.

Таким образом, число таких наборов равно:

$$n \cdot n - 1 \cdot \dots \cdot 1$$

то есть числу, равному произведению первых n подряд идущих натуральных чисел, оно обозначается $n!$ и читается «эн факториал».

Ответ: $n!$

Задача № 2

Сообщение

IT IS MORE THAN A FEELING

зашифровано с помощью шифра Сцитало. Может ли начало этого сообщения перейти в один из указанных фрагментов шифрованного текста:

- IMTF...
- IEEI...
- TSOE...
- IOAE...

Решение:

При использовании шифра Считало для формирования шифртекста сначала выбирается 1-ая буква открытого текста (вариант 3 не удовлетворяет этому требованию), затем $(k+1)$ -буква, $(2k+1)$ -буква и т.д., для некоторого k , равного числу букв в каждой строке считалы.

Значение k является постоянной величиной для данной считалы, в связи с чем:

- вариант 1 отвергается, так как для варианта 1 параметр $k = 4$ и после символа T должна идти буква A .
- вариант 2 тоже не верный, поскольку для него $k = 7$ и поэтому после E должна идти буква T ;

Остается единственный правильный вариант 4 при котором $k = 5$.

Ответ: 4 вариант.

Задача № 3

Сообщение

SOKYDIOLIGCWUUNO

зашифровано с помощью шифра вертикальной перестановки на ключе

1 2 3 4 5 6
3 5 4 1 6 2

Прочитайте данный текст.

Решение:

Известна длина ключа. В данном случае, число столбцов в ключевой таблице равна 6. Всего букв шифрованного текста 16. $16=2\cdot6+4$. Таким образом, приходим к выводу, что в таблице, в которую записывался изначально текст, находится три строки, последняя самая короткая, содержит 4 символа. В частности это означает, что в каждом из столбцов содержится по три буквы, за исключением последних двух 5 и 6 - в них по две буквы.

В условии задачи дан ключ зашифрования, поэтому можно выписать ключ расшифрования, просто поменяв его строки местами:

1 2 3 4 5 6
4 6 1 3 2 5

Так как первый столбец согласно ключу расшифрования должен стать четвертым, а он является «длинным» (то есть в нем 3 буквы), то его содержимое: SOK. Далее, второй столбец должен стать шестым, а он является «коротким» (то есть в нем 2 буквы), то его содержимое: YD и т.д. Получим следующую разбивку на столбцы.

S	Y	I	I	W	H
O	D	O	G	U	O
K		L	C	U	

Меняем их местами в соответствии с ключом расшифрования

I	W	I	S	H	Y
O	U	G	O	O	D
L	U	C	K		

Получаем открытое сообщение: I WISH YOU GOOD LUCK.

Ответ: *I WISH YOU GOOD LUCK.*

Задача № 4

Сколько различных шифртекстов можно получить, используя шифр перестановки, если открытый текст:

- РЕВОЛЮЦИЯ;
- КАРТИНА;
- ИГРАЛЬНАЯДОСКА.

Решение:

- Рассмотрим первое слово. В нем все буквы различны поэтому число различных слов, которые можно получить из данного, просто равно числу перестановок его букв, или что то же самое, числу ключей шифра перестановки при $n = 9$. Как известно из задачи 1, данное число равно $9!$.

- Второе слово имеет длину 7. Число перестановок его букв равно $7!$. В то же время надо заметить, что не всякая перестановка букв дает разные шифртексты. Это так, поскольку в данном слове 2 одинаковые буквы А, поэтому если их менять местами, получим один и тот же шифртекст (но при этом перестановки разные). Пусть имеем некоторую перестановку букв данного слова, и при этом буквы А оказались на местах i_1 и i_2 соответственно. Тогда та же перестановка, но в которой буквы А будут стоять на местах i_2 и i_1 соответственно, будет давать один и тот же шифртекст. Таким образом, каждому шифртексту соответствует в точности 2 различных перестановки (при этом очевидно, что различным шифртекстам соответствуют различные перестановки). Пусть теперь x – число различных шифртекстов. Поскольку число всех перестановок равно $7!$, то $2 \cdot x$ равно $7!$. Значит, $x = \frac{7!}{2}$.
- Данное словосочетание имеет длину 14. Число перестановок его букв равно $14!$. В то же время надо заметить, что не всякая перестановка букв дает разные шифртексты. Это так, поскольку в данном словосочетании 3 одинаковые буквы А, поэтому если их менять местами, получим один и тот же шифртекст (но при этом перестановки разные). Пусть имеем некоторую перестановку букв данного словосочетания, и при этом буквы А оказались на местах i_1, i_2, i_3 соответственно. Тогда та же перестановка, но в которой буквы А будут стоять на местах, скажем, i_2, i_3, i_1 соответственно, будет давать один и тот же шифртекст. Более того каким бы образом мы не переставляли между собой места i_1, i_2, i_3 - будем получать все тот же шифртекст. Таким образом, каждому шифртексту соответствует столько различных перестановок, сколько всего существует перестановок элементов множества $\{i_1, i_2, i_3\}$. А их всего в точности $3! = 6$. Пусть теперь x – число различных шифртекстов, тогда $6 \cdot x$ равно $14!$. Значит, $x = \frac{14!}{6}$.

Ответ: 362 880; 2 520; 14 529 715 200.

Задача № 5

Для зашифрования сообщения на русском языке его записывают в одну строку без пробелов и знаков препинания. В получившейся цепочке буквы нумеруются слева направо числами от 1 до L . Зашифрование происходит путем перестановки букв исходной цепочки по следующему правилу. Фиксируем два натуральных числа a и b . Буква с номером n в исходной цепочке должна в зашифрованной цепочке иметь номер, равный остатку от деления числа $a \cdot n + b$ на L (с одним исключением: если $a \cdot n + b$ нацело делится на L , то остаток полагается равным L). Известно, что в результате применения этого метода зашифрования к цепочке из 43 букв

СВЕТИТНЕЗНАКОМАЯЗВЕЗДАСНОВАМЫОТОРВАНЫОТДОМА

была получена цепочка

ТАЫТОЕОНСООВЗМЕВТРАДАЗЕДВМАЯНТОАЫСЗАИМНОНВК

При этих же значениях a и b , проведено зашифрование еще некоторой цепочки из 38 букв. Получилось вот что:

ВИДХЪВРЛМАОЯОЮАЮДДСЕМДРОИВВООЕОЗТООБНЗО

Найдите значения a и b и восстановите исходное сообщение.

Решение:

Для начала найдём в открытом тексте две уникальные буквы (по возможности близкие). Это, например, К и Я, стоящие соответственно на 12 и 16 позициях в открытом тексте. В шифрованном тексте они стоят соответственно на местах 43 и на 28.

Составляем систему уравнений

$$\begin{cases} 12a + b = 43k \\ 16a + b = 28 + 43l \end{cases}$$

Следовательно $4a = 28 + 43m$. При $m = 0$ находим $a = 7$, из первого уравнения находим $b = 2$.

Расшифровав второй текст, получим искомое сообщение:

МОРОЗВОЕВОДАДОЗОРОМОБХОДИТВЛАДЕНЬЯСВОИ

Ответ: МОРОЗВОЕВОДАДОЗОРОМОБХОДИТВЛАДЕНЬЯСВОИ.

Задача № 6

Сообщение записано в таблицу размера 7×3 слева направо сверху вниз. Затем сверху вниз были выписаны буквы из таблицы: сначала из пятого столбца таблицы, затем из первого, потом из седьмого, второго, четвертого, шестого и третьего:

ВАБОЛВЕЫЕКЪТСРТЙЕ.

Что это было за сообщение?

Решение:

Всего в данную таблицу вмещается 21 буква. В то же время сообщение имеет длину, равную 17. Это означает, что в третьей (последней) строке таблицы последние 4 ячейки не заполнены, а значит столбцы с номерами с 4 по 7 являются короткими, то есть в них содержится только по две буквы.

1	2	3	4	5	6	7

Зная это, определим разбивку текста на столбцы.

ВА БОЛ ВЕ ЫЕК ЪТ СР ТЙЕ.

Остается только вписать в соответствии с этой разбивкой буквы в столбцы, как сказано в условии задачи.

1	2	3	4	5	6	7
Б	Ы	Т	Ь	В	С	В
О	Е	Й	Т	А	Р	Е
Л	К	Е				

Получим ответ:

БЫТЬ В СВОЕЙ ТАРЕЛКЕ

Ответ: БЫТЬ В СВОЕЙ ТАРЕЛКЕ.