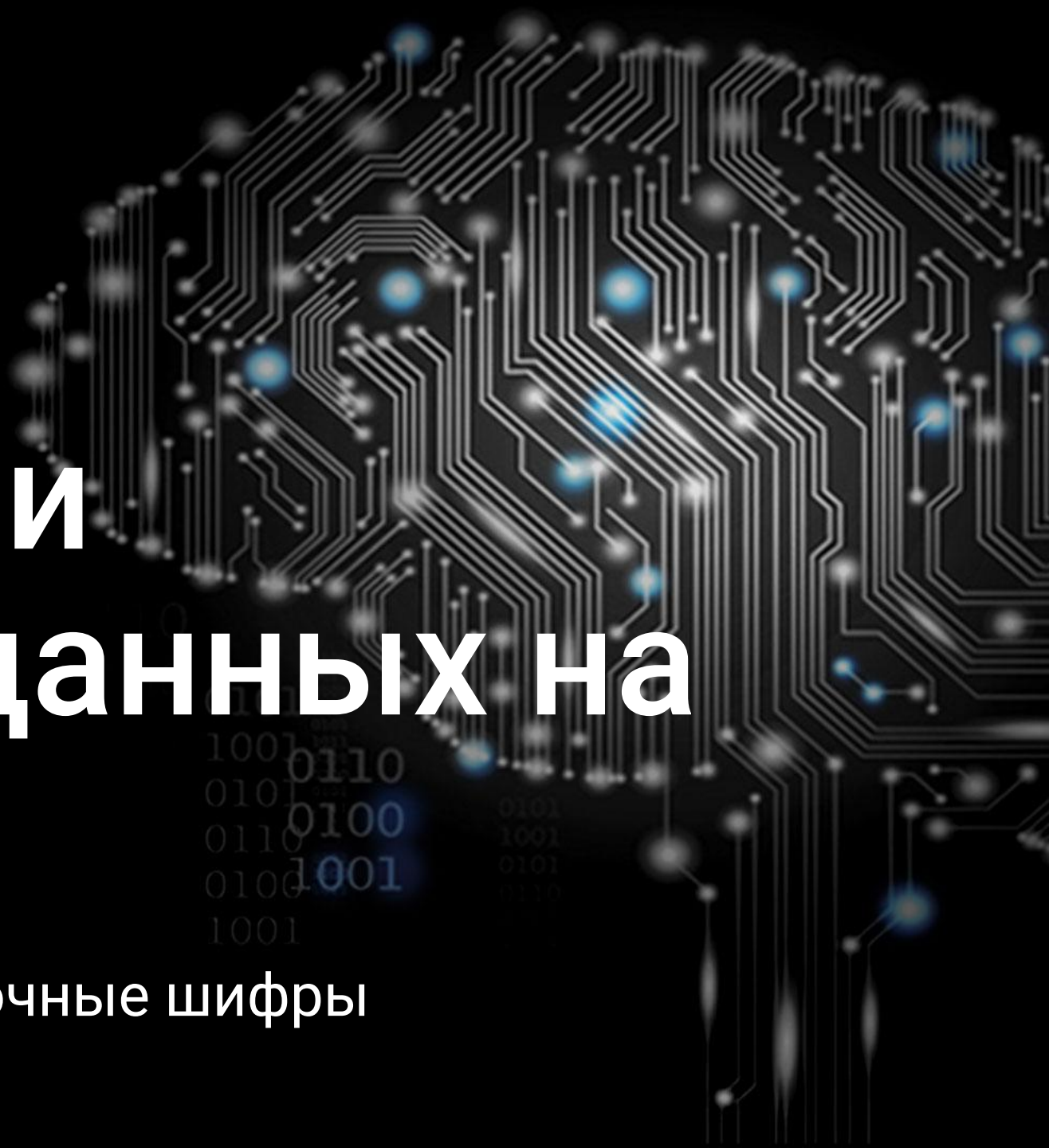
GeekBrains



Алгоритмы и структуры данных на языке C

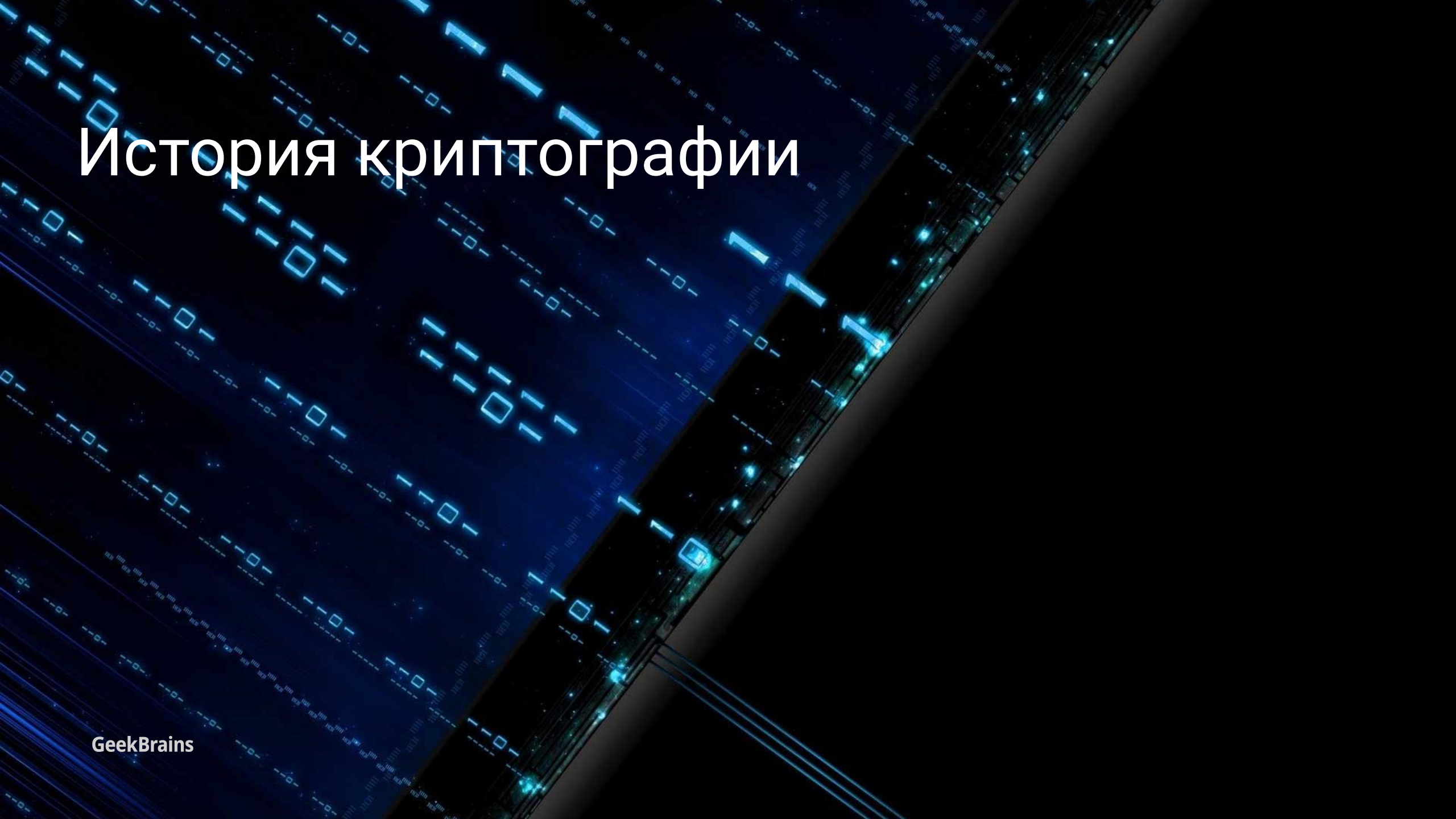
Краткая история. Перестановочные шифры

Краткая история. Перестановочные шифры

В этом видео

1. История криптографии
2. Перестановочный шифр и его расшифровка
3. Взлом перестановочного шифра
4. Маршрутный шифр

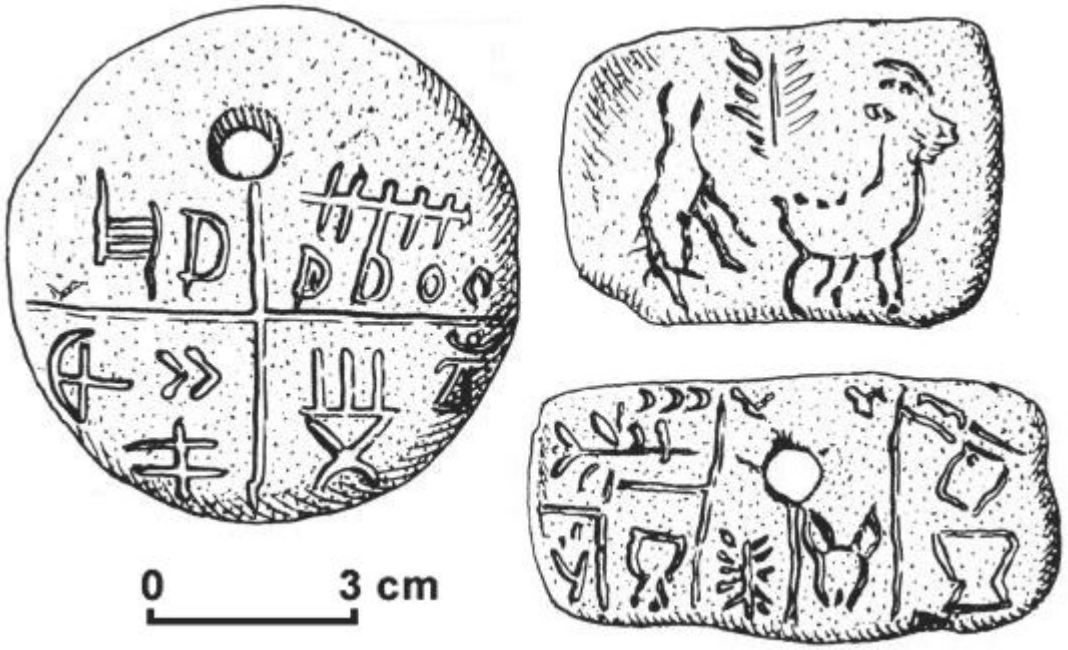
История криптографии



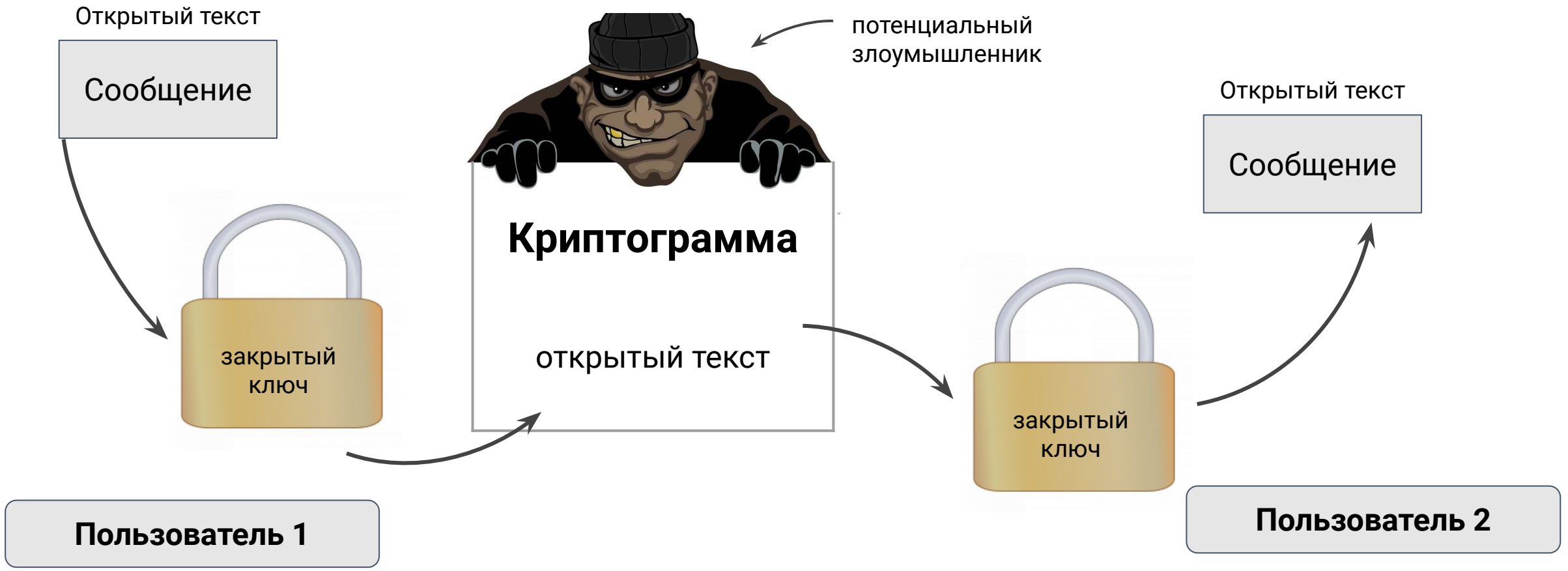
GeekBrains

Классические методы

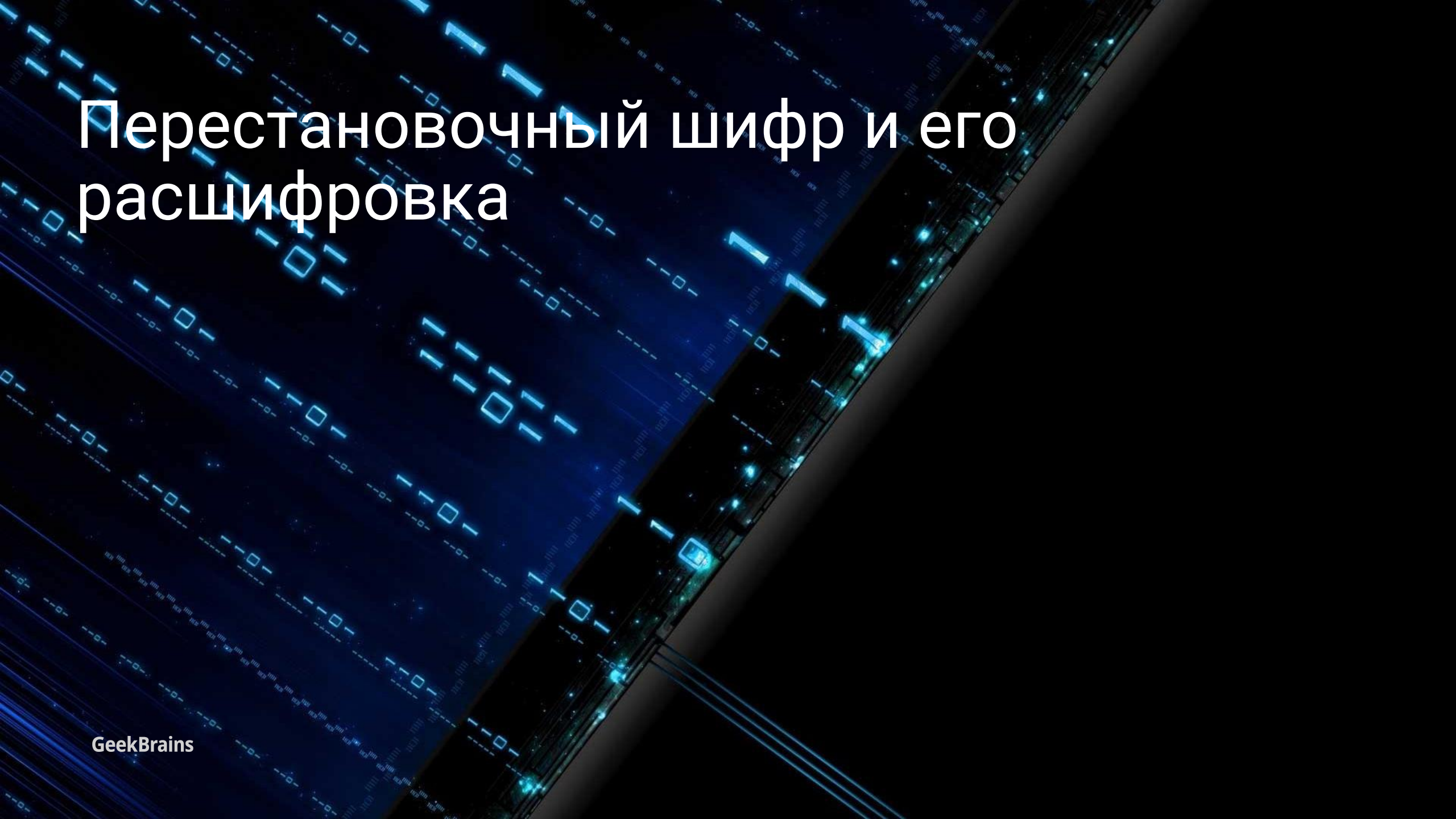
security through obscurity



Новые методы шифрования и криптоанализ

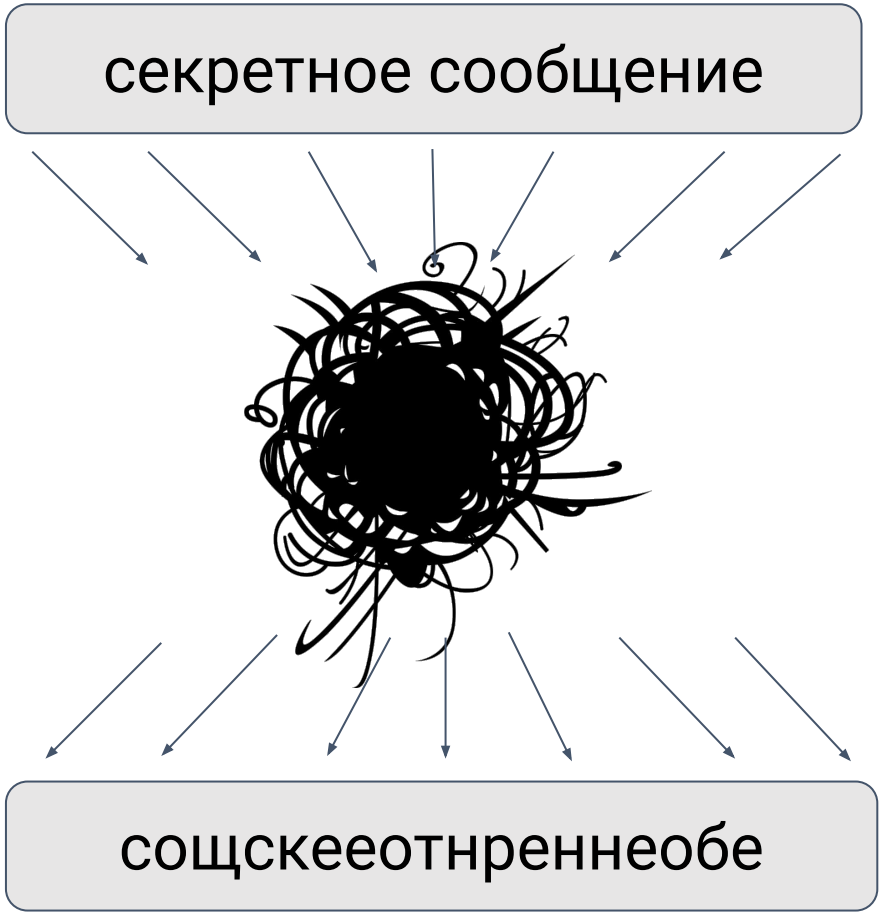


Перестановочный шифр и его расшифровка



GeekBrains

Перестановочные шифры



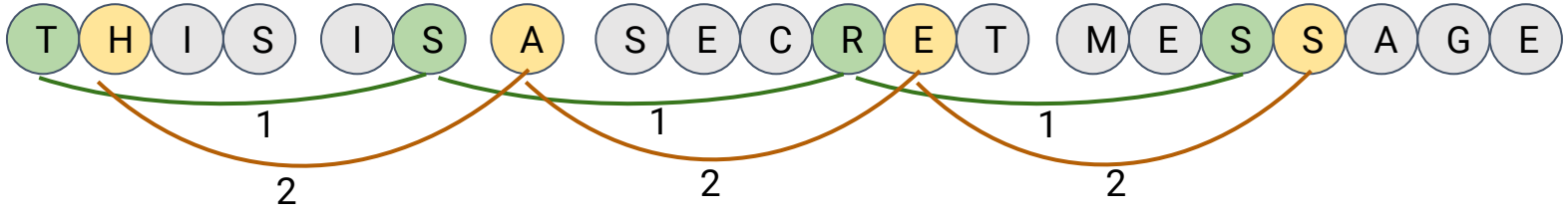
Перестановка строк/столбцов

THIS IS A SECRET MESSAGE

T	H	I	S	I
S	A	S	E	C
R	E	T	M	E
S	S	A	G	E

TSRS	HAES	ISTA	SEMG	ICEE

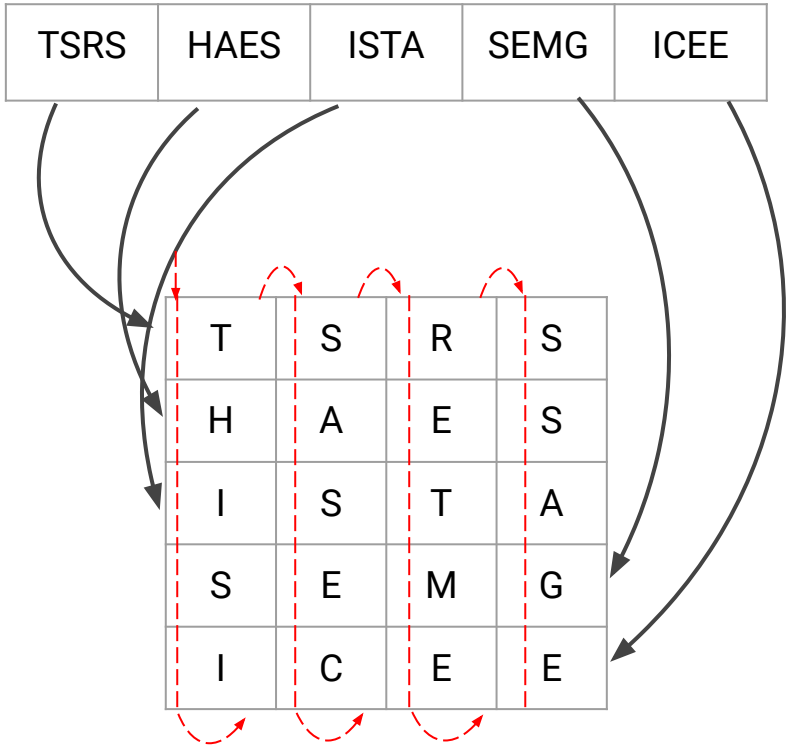
KEY = 4



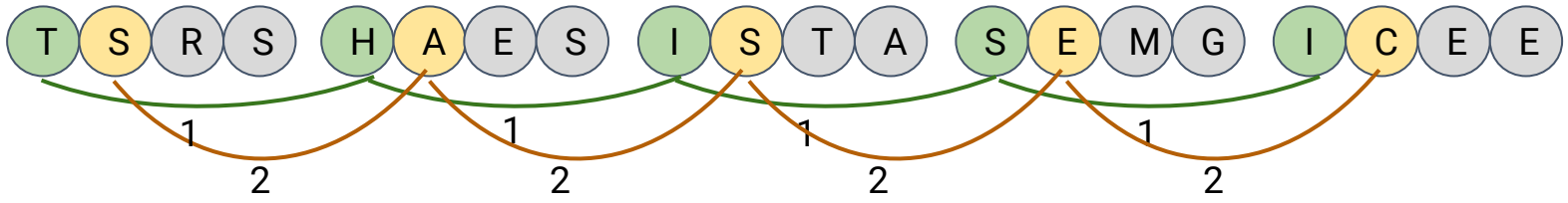
КЛЮЧ = 4 = (N пропускаемых при чтении входящей строки символов)

ШИФРОВАНИЕ → запись в R строк и C столбцов

РАСШИФРОВКА → запись в C строк и R столбцов



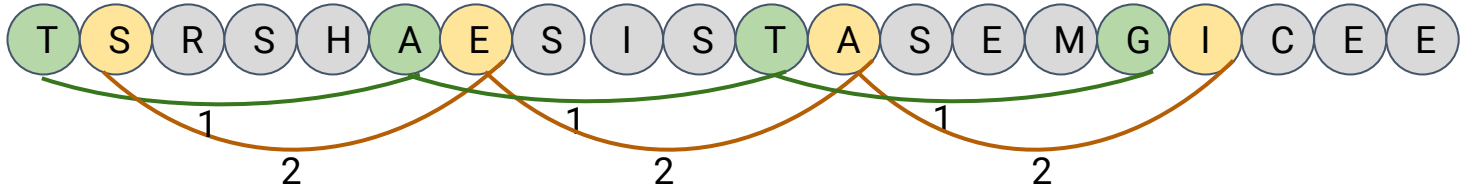
KEY = 4



THISISASECRETMESSAGE

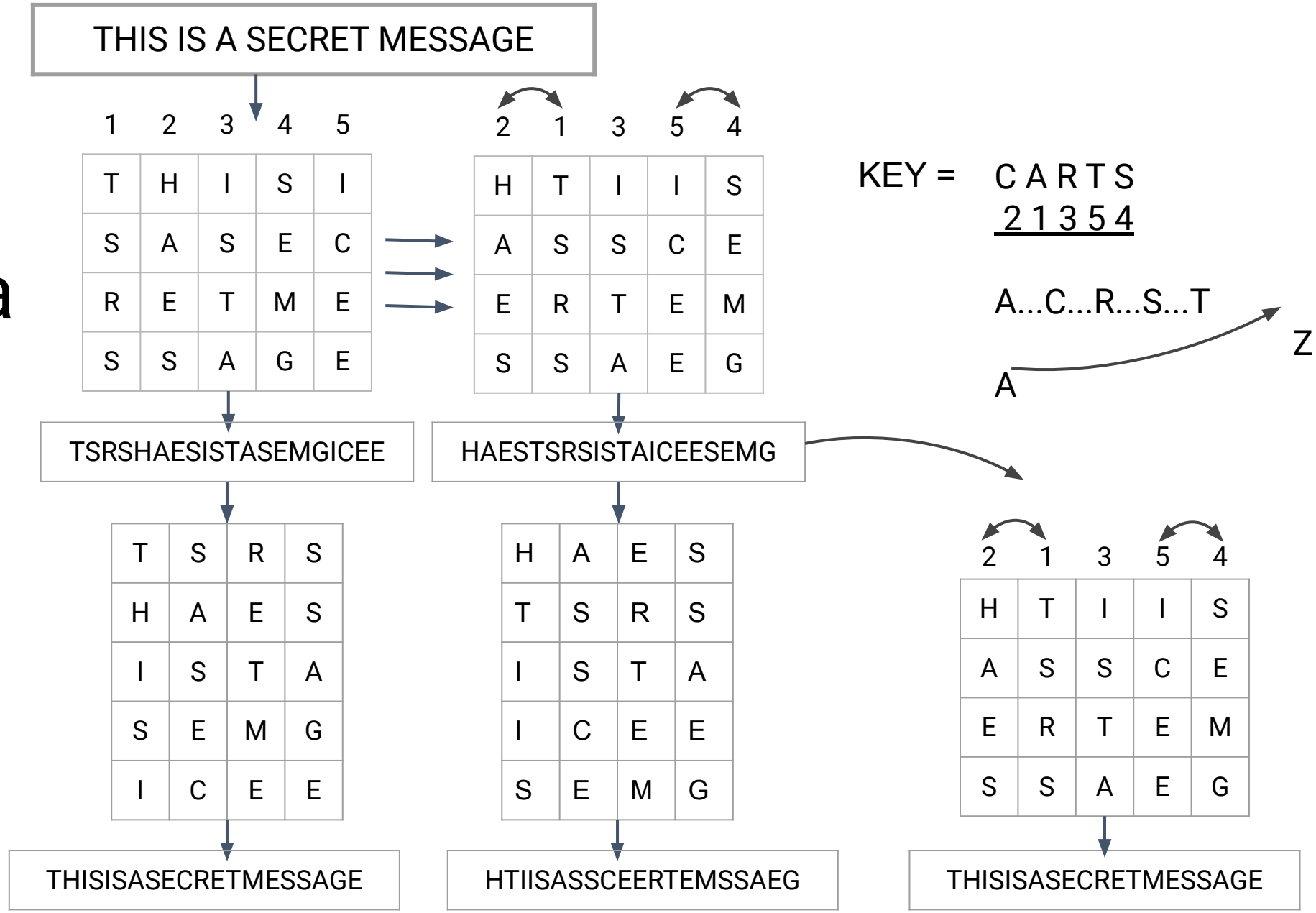
T	S	R	S	H
A	E	S	I	S
T	A	S	E	M
G	I	C	E	E

KEY = 5



TATGSEAIRSSCSIEEHSME

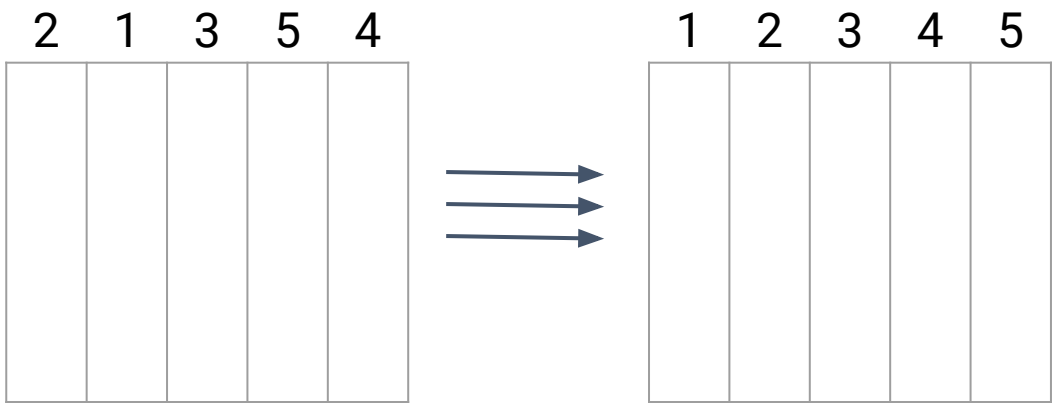
Перестановка столбцов



Расшифровка сообщения с перестановкой столбцов

CARTS → A...C...R...S...T

21354 → 1...2...3...4...5

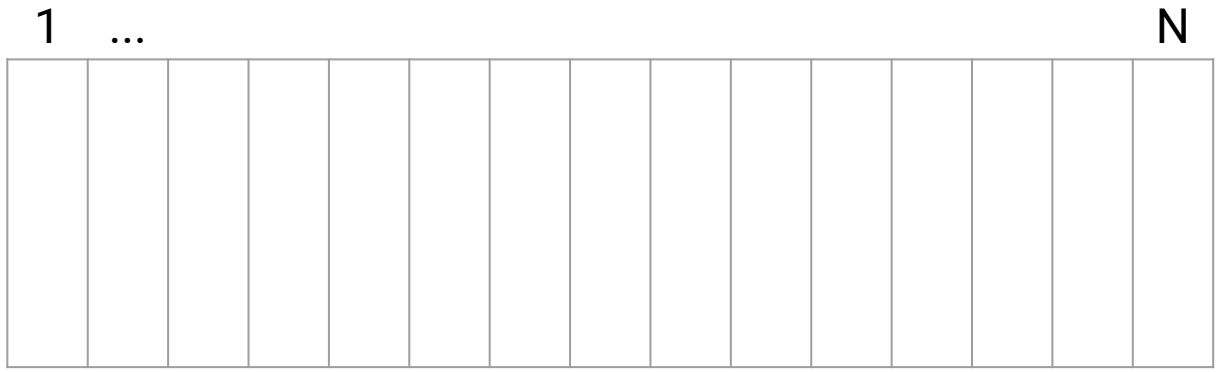



```
int mapping[2] = 1
int inverse_mapping[1] = 2
```

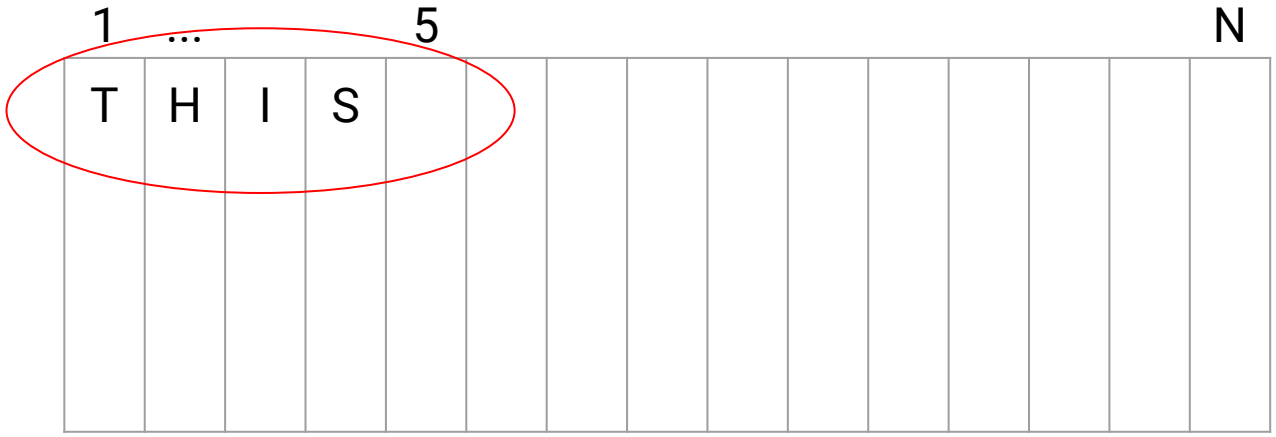
Взлом перестановочного шифра

GeekBrains

Взлом перестановочного шифра



Для 10 столбцов
3 628 800 вариантов



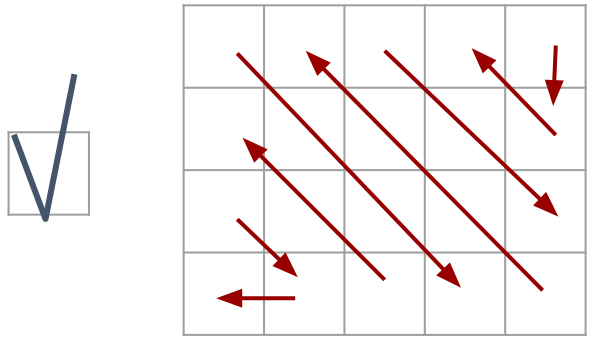
Для 10 столбцов
зная 5 столбцов
30 240 вариантов

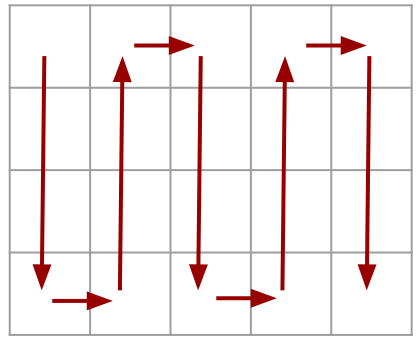
Маршрутный шифр

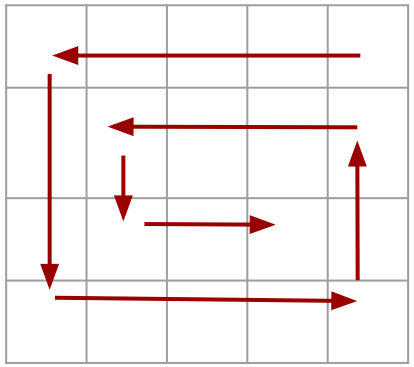
Маршрутный шифр

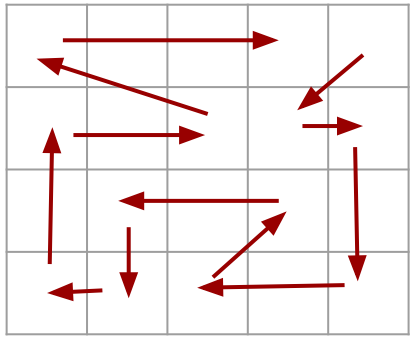
THIS IS A SECRET MESSAGE

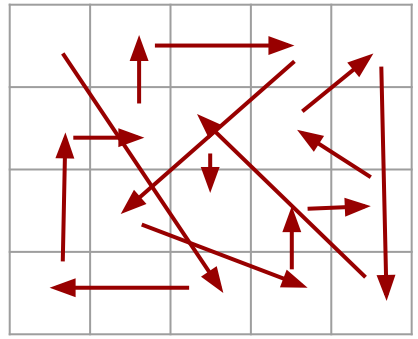
T	I	E	T	S
H	S	C	M	A
I	A	R	E	G
S	S	E	S	E











Итоги

Рассмотрели:

- История криптографии
- Перестановочный шифр и его расшифровка
- Взлом перестановочного шифра
- Маршрутный шифр