Интуитивная криптография

(до начала XVI века)

Базовая модель классической криптосистемы

Угрозы в фокусе темы

Шифр «Сцитала» (Scytale) (Спарта V век до н.э.)

- **Открытый текст:**

ПРИМЕРШИФРАСЦИТАЛА

П	Р	И	М	Е	Р
Ш	И	Ф	Р	А	С
Ц	И	Т	А	Л	А

- **Шифротекст:**

ПШЦРИИИФТМРАЕАЛРСА

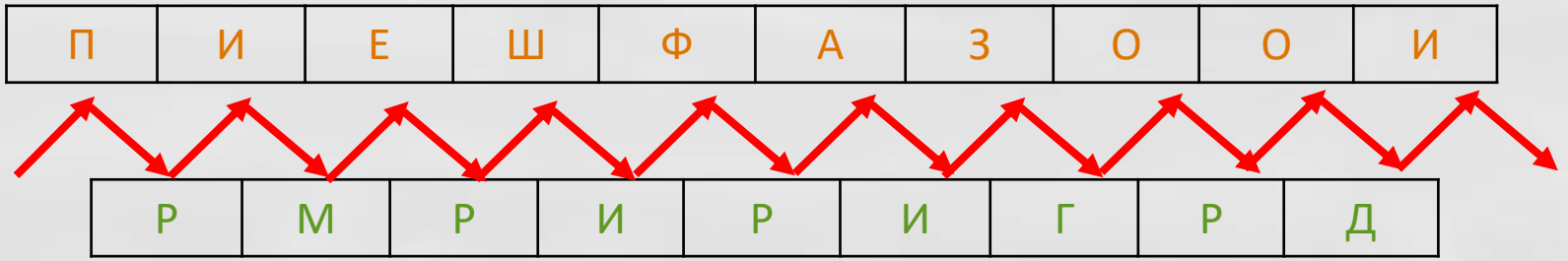
Пример атаки

- Ключом шифра является диаметр цилиндра, который предположительно не может превосходить 10 сантиметров. При высоте строки в 1 сантиметр на одном витке такого жезла уместится не более 32 букв $10\pi < 32$. Таким образом, число перебираемых вариантов вряд ли превосходит 32.
- Методика взлома (Аристотель): на длинный конус наматывалась лента, а затем эту ленту начинали сдвигать по конусу. Там, где буквы текста формировали слова или слоги, диаметр конуса совпадал с диаметром цилиндра.
- Это пример атаки методом **«грубой силы»** (*brute force*) – полный перебор ключей (секретов) шифра при известном алгоритме зашифровки. Чтобы предотвратить этот тип атаки, число возможных ключей должно быть очень большим

Шифр изгороди (rail fence)

- **Открытый текст:**

ПРИМЕРШИФРАИЗГОРОДИ



- **Шифротекст:**

ПИЕШФАЗООИРМРИРИГРД

Шифр Атбаш (Atbash), моноалфавитная замена (substitution) (1 век н.э.)

- **Открытый текст:**

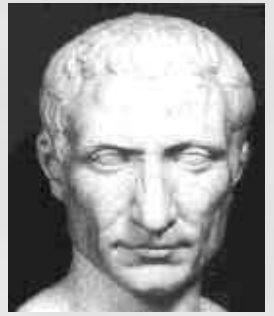
ПРИМЕРШИФРААТБАШ

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

- **Шифротекст:**

СРЧФЪРЗЧМРЯЯОЮЯЗ

Шифр Цезаря (1 век до н.э.)



- **Открытый текст:**

ПРИМЕРШИФРАЦЕЗАРЯ

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

- **Шифротекст:**

Т

ROT13

Еще совсем недавно (в 1980-х годах) применялся метод шифрования ROT13, в котором использовался сдвиг алфавита на 13 букв вместо трех. Этот шифр использовался в различных онлайновых форумах для публикации запрещенной информации, для ее распространения среди пользователей.

Криптоанализ

- Шифры «Изгородь», «Атбаш», «Цезаря» основаны на знании алгоритма
- Это примеры бесключевых шифров
- Взлом подобных шифров не являются предметом криптоанализа