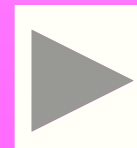
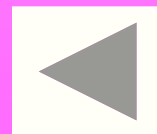


Способы шифрования

Завершить

Содержание

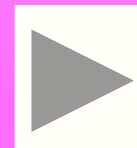
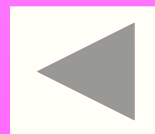
- 1. [Основы криптографии](#)
- 2. [Первый шифр](#)
- 3. [Требования к шифру](#)
- 4. [Классы шифров](#)
- 5. [Квадрат Полибия](#)
- 6. [Шифр Цезаря](#)
- 7. [Шифр Виженера](#)
- 8. [Шифр аббата Тритемиуса](#)
- 9. [Тарабарская грамота](#)
- 10. [Транс позиция](#)
- 11. [Решето Кардано](#)



Основы криптографии

- Криптография – тайнопись.
- Данный термин ввел помощник Кромвеля, который вел его переписку.

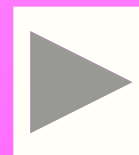
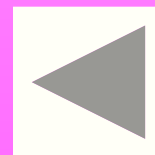
К содержанию



Первый шифр

- Первым шифром был скитала V, VI век до н.э.

К содержанию



скитала

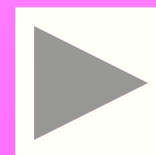
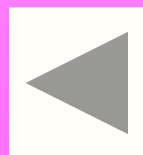
- Устройство: 2 палки одинакового диаметра. Одна палка передается абоненту. Он наматывает папирус на палку и вертикально пишет текст. Потом отправляет папирус.
- Что бы расшифровать необходимо намотать папирус на палку того же диаметра и прочитатъ.

Назад

Требования к шифру

- 1. Однозначность (каждому символу соответствует только 1 символ или комбинация)
- 2. Трудноразгадываемость
- 3. Целесообразность трудности.

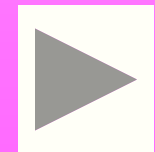
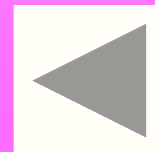
К содержанию



Классы шифров

- Существует 2 класса шифров:
- 1. «Подстановка»
 - шифр простой замены
- 2. «Перестановки»
 - шифр, в котором переставляются СИМВОЛЫ

К содержанию



Квадрат Полибия

- Древняя Греция, II век до н. э.
- Смысл заключается в том, что составляется [Таблица Полибия](#). Шифрование происходит следующим способом: буква шифруется координатами, то есть (номер строки, номер столбца).
- Например: А = 11, О = 34

К содержанию

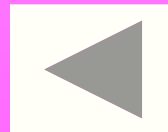


Таблица Полибия

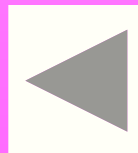
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Назад

Шифр Цезаря

- Древний Рим, I век до н. э.
- Использование сдвига алфавита на 4 символа
- Август, живший в то же время, использовал сдвиг на 2 буквы.

К содержанию



Шифр Виженера

- Для шифрования использовал:
- Ключ;
- [Таблицу Виженера](#).
- Например:
- Ключ: гадание.
- Зашифровать надо слово «дева».
- В итоге получится слово «зежа»

К содержанию

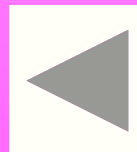


Таблица Виженера

- Алгоритм шифрования:
- «Д» - определяет столбец
- «Г» - определяет строку
- На пересечении строки и столбца находится закодированная буква. В данном случае «З»

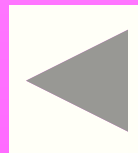
А	Б	В	Г	Д	Е	Ж	З
Б	В	Г	Д	Е	Ж	З	И
В	Г	Д	Е	Ж	З	И	К
Г	Д	Е	Ж	З	И	К	Л
Д	Е	Ж	З	И	К	Л	М

Назад

Шифр аббата Тритемиуса

- Способ шифрования: пронумеровать буквы алфавита по порядку.
- Выбрать слово-ключ.
- Написать кодируемое слово, под ним слово-ключ, и сложить цифры, соответствующие буквам в словах.
- Последовательность цифр и будет зашифрованным сообщением.
- Пример

К содержанию



Пример

- Ключ: гадание
- Слово: дева

д	е	в	а				
5	6	3	1				
г	а	д	а	н	и	е	
4	1	5	1				
и	ж	з	б				
9	7	8	2				

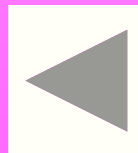
1	2	3	4	5	6	7	8
А	Б	В	Г	Д	Е	Ж	З

Назад

Тарабарская грамота

- Один из первых русских способов шифрования информации.
- Сущность: сопоставляются согласные буквы.
- При шифровании согласные меняются, а гласные остаются теми же.
- Пример

К содержанию



Пример

- Зашифруем слово «шифр».
- Получится слово «ВИЗМ»

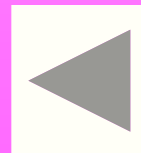
Б	В	Г	Д	Ж	З	К	Л	М	Н
Щ	Ш	Ч	Ц	Х	Ф	Т	С	Р	П

Назад

Транспозиция

- Тип шифра: по столбцам, по ключу.
- Выбирается слово-ключ, в нем нумеруются буквы по алфавиту, под ключом записывается шифруемая фраза.
- Шифровка пишется по номерам столбцов.
- Пример

К содержанию



Пример

- Слово-ключ: телега
- Фраза: «Рыба с головы гниет»
- Шифровка имеет вид:
- «ГГБС ЫАЫЛ ИАВТ
БОР ОН»

Т	Е	Л	Е	Г	А
6	3	5	4	2	1

6	3	5	4	2	1
Р	Ы	Б	А	С	Г
О	Л	О	В	Ы	Г
Н	И	Е	Т	А	Б

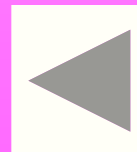
Назад

Решето Кардано

- Это таблица (решетка) $2n$ на $2n$ с четным количеством строк и столбцов.
- Алгоритм: берем трафарет, накладываем на такую же таблицу на бумаге и записываем сообщение. Поворачиваем на 90 градусов и записываем итак далее.
- Если не хватает фразы идет перечисление алфавита.
- [Требования к решетке](#)
- [Пример](#)

К содержанию

Завершить



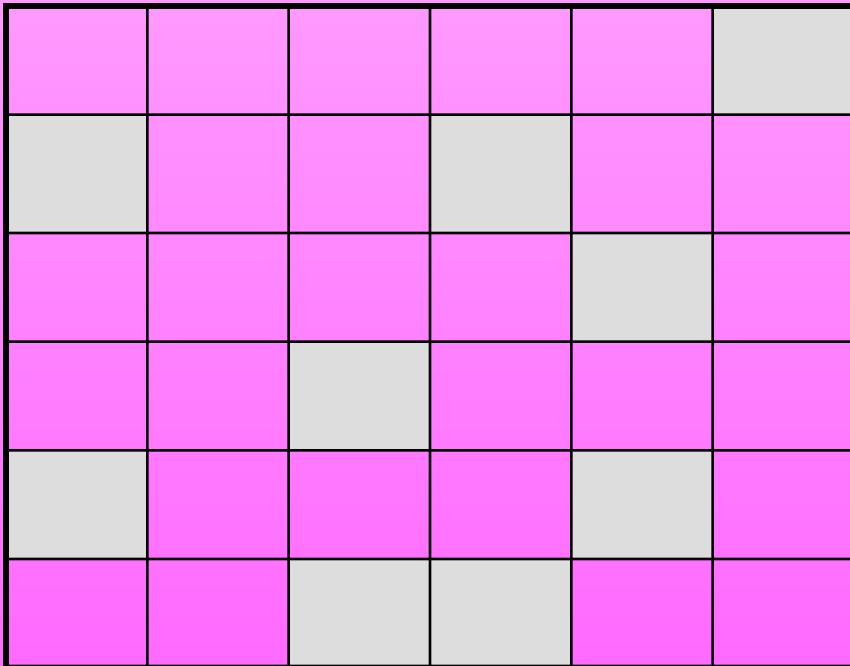
Требования к решетке

- 1. Ни одна дырочка не должна попасть на клетку дважды;
- 2. Ни одна клетка не должна остаться пустой.

Назад

Пример

- Фраза «У лукоморья дуб зеленый златая цепь на дубе»
- Поворот на 90 градусов в право



У	Ы	Е	П	Й	Я
Д	Ь	Л	У	У	Н
З	К	Л	А	Б	О
А	Д	З	М	Т	О
Е	А	У	Я	Л	Б
Е	Р	Е	Н	Ь	Ц

Назад