Шифрование

Шифрование

Шифрование — обратимое преобразование информации в целях сокрытия от неавторизованных лиц, с предоставлением, в это же время, авторизованным пользователям доступа к ней. Процесс преобразования осуществляется с использованием специальных объектов (ключей).

Различают две составляющих процесса преобразования – **зашифровывание** и **расшифровывание**. Обе эти составляющие реализуются при помощи определенных алгоритмов.

Совокупность алгоритмов зашифровывания и расшифровывания составляет **алгоритм шифрования** (шифр, криптосистему).

Шифрование

Криптография – это наука о методах обеспечения конфиденциальности, целостности данных, аутентификации. Кроме систем шифрования в сферу изучения криптографии также входят системы электронной подписи (ЭЦП), хеш-функции, управление ключами, получение скрытой информации, квантовая криптография.

Криптографический анализ (криптоанализ) – методы нарушения целостности и конфиденциальности зашифрованной информации.

Криптографическая стойкость (криптостойкость) – способность противостоять криптоанализу.

Шифрование

Алгоритм шифрования считается **криптостойким**, если для его раскрытия необходимы либо огромные вычислительные и финансовые ресурсы, либо большое количество ранее перехваченных исходных и зашифрованных сообщений, либо такие затраты времени, что к моменту раскрытия информация безнадежно утратит актуальность.

Шифрование

Классификация алгоритмов шифрования

1. **Симметричные алгоритмы шифрования** – как отправитель, так и получатель используют один и тот же ключ.

1.1. **Блочные алгоритмы шифрования** - шифрование производится блоками, размер блока зависит от конкретного криптографического алгоритма.

1.1.1. **Шифры замены** – одни блоки заменяются на другие в определенной последовательности.

1.1.2. **Шифры перестановки** – одни блоки переставляются на место других блоков в определенной последовательности.

Шифрование

Классификация алгоритмов шифрования (продолжение)

1.2. **Потоковые алгоритмы шифрования** – шифрование последовательно всего объема информации с использованием гаммирования.

1.3. **Составные алгоритмы шифрования** – шифрование с использованием методов и блочных, и потоковых алгоритмов.

2. **Асимметричные алгоритмы шифрования** – для зашифровывания и расшифровывания используются два разных ключа, сгенерированных по одному принципу. При этом отправителю не известен ключ получателя.

Блочные шифры

Блочные шифры

Для шифрования исходное (открытое) сообщение делится на блоки, размер которых определен для каждого конкретного шифра. Зашифровывается и расшифровывается каждый блок отдельно.

Блочные шифры

1.1.1. Шифры замены

В шифрах замены происходит замена одних блоков текста на другие в определенной последовательности.

Блочные шифры

1.1.1. Шифры замены

Различают шифры замены:

- шифры однозначной замены;
- полиграммные шифры;
- омофонические шифры;
- полиалфавитные шифры.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифры однозначной замены предполагают, что каждый символ исходного сообщения должен быть заменен одним символом (одной комбинацией символов) алфавита замены.

Такие шифры еще называют моноалфавитными или простыми подстановочными.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Цезаря

- Исходный алфавит выписывается в строку, затем под ним, в следующую строку, выписывается тот же алфавит, но с определенным циклическим сдвигом влево.
- Ключом в шифре Цезаря является величина сдвига нижней строки алфавита. Количество возможных ключей равно количеству символов алфавита, который был использован (для русского алфавита – 33).

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Цезаря

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В

Пример:

Ключ шифрования К=3										
М:	И	Н	Ф	О	Р	М	А	Ц	И	Я
С:	Л	Р	Ч	С	У	П	Г	Щ	Л	В

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Лозунговый шифр

- В качестве ключа используется определенное слово – лозунг.
- В первую строку таблицы шифрозамен также записывается исходный алфавит, а вторая строка заполняется сначала буквами лозунга (причем повторяющиеся буквы отбрасываются), а затем остальными буквами алфавита, не вошедшими в лозунг, в алфавитном порядке.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Лозунговый шифр

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Т	Р	А	Н	С	Л	Я	О	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	М	П	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю

Пример:

К:	Т	Р	А	Н	С	Л	Я	Т	О	Р
М:	П	Р	О	Ц	Е	С	С	О	Р	-
С:	И	Й	З	Х	Л	К	К	З	Й	-

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Полибианский квадрат

Для создания таблицы шифрозамен используется квадратная матрица, количество ячеек которой должно позволить разместить в ней используемый алфавит с условием, что количество пустых (незаполненных) ячеек окажется минимальным. Строки и столбцы матрицы нумеруются. В матрицу вписываются буквы используемого алфавита, оставшиеся пустыми ячейки заполняются какими-либо заранее оговоренными произвольными символами.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Полибианский квадрат

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	С	Т	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	-	-	-

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Полибианский квадрат

- Ключами являются размер матрицы (для русского алфавита – 6x6), маршрут вписывания букв алфавита в матрицу (по строкам или по столбцам).
- Результатом зашифровывания для каждой буквы исходного сообщения является адрес ячейки, в которой она расположена.
- При расшифровывании произвольные символы отбрасываются.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Полибианский квадрат

Пример:

К:	6	x	6	-	-	-	-	-	-	-	-	-	-
М:	Ф	О	Р	М	А	Т	И	Р	О	В	А	Н	И	Е
С:	44	34	36	32	11	42	24	36	34	13	11	33	24	16

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

Таблица шифрозамент представляет собой квадратную матрицу, размер которой определяется аналогично размеру матрицы для полибианского квадрата.

Однако дополнительно в данном шифре используется лозунг, который первым вписывается матрицу по строкам (причем повторяющиеся буквы лозунга отбрасываются), а затем матрица заполняется буквами алфавита, не вошедшими в лозунг, оставшиеся пустыми ячейки заполняются какими-либо заранее оговоренными произвольными символами.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

- Ключами являются размер матрицы (для русского алфавита – 6x6) и секретное слово-лозунг.
- При зашифровывании каждая буква исходного сообщения заменяется буквой, расположенной под ней в том же столбце. Если буква находится в последней строке матрицы, то она заменяется самой верхней буквой столбца.
- При расшифровывании произвольные символы отбрасываются.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

Пример:

А	П	Р	О	К	С
И	М	Ц	Я	Б	В
Г	Д	Е	Е	Ж	З
Й	Л	Н	Т	У	Ф
Х	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	-	-	-

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

Пример:

К:	А	П	П	Р	О	К	С	И	М	А	Ц	И	Я	-	6	х	6
М:	П	Р	О	Г	Р	А	М	М	И	Р	О	В	А	Н	И	-	-
С:	М	Ц	Я	Й	Ц	И	Д	Д	Г	Ц	Я	З	И	Ш	Г	-	-

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

В полиграммных шифрах замене подлежит сразу блок символов исходного сообщения. Однако, по аналогии с шифрами однозначной замены, существует только один вариант такой замены.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

- Таблица шифрозамен формируется аналогично таблице для шифра Трисемуса.
- Ключами являются размер матрицы (для русского алфавита – 6x6) и секретное слово-лозунг.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

- Исходное сообщение разбивается на биграммы. В биграммах не должно содержаться двух одинаковых символов, в случае, если такое случается, то между одинаковыми символами добавляется какой-либо заранее оговоренный символ, как правило, редко встречающаяся буква алфавита (для русского языка часто используется буква Я).
- В случае если последняя биграмма сообщения содержит одну (последнюю) букву, к ней также добавляется вспомогательный символ.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

Зашифровываются биграммы исходного текста следующим образом:

1) Если символы биграммы исходного текста встречаются в таблице шифрозамен в одной строке, то они заменяются символами, расположенные в той же строке, справа от исходных символов. Если символ является последним в строке, то он заменяется первым символом этой же строки.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

Зашифровываются биграммы исходного текста следующим образом:

2) Если символы биграммы исходного текста встречаются в одном столбце, то они заменяются символами того же столбца, находящимися непосредственно под ними. Если символ является нижним в столбце, то он заменяется первым символом этого же столбца.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

Зашифровываются биграммы исходного текста следующим образом:

3) Если символы биграммы исходного текста находятся в разных столбцах и разных строках, то они заменяются символами, находящимися в тех же строках, но соответствующими другим углам прямоугольника, образованного этими строками и столбцами.

Блочные шифры

1.1.1. Шифры замены

Полиграммные шифры

Шифр Playfair (Плейфера)

При расшифровывании эти правила используются в обратном порядке, дополнительные символы, если они не входят в состав слов в исходном сообщении, отбрасываются.

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

Пример:

А	У	Т	Е	Н	И
Ф	К	Ц	Я	Б	В
Г	Д	Ё	Ж	З	Й
Л	М	О	П	Р	С
Х	Ч	Ш	Щ	Ъ	Ы
Ь	Э	Ю	-	+	/

Блочные шифры

1.1.1. Шифры замены

Шифры однозначной замены

Шифр Трисемуса (Тритемия)

Пример:

К:	А	У	Т	Е	Н	Т	И	Ф	И	К	А	Ц	И	Я	-	6	х	6
М:	П	Р	О	Г	Р	А	М	М	И	Р	О	В	А	Н	И	Е	-	-
	ПР	ОГ	РА	МЯ	МИ	РО	ВА	НИ	ЕЯ									
С:	РС	ЛЁ	ЛН	ПК	СУ	СП	ФИ	ИА	ЯЖ	-	-	-	-	-	-	-	-	-

Блочные шифры

1.1.1. Шифры замены

Омофонические шифры

Для омофонических шифров количество замен символов исходного сообщения больше, чем один вариант, такие шифры еще называют шифрами многозначной замены.

Блочные шифры

1.1.1. Шифры замены

Омофонические шифры

- При формировании таблицы шифрозамен каждой букве алфавита ставится в соответствие несколько символов, число которых прямо пропорционально частоте встречаемости буквы. Чем чаще используется буква в языке, тем большее число шифрозамен должно быть для нее предусмотрено (рис. 6).
- Ключом шифра является количество символов, из которых состоит каждая шифрозамена.

Блочные шифры

1.1.1. Шифры замены

Омофонические шифры

При зашифровывании буква исходного сообщения заменяется любой шифрозаменой из столбца, соответствующего этой букве. Если буква в исходном сообщении встречается повторно, то она заменяется другой шифрозаменой.

Блочные шифры

1.1.1. Шифры замены Омофонические шифры

№	Пробел	А	Б	В	…	М	…	О	…	Р	…	Я
1	012	311	128	175	…	037	…	248	…	064	…	266
2	042	357	950	194	…	149	…	267	…	189	…	333
…	…	…	…	…	…	…	…	…	…	…	…	…
13	278	495	990	199		349		303		374		749
…	…	…	…	…	…	…	…	…	…	…	…	…
17	342	519		427		760		306		469		845
…	…	…	…	…	…	…	…	…	…	…	…	…
27	437	637		524		777		432		554		
…	…	…	…	…	…	…	…	…	…	…	…	…
38	457	678		644				824		721		
…	…	…	…	…	…	…	…	…	…	…	…	…
42	628	776						828		954		
…	…	…	…	…	…	…	…	…	…	…	…	…
69	681	901						886				
…	…	…	…	…	…	…	…	…	…	…	…	…
94	974							903				
…	…	…	…	…	…	…	…	…	…	…	…	…

Блочные шифры

1.1.1. Шифры замены

Омофонические шифры

Пример:

К:	З				
М:	Б	Р	А	В	О
С:	950	189	357	199	248

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Таблица Трисемуса

Таблица Трисемуса представляет собой матрицу со стороной, равной количеству символов в используемом для шифрования алфавите (для русского языка – 33). В первую строку матрицы записываются буквы в порядке их очередности в алфавите, во вторую – те же буквы, но с циклическим сдвигом на одну позицию влево, в третью – с циклическим сдвигом на две позиции влево и т.д.

Блочные шифры

Шифр Виженера (часть)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Таблица Трисемуса

При шифровании буквы исходного текста располагаются в первой строке матрицы. Первая буква исходного текста шифруется по первой строке матрицы, вторая буква по второй строке матрицы и так далее.

В случае, если количество букв в исходном тексте больше количества строк матрицы, то строки матрицы используются циклически, то есть после последней строки снова используется первая.

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Таблица Трисемуса

Пример:

К:	1	2	3	4	5	6	7	8
М:	К	Л	А	С	Т	Е	Р	Ы
С:	К	М	В	Ф	Ц	К	Ц	В

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Шифр Виженера

В основе шифра лежит таблица Трисемуса.

Ключом является произвольное слово, состоящее из символов используемого алфавита.

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Шифр Виженера

В начале шифрования по первому символу исходного сообщения в первой строке матрицы выбирается столбец, а по первому символу ключа в первом столбце – строка. На пересечении выбранных строки и столбца находится первый символ зашифрованного сообщения.

Следующий символ зашифрованного сообщения определяется на основании второго символа исходного сообщения и ключа и так далее.

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Шифр Виженера

В случае, если длина ключа меньше, чем длина исходного сообщения, то символы ключа используются повторно в том же порядке, как они расположены в ключе.

Блочные шифры

Шифр Виженера (часть)

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л

Блочные шифры

1.1.1. Шифры замены

Полиалфавитные шифры

Шифр Виженера

Пример:

К:	С	И	Г	Н	А	Л	С	И	Г	Н	А
М:	К	О	Д	И	Р	О	В	А	Н	И	Е
С:	Ь	Ч	Ж	Ц	Р	Ъ	У	И	Р	Ц	Е

Блочные шифры

1.1.2. Шифры перестановки

Шифры перестановки так же относятся к блочным шифрам, при шифровании одни блоки заменяются другими (переставляются) в последовательности, определенной алгоритмом.

Различают шифры одинарной (простой) перестановки и шифры множественной (сложной) перестановки.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

При шифровании с использованием шифров одинарной перестановки замена одних символов исходного сообщения на другие происходит один раз.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

Для шифрования используется таблица перестановок, в первую строку которой записываются номера символов исходного сообщения, количество столбцов равно количеству символов исходного сообщения.

Во вторую строку записываются те же номера, что и в первую, но переставленные произвольным образом.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

При шифровании каждый символ исходного сообщения определяется по его номеру в первой строке и переставляется на новое место в соответствии с номером, полученным из второй строки того же столбца.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

Ключом является вторая строка таблицы. Для расшифрования используется та же самая таблица.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
2	4	14	15	1	13	10	7	8	12	5	3	9	6	11

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

К:	2	4	14	15	1	13	7	10	8	12	5	3	9	6	11
М:	М	Н	О	Г	О	З	А	Д	А	Ч	Н	О	С	Т	Ь
С:	Н	Г	Т	Ь	М	С	А	Ч	Д	О	О	О	А	З	Н

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр блочной одинарной перестановки

При использовании данного способа блоком является совокупность определенного количества символов исходного сообщения. Исходное сообщение разбивается на блоки. Если исходное сообщение не кратно размеру блока, тогда оно при шифровании дополняется произвольными, заранее оговоренными, символами.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр блочной одинарной перестановки

Символы в блоке нумеруются, формируется таблица перестановок для блока аналогично таблице для шифра простой одинарной перестановки. Таблица перестановок последовательно применяется ко всем блокам исходного сообщения.

При расшифровывании произвольные символы отбрасываются.

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

1	2	3	4
2	4	1	3

Блочные шифры

1.1.2. Шифры замены

Шифры одинарной перестановки

Шифр простой одинарной перестановки

К:	2	4	1	3	2	4	1	3	2	4	1	3	2	4	1	3
М:	Р	Е	Д	А	К	Т	И	Р	О	В	А	Н	И	Е	-	-
С:	Д	Р	А	Е	И	К	Р	Т	А	О	Н	А	-	И	-	Е