# Лекция по криптографии

# Зачем нужна криптография

Как передать нужную информацию нужному адресату в тайне от других?

1. *Создать абсолютно надежный, недоступный для других канал связи между абонентами.*
2. *Использовать общедоступный канал связи, но скрыть сам факт передачи информации.*
3. *Использовать общедоступный канал связи, но передавать по нему информацию в преобразованном виде, чтобы восстановить ее мог только адресат.*

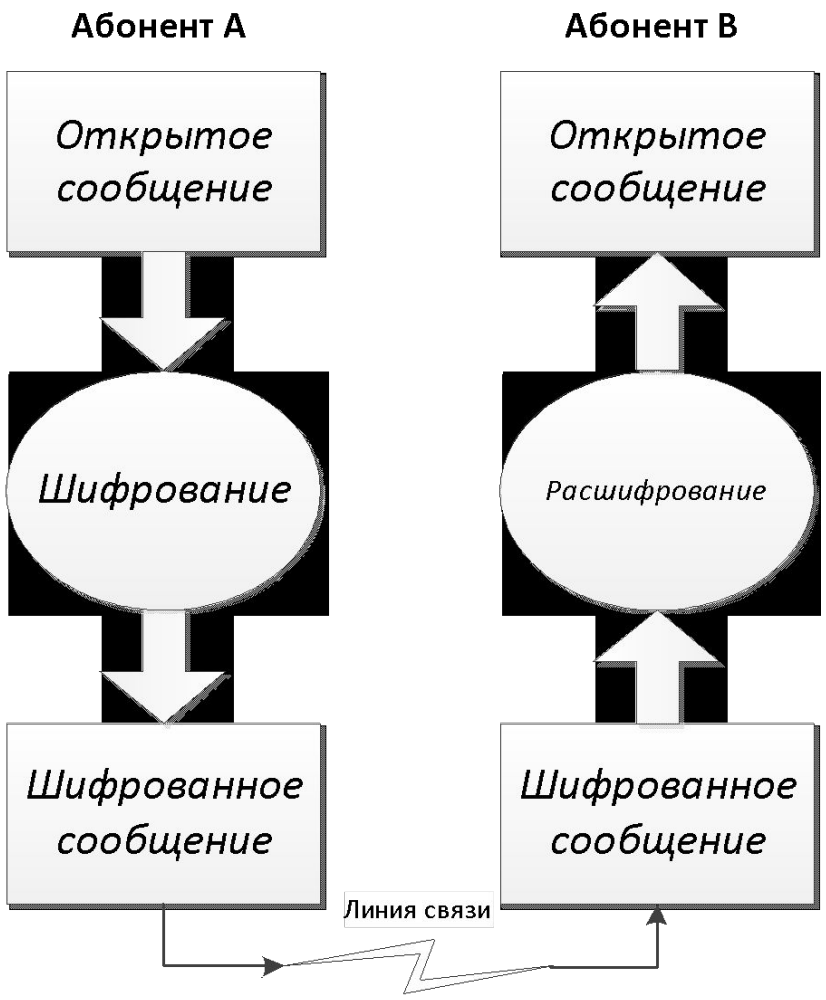
# Что такое криптография

**Криптография** («криптос» - тайна, «графэйн» - писать) - *наука о методах обеспечения*

- *конфиденциальности (невозможности прочтения информации посторонним)*
- *аутентичности (целостности и подлинности авторства, а также невозможности отказа от авторства)*

*информации.*

# Основные термины криптографии



# Основные термины криптографии

Обозначим буквой

- $X$ - открытое сообщение,
- $Y$ - шифрованное сообщение,
- $f$ - правило шифрования,
- $g$ - правило расшифрования.

Тогда зашифрование $X$ в $Y$ можно записать в виде

$$f(X) = Y.$$

Обратное преобразование (то есть получение открытого сообщения $X$ путем расшифрования $Y$) запишется в виде соотношения

$$g(Y) = X.$$

# Основные термины криптографии

Используя понятие *ключа*, процесс зашифрования можно описать в виде соотношения:

$$f_k(X) = Y,$$

в котором $k$ - выбранный ключ, известный отправителю и адресату.

Обратное шифрпреобразование в таком случае запишется так:

$$g_k(Y) = X.$$

# Простейшие шифры

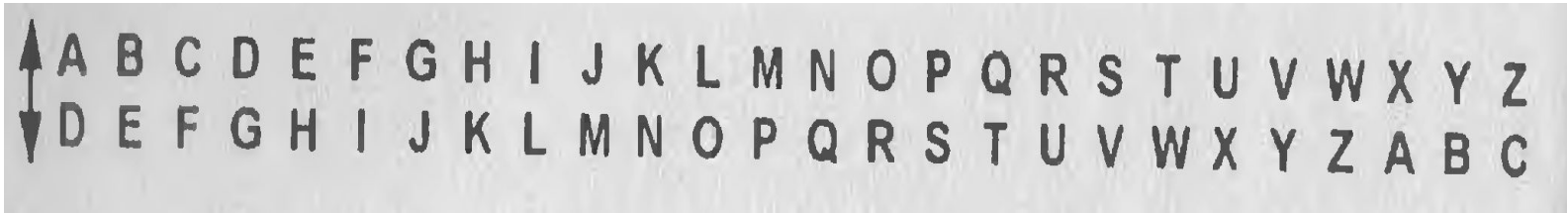

*Шифрами замены* называются такие шифры, преобразования в которых приводят к замене каждого символа открытого сообщения на другие символы - *шифробозначения*, причем порядок следования шифробозначений совпадает с порядком следования соответствующих им символов открытого сообщения.

# Простейшие шифры


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

# Примеры шифров замены

***Шифр Цезаря.*** Заключается в замене букв открытого текста (верхней строки) на буквы (нижней строки) в соответствии с таблицей:




Например, слово CAESAR шифровалось бы как:

FDHVDU

# Примеры шифров замены

Рассмотрим шифр простой замены, соответствующий таблице:

| А | Б | В | Г | Д | Е | Ж | З | И | К | Л | М | Н | О | П | Р | С | Т | У | Ф | Х | Ц | Ч | Ш | Щ | Ы | Ь | Э | Ю | Я |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 11 | 98 | 33 | 42 | 19 | 13 | 87 | 54 | 43 | 49 | 48 | 50 | 69 | 32 | 73 | 18 | 81 | 29 | 76 | 74 | 22 | 31 | 90 | 59 | 67 | 77 | 91 | 12 | 52 | 45 |

В этом случае, например слово «ПОБЕДА» перейдет в:

73 32 98 13 19 11

Такой шифр называется шифром *цифровой простой замены*.

# Примеры шифров замены

- А. Конан Дойл «Пляшущие человечки»

- Ж. Верн «Путешествие к центру Земли»

# Примеры шифров замены

***Шифр Полибия.***

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

Например, при шифровании слова «Греция» получим следующую криптограмму:

52 12 35 54 34 33

# Понятие шифра перестановки

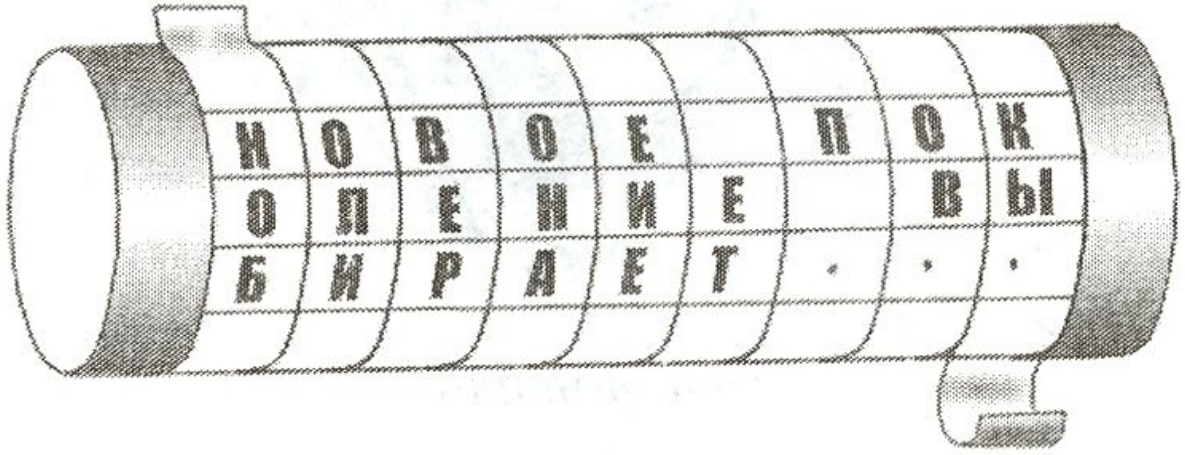
Таблица шифра перестановки для текста длины $n$:

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

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.

# Примеры шифров перестановки

***Шифр сцитало***.




Ключом данного шифра являлся диаметр палки (сциталы).

# Примеры шифров перестановки

***Шифр маршрутной перестановки.***
Зашифруем, например, фразу:

ПРИМЕРМАРШРУТНОЙПЕРЕСТАНОВКИ

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

# Задача № 1

Имеется криптограмма

HFPSHJB

Найдите исходное сообщение, если известно, что шифрпреобразование заключалось в следующем. Пусть $x_1, x_2$ - корни трехчлена $x^2 + 5x + 4$. К порядковому номеру каждой буквы в английском алфавите прибавлялось значение многочлена

$$f(x) = x^6 + 5x^5 + 4x^4 + x^3 + 6x^2 + 9x + 5$$

вычисленное либо при $x = x_1$, либо при $x = x_2$ (в неизвестном порядке), а затем полученное число заменялось соответствующей ему буквой.

**Ответ:** GEORGIA

**Решение:**

Для данного многочлена верно разложение:

$$f(x) = (x^2 + 5x + 4)(x^4 + x + 1) + 1.$$

Поэтому, и при $x = x_1$, и при $x = x_2$ значение $f(x) = 1$. Если теперь шифрованное сообщение представить в виде цифровом виде, получим

8 6 16 19 8 10 2

Отнимем от каждого значение 1, получим:

7 5 15 18 7 9 1,

приводим обратно к буквенному виду, получаем:

GEORGIA

# Задача № 2

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:

**ВАБОЛВЕЫЕКЬТСРТЙЕ**.

Что это было за сообщение?

| 1 | 2 | 3 | 4 | 5 | 6 | 7 |
|---|---|---|---|---|---|---|
| | | | | | | |
| | | | | | | |
| | | | | | | |

Определим разбивку текста на столбцы:

**ВА БОЛ ВЕ ЫЕК ЬТ СР ТЙЕ.**

Впишем в соответствии с этим в таблицу:

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

# Спасибо за внимание!