МЕТОДЫ ШИФРОВАНИЯ

Информационная безопасность

Симметричные и асимметричные методы

$$T \xrightarrow{k} T' \xrightarrow{k} T$$

Метод шифрования называется симметричным, если для прямой и обратной процедур используется один и тот же ключ (k).

Метод шифрования называется асимметричным, если ключ, используемый для шифрования текста (p) отличается от ключа (q), используемого для расшифрования текста.

$$T \xrightarrow{p} T' \xrightarrow{q} T$$

Блочные и потоковые шифры

Шифр блочный –
данные шифруются порциями
одинакового размера, называемыми блоками,
и результат зашифрования очередного блока
зависит только от значения этого блока
и от значения ключа шифрования,
и не зависит от расположения блока в
шифруемом массиве и от других блоков массива.

Шифр потоковый –
результат зашифрования очередной порции данных
зависит от самой этой порции и от всех предыдущих
данных шифруемого массива.

Простые шифры

- **Шифр перестановок** – заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр **/P – permutation/**.

- **Шифр замен** – заключается в замене одних значений на другие по индексной таблице, замене подвергаются группы элементов шифруемого блока – битов или символов **/S – substitution/**.

- **Шифр функциональных преобразований** – заключается в выполнении сдвигов, логических и арифметических операций над элементами данных **/F – function/**.

ШИФР ПЕРЕСТАНОВКИ

Понятие шифра перестановки

Шифр перестановок – заключается в перестановках структурных элементов шифруемого блока данных – битов, символов, цифр **/P – permutation/**.

Ключом к шифру простой перестановки является правило перестановки символов в блоке открытого текста.

	на место символа с номером	подставить символ с номером	
1234ABCD5678	1	4	4321DCBA8765
	2	3	
Открытый текст	3	2	Шифртекст
	4	1	

В случае, если размер текста не кратен размеру блока, последний блок текста дополняется справа пробелами.

Шифр простой перестановки

Простейший вариант шифра простой перестановки – поменять соседние буквы местами (размер блока текста – 2 символа).

Открытый текст МАМА МЫЛА РАМУ

Блоки открытого текста МА МА М ЫЛ А РА МУ

Перестановка символов АМ АМ М ЛЫ А АР УМ

Шифртекст АМАММ ЛЫ ААРУМ

Шифр циклической перестановки

Рассмотрим циклическую перестановку символов.

В данном случае размер текста (14 символов)
не кратен размеру блока (3 символа), поэтому
текст дополняется справа пробелами (1 пробел).

Открытый текст | МАМА МЫЛА РАМУ |

Блоки открытого текста | МАМ | А М | ЫЛА | РА | МУ |

Перестановка символов | АММ | МА | ЛАЫ | РА | У М |

Шифртекст | АММ МАЛАЫРА У М |

Стойкость шифра перестановок

Ключ к шифру можно записать в виде последовательности чисел, определяющих порядок перестановки символов в блоке.

Например, для перестановки

ABCD6789 → DCBA9876

ключ можно запомнить как набор чисел k = { 4, 3, 2, 1 }.
При этом размер блока соответствует количеству чисел.

Стойкость шифра перестановок зависит от размера блока текста и определяется количеством возможных перестановок символов в блоке текста размером n символов, что составляет $P_n = n!$

Взлом шифра перестановок

Вне зависимости от размера шифртекста и размера блока,
для подбора ключа достаточно использовать только один блок.

Например, в первом блоке шифртекста (поскольку там есть пробел) могут быть или два полных слова, или одно слово целиком и начало второго слова (а продолжение второго слова – в следующем блоке).

```
йядо дям
ачысм х
тпысн хе
вклаи ,р
д  гаено
ш т уукв
н,маегоз
```

Шифртекст

Количество осмысленных слов,
которые можно составить из этих букв
(дважды используя символы Д и Я),
весьма ограничено и существенно меньше
полного числа ключей 8! = 40 320

йядо дям → мой дядя

Взлом шифра перестановок

Аналогично, так как в последнем блоке
есть запятая, но нет пробела,
то в блоке или отдельное полное слово,
или его окончание, что легко проверить.

`н,маегоз` → `занемог,`

Таким образом, можно
восстановить ключ перестановки
k = { 3, 8, 5, 2, 4, 7, 6, 1}
по одному единственному блоку
(в данном случае – первому
или последнему), а зная ключ –
и весь открытый текст.

```
йядо дям
ачысм х
тпысн хе
вклаи ,р
д  гаено
ш т уукв
н,маегоз
```

Шифртекст

→

```
мой дядя
 самых ч
естных п
равил, к
огда не
в шутку
занемог,
```

Открытый текст

Статистика появления символов

Поскольку в шифртексте меняется только порядок символов, но сами символы используются те же, что и в открытом тексте, то алфавиты открытого текста и шифртекста совпадают.

Кроме того, совпадает частота появления отдельных символов.

```
мой дядя
 самых ч
естных п
равил, к
огда не
в шутку
занемог,
```

Открытый текст

_	9		
н	4	у	2
д	3	х	2
е	3	ы	2
м	3	я	2
н	3	з	1
о	3	и	1
,	2	й	1
в	2	л	1
г	2	п	1
к	2	р	1
с	2	у	1
т	2	ш	1

```
йядо дям
ачысм х
тпысн хе
вклаи ,р
д гаено
ш т уукв
н,маегоз
```

Шифртекст

ШИФР ЗАМЕН

Понятие шифра замен

Шифр замен – заключается в замене одних значений на другие по индексной таблице, замене подвергаются группы элементов шифруемого блока – битов или символов **/S – substitution/**.

Ключом к шифру замен является таблица замен символов (кодовых слов) в блоке открытого текста.

вместо	подставить
1	!
2	@
3	#
4	$
A	%
B	^
C	&
D	*

1234ABCD

Открытый текст

!@#$%^&*

Шифртекст

Шифр Цезаря

Шифр Цезаря является частным случаем шифра простой замены (одноалфавитной подстановки).

Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке.

При шифровании исходного текста каждая буква заменяется другой буквой того же алфавита по следующему правилу:
заменяющая буква определяется путем смещения по алфавиту к концу от исходной буквы на k букв. При достижении конца алфавита выполняется циклический переход к его началу.

Ключом шифра является величина сдвига k.

Пример шифра Цезаря

Шифр Цезаря является частным случаем шифра простой замены.

Пример: Алфавит А = { _, А, Л, М, Р, У, Ы} Ключ $k = 1$

Открытый текст МАМА МЫЛА РАМУ

Таблица замен

_	→	А
А	→	Л
Л	→	М
М	→	Р
Р	→	У
У	→	Ы
Ы	→	_

Шифртекст РЛРЛАР МЛАУЛРЫ

Статистика появления символов

Несмотря на то, что частота появления символов в тексте меняется, тем не менее можно сопоставить частоты разных символов в открытом тексте и шифртексте.

Пример: Алфавит А = { _, А, Л, М, Р, У, Ы} Ключ $k = 1$

Открытый текст МАМА МЫЛА РАМУ

Шифртекст РЛРЛАР МЛАУЛРЫ

Символ открытого текста	Частота	Символ шифртекста
А	4	Л
М	4	Р
_	2	А
Л	1	М
Р	1	У
У	1	Ы
Ы	1	_

Подбор ключа шифра Цезаря

Вне зависимости от размера шифртекста и размера алфавита,
для подбора ключа достаточно подобрать пару
(символ открытого текста) для единственного символа шифртекста,
например, вычислением статистики появления отдельных символов.

На практике частота появления символов в открытом тексте
неизвестна. Однако можно сделать предположение
о содержании и характере открытого текста
(художественный, технический, жаргонный и т.д.),
а также использовать статистику предыдущих сообщений.

Общее количество возможных ключей для шифра Цезаря равно
размеру алфавита открытого текста.