

# ИЗ ИСТОРИИ КРИПТОГРАФИИ И ШИФРОВАНИЯ. ШИФР «ПЕРЕКРЁСТОК»

**Сосновский район Нижегородской области  
Филиал МБОУ Сосновская СШ № 1 «Рожковская ОШ»  
Учитель информатики – Лобанов С. В.  
2018/2019 учебный год**

---

# ШИФРОВАНИЕ И КРИПТОГРАФИЯ

- История криптографии** насчитывает около 4 тысяч лет. В качестве основного критерия периодизации криптографии возможно использовать технологические характеристики используемых методов шифрования.
- Первый период (приблизительно с 3-го тысячелетия до н. э.) характеризуется господством моноалфавитных шифров (основной принцип — замена алфавита исходного текста другим алфавитом через замену букв другими буквами или символами).
  - Второй период (хронологические рамки — с IX века на Ближнем Востоке (Ал-Кинди) и с XV века в Европе (Леон Баттиста Альберти) — до начала XX века) ознаменовался введением в обиход полиалфавитных шифров.

# ШИФРОВАНИЕ И КРИПТОГРАФИЯ

- Третий период (с начала и до середины XX века) характеризуется внедрением электромеханических устройств в работу шифровальщиков. При этом продолжалось использование полиалфавитных шифров.
- Четвёртый период — с середины до 70-х годов XX века — период перехода к математической криптографии. В работе Шеннона появляются строгие математические определения количества информации, передачи данных, энтропии, функций шифрования. Обязательным этапом создания шифра считается изучение его уязвимости к различным известным атакам — линейному и дифференциальному криптоанализу. Однако до 1975 года криптография оставалась «классической» или же, более корректно, криптографией с секретным ключом.

- 
- Современный период развития криптографии (с конца 1970-х годов по настоящее время) отличается зарождением и развитием нового направления — криптография с открытым ключом. Её появление знаменуется не только новыми техническими возможностями, но и сравнительно широким распространением криптографии для использования частными лицами. Правовое регулирование использования криптографии частными лицами в разных странах сильно различается — от разрешения до полного запрета.

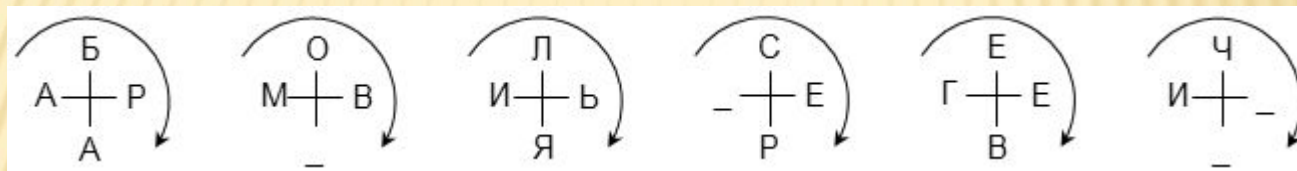
# ШИФР «ПЕРЕКРЁСТОК»

---

Для перемешивания букв могут использоваться фигуры специального вида. Один из таких способов носит название «перекресток». Открытый текст записывают вокруг фигур заранее оговоренным способом - в нашем случае по часовой стрелке

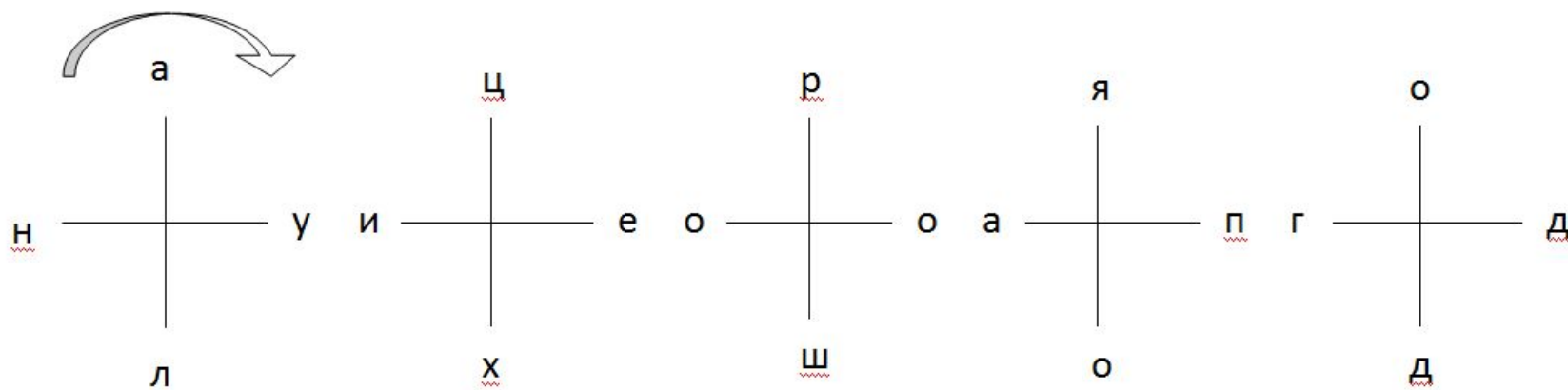
# ПРИМЕРЫ ШИФРА

Таким образом, сообщение «АБРАМОВ ИЛЬЯ СЕРГЕЕВИЧ» может выглядеть следующим образом:



Буквы берутся построчно. Вначале берется оговоренное количество букв ( $N$ ) из первой строки, затем удвоенное количество букв ( $2N$ ) из второй и снова  $N$  букв из третьей строки. Например, при  $N = 3$  шифрограмма будет выглядеть «БОЛАРМВИЪА\_ЯСЕЧ\_ЕГЕИ\_РВ\_».

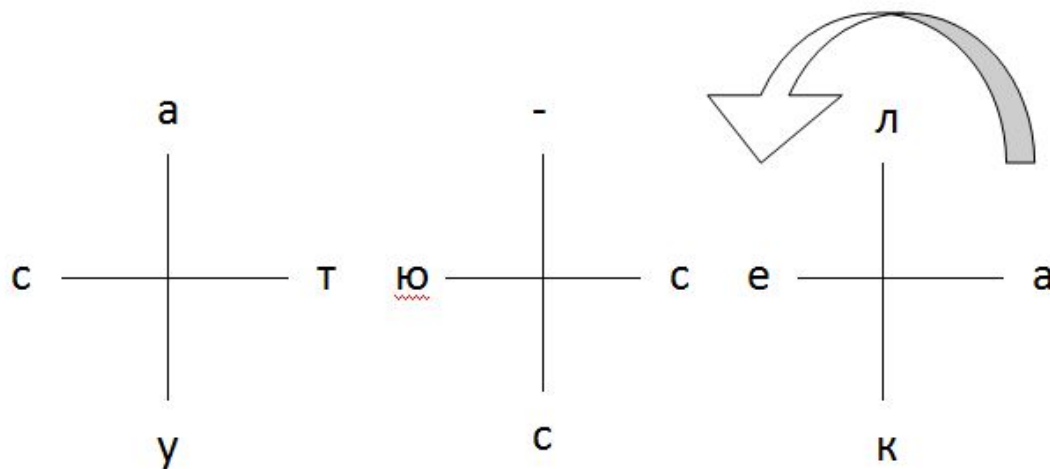
# ЕЩЁ ПРИМЕР – НА УЛИЦЕ ХОРОШАЯ ПОГОДА



N=4

Получаем - АЦРЯНУИЕООАПЛХШООГДА|

# АЛЕКС - ЮСТАСУ

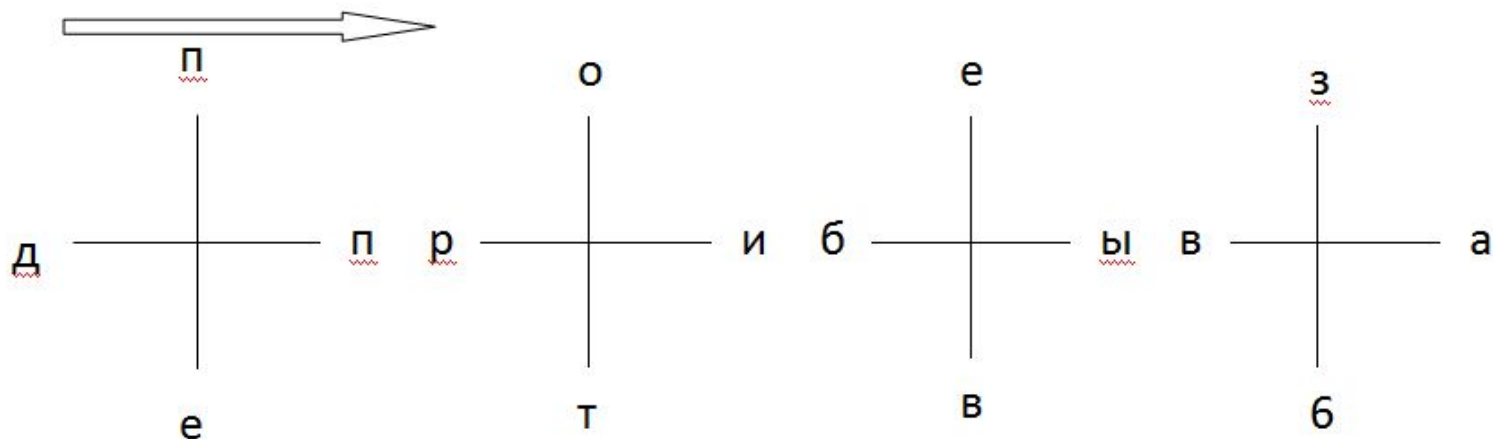


N=2, слева направо

Получаем – А-СТЮСУСЛЕАК|



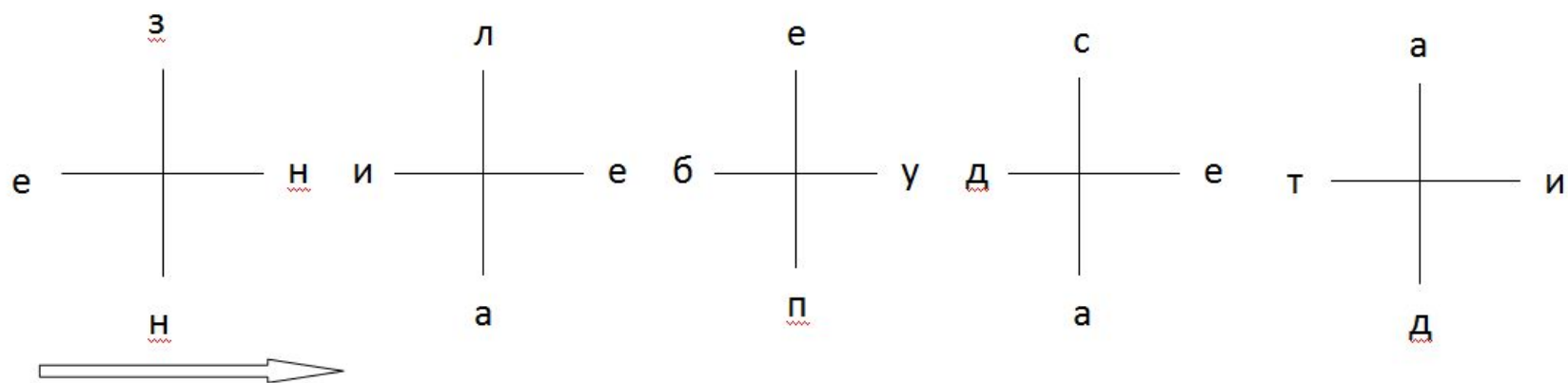
# ПОЕЗД ПРИБЫВАЕТ В 6.



Кодируем по часовой стрелке

Получаем: дппероитбевывзаб

# НАПАДЕНИЕ БУДЕТ ИЗ ЛЕСА



Кодируем против часовой стрелке слева направо

Получаем: иатдесдауебпелианзен