Шифрование методами замены

В криптографии рассматриваются четыре типа подстановки (замены): моноалфавитная, полиалфавитная, гомофоническая и полиграммная.

Далее всюду в примерах использовано кодирование букв русского алфавита, приведенное в табл. 1.

Таблица 1. Кодирование букв русского алфавита

Буква	А	Б	В	Г	Д	Е	ж	З	И	И	К	Л
Код	00	01	02	03	04	05	06	07	08	09	10	11
Буква	М	Н	о	П	Р	С	Т	У	Ф	Х	Ц	Ч
Код	12	13	14	15	16	17	18	19	20	21	22	23
Буква	Ш	щ	Ъ	ы	Ь	Э	Ю	Я	D (пробел)			
Код	24	25	26	27	28	29	30	31	32			

При ***моноалфавитной замене*** каждой букве алфавита открытого текста ставится в соответствие одна буква шифртекста из этого же алфавита.

Общая формула моноалфавитной замены выглядит следующим образом

$$y_i = k_1 x_i + k_2 (mod n),$$

где y_i — i-й символ алфавита k_1 и k_2 — константы, x_i — i-й символ открытого текста (номер буквы в алфавите), n — длина используемого алфавита

Основным недостатком рассмотренного метода является то, что статистические свойства открытого текста (частоты появления букв) сохраняются и в шифртексте

Пример 1. Открытый текст «ШИФРОВАНИЕ ЗАМЕНОЙ» Подстановка задана табл 2

Таблица 2 Подстановка алфавита для шифрования заменой

Алфавит исходного текста	А	Б	В	Г	Д	…	Ь	Э	Ю	Я	А
Алфавит шифртекста	D	Я	Ю	Э	Ь	…	Д	Г	В	Б	А

Шифртекст «ИШМРТЮПУШЫАЩаФЫУТЧ»

Шифр, задаваемый формулой

$$y_i = x_i + ki (mod n),$$

где *ki* — i- *я* буква ключа, в качестве которого используется слово или фраза

$$a \bmod b = a - b \times \mathrm{floor}(a/b) \quad (*)$$

называется *шифром Вижинера*

Пример 2. Открытый текст «ЗАМЕНА» Подстановка задана в табл 3

Таблица 3 Подстановка шифра Вижинера

З	А	М	Е	н	А
К	Л	Ю	Ч	к	Л

$y_i = 8 + 11(\text{mod}33) = 19 \rightarrow$- Т,

$y_З = 1 + 12(\text{mod}33) = 13 \rightarrow M,$

$y_i = 13+31(\text{mod}33)= 11 \rightarrow$ К,

$У4 = 6 + 24(\text{mod } 33) = 30 \rightarrow$ Э,

$y_i = 14 + 11(\text{mod}33) = 25 \rightarrow$ Ш,

$y_В = 1 + 12(\text{mod } 33) = 13 \rightarrow M$

Шифртекст «ТМКЭШМ»

Шифры Бофора используют формулы

$$y, = k, - x, (\text{mod n}) \text{ и } y = ж, — fci(\text{mod}n)$$

Полиалфавитная замена использует несколько алфавитов шифртекста Пусть используется *k* алфавитов Тогда открытый текст

$$X = XiX\text{-}l...XkXk+\backslash\text{---}X2kX\text{-}2k+\backslash ...$$

заменяется шифртекстом

$$Y = /l(\hat{}l)/2(\hat{}2) \ldots A(\hat{}fc)/l(a\text{-}t+l) \ldots \bullet fk\{x'ik\}fl(x2k+l) \bullet\bullet\text{-},$$

где *fi[x^)* означает символ шифртекста алфавита г для символа открытого текста *Xj*.

Пример 3. Открытый текст: «ЗАМЕНА», *k* = 3. Подстановка задана таблицей 4 Шифртекст- «7б 31 61 97 84 48».

Гомофоническая замена одному символу открытого текста ставит в соответствие несколько символов шифртекста. Этот метод применяется для искажения статистических свойств шифртекста.

Пример 4. Открытый текст «ЗАМЕНА» Подстановка задана табл. 4.

Таблица .4- Подстановка алфавита гомофонической замены

Алфавит открытого	А	Б	…	Е	Ж	З	…	М	Н	…
Алфавит шифртекста	17 31 48	23 44 63	… …	97 51 15	47 67 33	76 19 59	… …	32 28 61	55 84 34	… …

Шифртекст. «76 17 32 97 55 31»

Таким образом, при гомофонической замене каждая буква открытого текста заменяется по очереди цифрами соответствующего столбца.

Полиграммная замена формируется из одного алфавита с помощью специальных правил. В качестве примера рассмотрим шифр *Плэйфера*

В этом шифре алфавит располагается в матрице Открытый текст разбивается на пары символов *x^.x,^.* Каждая пара символов открытого текста заменяется на пару символов из матрицы следующим образом:

- если символы находятся в одной строке, то каждый из символов пары заменяется на стоящий правее его (за последним символом в строке следует первый),
- если символы находятся в одном столбце, то каждый символ пары заменяется на символ, расположенный ниже его в столбце (за последним нижним символом следует верхний),
- если символы пары находятся в разных строках и столбцах, то они считаются противоположными углами прямоугольника Символ, находящийся в левом углу, заменяется на символ, стоящий в другом левом углу, замена символа, находящегося в правом углу, осуществляется аналогично,
- если в открытом тексте встречаются два одинаковых символа подряд, то перед шифрованием между ними вставляется специальный символ (например тире)

Пример 5. Открытый текст. «ШИФР ПЛЭЙФЕРА» Матрица алфавита представлена в табл. 5.

Таблица.5. Матрица алфавита шифра Плэйфера

А	Ж	Б	м	ц	в
Ч	Г	Н	ш	д	о
Е	Ш	.	х	У	п
	З	ъ	р	и	и
С	ь	к	э	т	л
Ю	я	а	ы	ф	—

Шифртекст: «РДЫИ-СТ-И.ХЧС»

При рассмотрении этих видов шифров становится очевидным, что чем больше длина ключа (например в шифре Вижинера), тем лучше шифр Существенного улучшения свойств шифртекста можно достигнуть при использовании шифров с автоключом

Шифр, в котором сам открытый текст или получающаяся криптограмма используются в качестве ключа, называется шифром с автоключом. Шифрование в этом случае начинается с ключа, называемого первичным, и продолжается с помощью открытого текста или криптограммы, смещенной на длину первичного ключа

Пример 6. Открытый текст «ШИФРОВАНИЕ ЗАМЕНОЙ». Первичный ключ. «КЛЮЧ». Схема шифрования с автоключом при использовании открытого текста представлена в табл. 6.

Таблица.6. Схема шифрования с автоключом при использовании открытого текста

Ш	и	Ф	Р	0	в	А	Н	и	Е	а	З	А	м	Е	Н	0	И
К	л	Ю	Ч	Ш	и	Ф	Р	о	В	А	Н	И	Е	а	З	А	М

36	21	52	41	40	12	22	31	24	09	34	22	10	19	39	22	16	23
в	Ф	Т	3	Ж	Л	Х	Ю	Ч	И	А	Х	И	Т	Е	Х	П	Ц

Схема шифрования с автоключом при использовании криптограммы представлена в табл. 7.

Таблица .7. Схема **шифрования с автоключом при использовании** криптограммы

Ш	и	Ф	Р	о	В	А	Н	И	Е	а	3	А	М	Е	Н	0	И
К	л	Ю	Ч	в	Ф	Т	3	С	Ч	У	Х	Ъ	Э	У	Э	Ы	И
36	21	52	41	18	24	20	22	27	30	53	30	24	43	26	44	39	20
в	Ф	Т	3	С	Ч	У	Х	Ъ	э	У	э	Ы	И	Щ	К	И	У

Для шифрования используются и другие методы перестановки символов открытого текста в соответствии с некоторыми правилами

Пример 7. Открытый текст «ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ»

Ключ (правило перестановки) группы из восьми букв с порядковыми номерами 1 2 8 переставить в порядок 38152764

Шифртекст «ФНШОИАВРПСИЕЕЕРПНИТВАОКО»

Можно использовать и усложненную перестановку Для этого открытый текст записывается в матрицу по определенному ключу А] Шифртекст образуется при считывании из этой матрицы по ключу *Ку*

Пример .8. Открытый текст «ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ»

Матрица из четырех столбцов приведена в табл 8, где запись по строкам в соответствии с ключом /\i 5 3 1 2 4 6. а чтение по столбцам в соответствии с ключом Кз 4231

Таблица 8. Матрица алфавита с перестановкой из четырех столбцов

1	И	Е	D	п
2	Е	Р	Е	с
3	0	В	А	Н
4	Т	А	Н	о
5	Ш	И	Ф	Р
6	в	К	0	и
к>^2	1	2	3	4

Шифртекст «ПСНОРЙЕРВАИКПЕАНФОИЕОТШВ»

Наиболее сложные перестановки осуществляются по гамильтоновым путям, которых в графе может быть несколько

Пример 9. Открытый текст «ШИФРОВАНИЕ ПЕРЕСТАНОВКОЙ» Ключ — гамильтонов путь на графе (рис 2)

Шифртекст «ШАОНИРФВИЕЕСЕППРТОВЙАОНК»

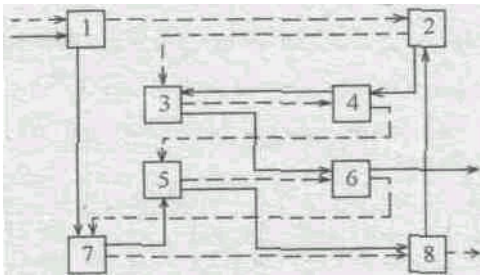

Рис. 2. Гамильтонов путь на графе

Чтение криптограммы (1-7-5-8-2-4-3-6)

Запись открытого текста (1-2-3-4-5-6-7-8)

Необходимо отметить, что для данного графа из восьми вершин можно предложить несколько маршрутов записи открытого текста и несколько гамильтоновых путей для чтения криптограмм.

В 1991 г В М Кузьмин предложил схему перестановки, основанную на кубике Рубика Согласно этой схеме открытый текст записывается в ячейки граней куба по строкам После осуществления заданного числа заданных поворотов слоев куба считывание шифртекста осуществляется по столбцам Сложность расшифрования в этом случае определяется числом ячеек на гранях куба и сложностью выполненных поворотов слоев. Перестановка, основанная на кубике Рубика, получила название объемной (многомерной) перестановки

В 1992—94 гг идея применения объемной перестановки для шифрования открытого текста получила дальнейшее развитие Усовершенствованная схема перестановок по принципу кубика Рубика, в которой наряду с открытым текстом перестановке подвергаются и функциональные элементы самого алгоритма шифрования, легла в основу секретной системы «Рубикон» В качестве прообразов пространственных многомерных структур, на основании объемных преобразований которых осуществляются перестановки, в системе «Рубикон» используются трехмерный куб и тетраэдр