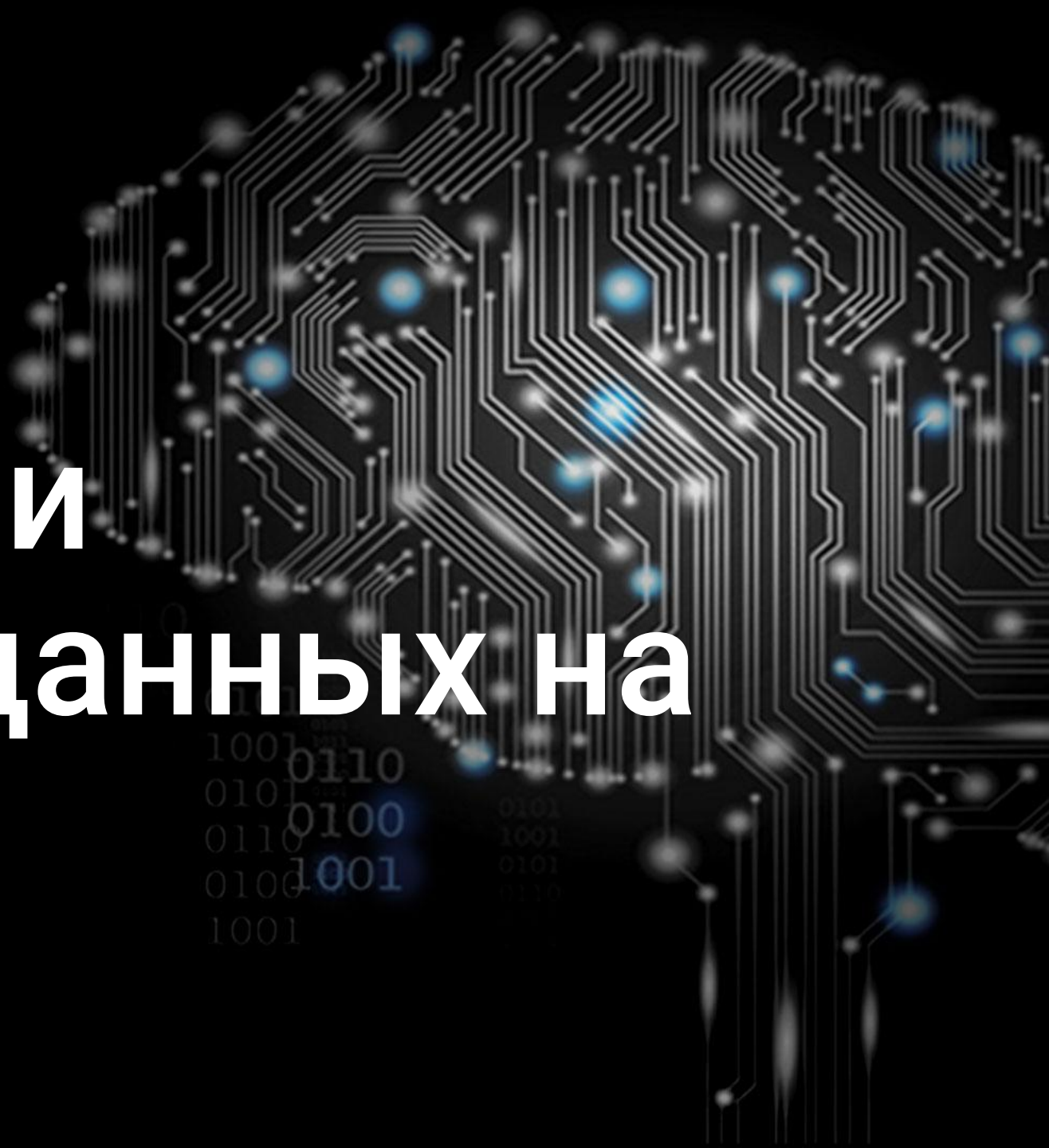
GeekBrains



Алгоритмы и структуры данных на языке C

Шифры подстановки

GeekBrains

Шифры подстановки

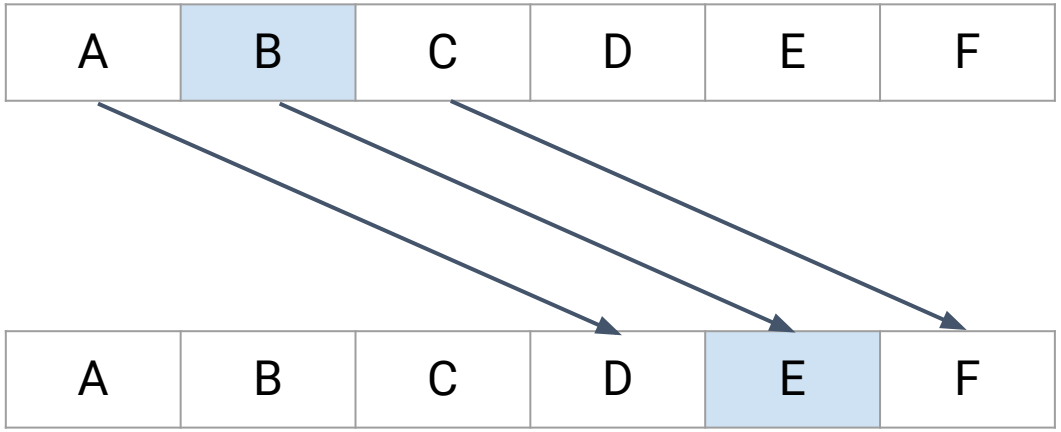
В этом видео

1. Шифр Цезаря
2. Шифр Виженера
3. Простой подстановочный шифр
4. Одноразовый блокнот

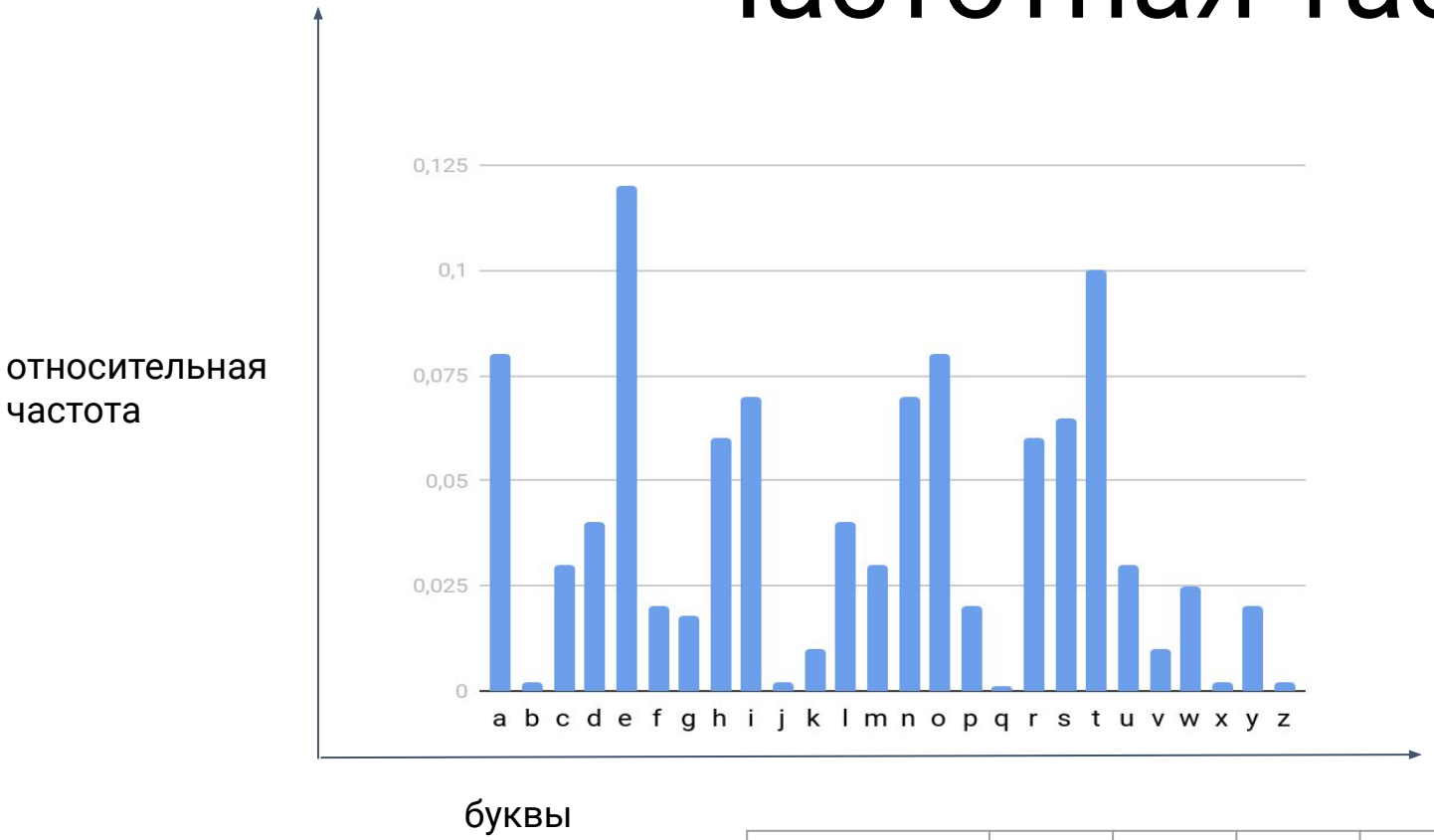
Шифр Цезаря

Шифр Цезаря

Вид шифра подстановки, в котором каждый символ в открытом тексте заменяется символом, находящимся на некотором постоянном числе позиций левее или правее него в алфавите.



Частотная таблица



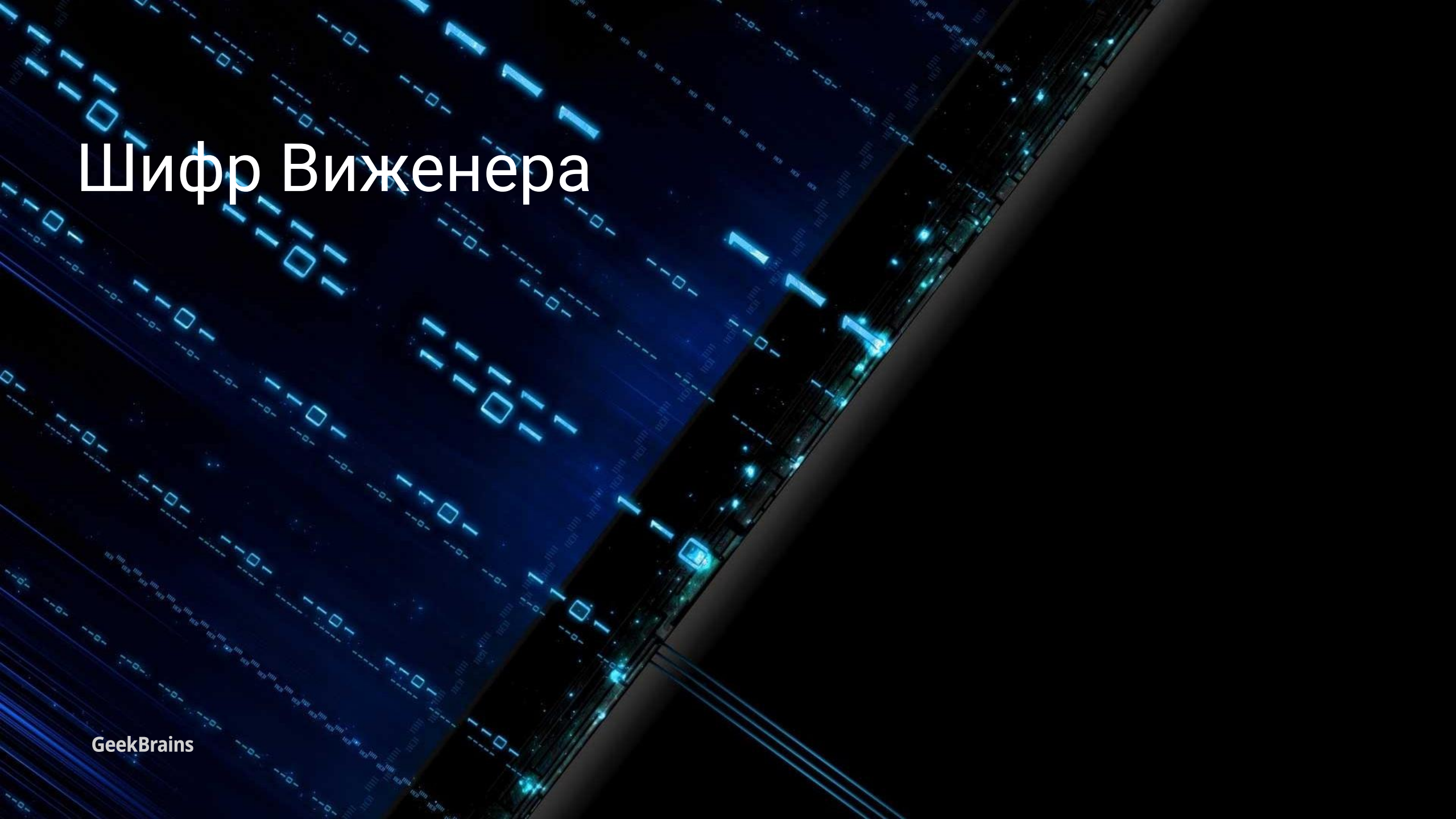
THIS IS A SECRET MESSAGE

WKLVL VDVHF UHWPH VVDJH

Частотная таблица для маленьких сообщений может отличаться

Буква	D	F	H	J	K	L	P	U	V	W
Число вхождений	2	1	4	1	1	2	1	1	5	2

Шифр Виженера



GeekBrains

Шифр Виженера

Метод полиалфавитного шифрования буквенного текста с использованием ключевого слова.

Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E	B	R	A	S	Z	E

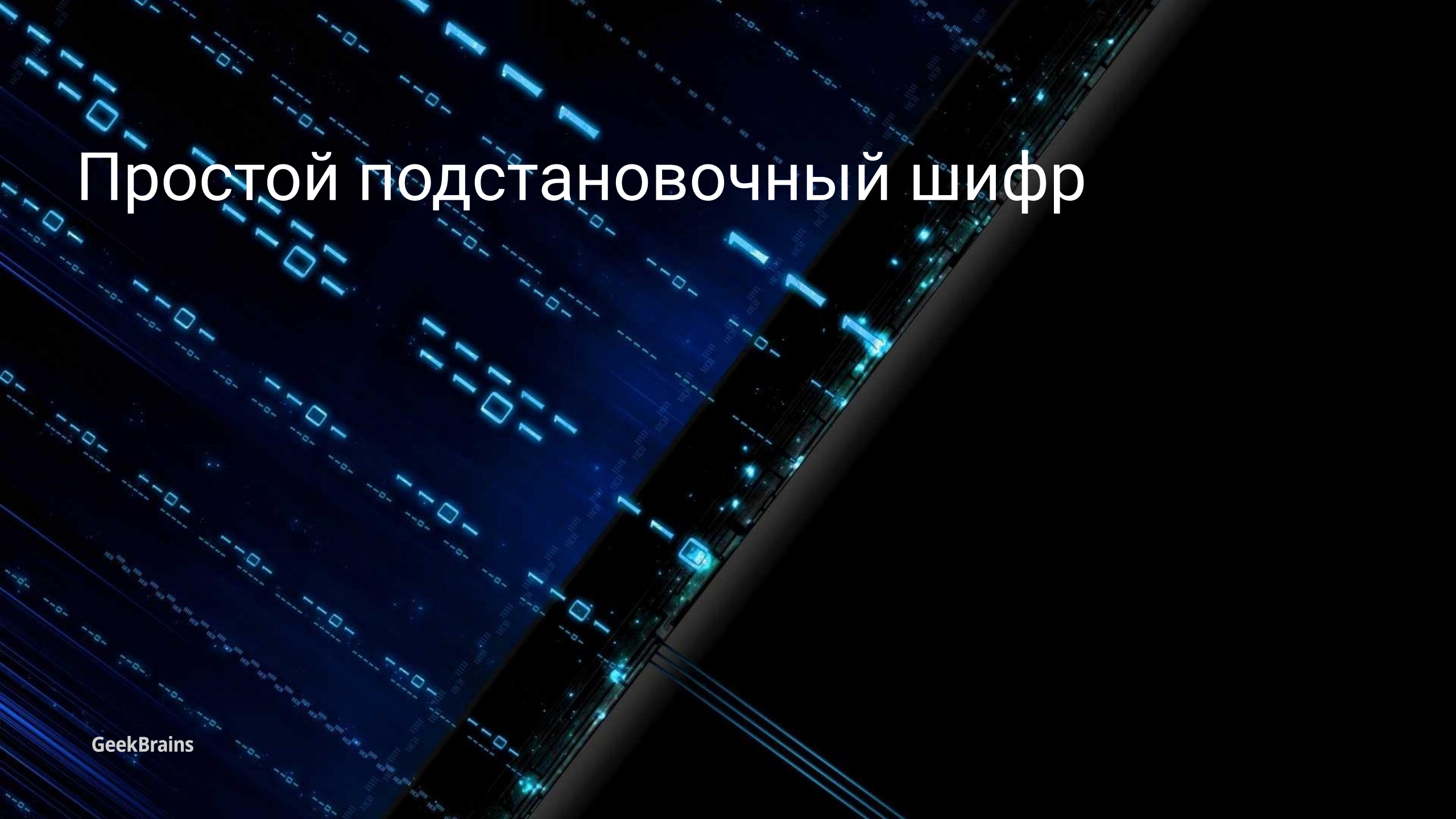
T	H	I	S	I	S	A	S	E	C	R	E	T	M	E	S	S	A	G	E

Ключевое слово записывается параллельно открытому тексту, повторяясь необходимое количество раз.

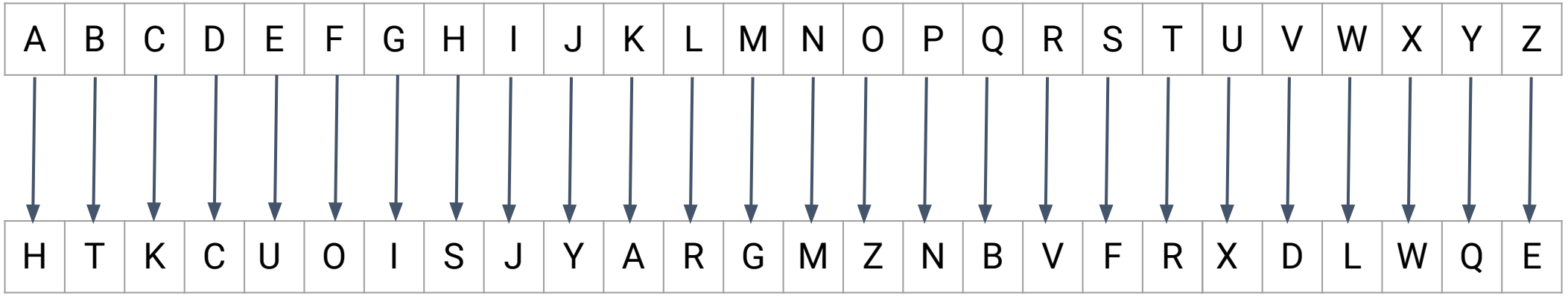
Таблица сдвигов шифра Виженера

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

Простой подстановочный шифр



Простой подстановочный шифр



Ключ:

HTKCUOISJYARGMZNBVFPXDLWQE

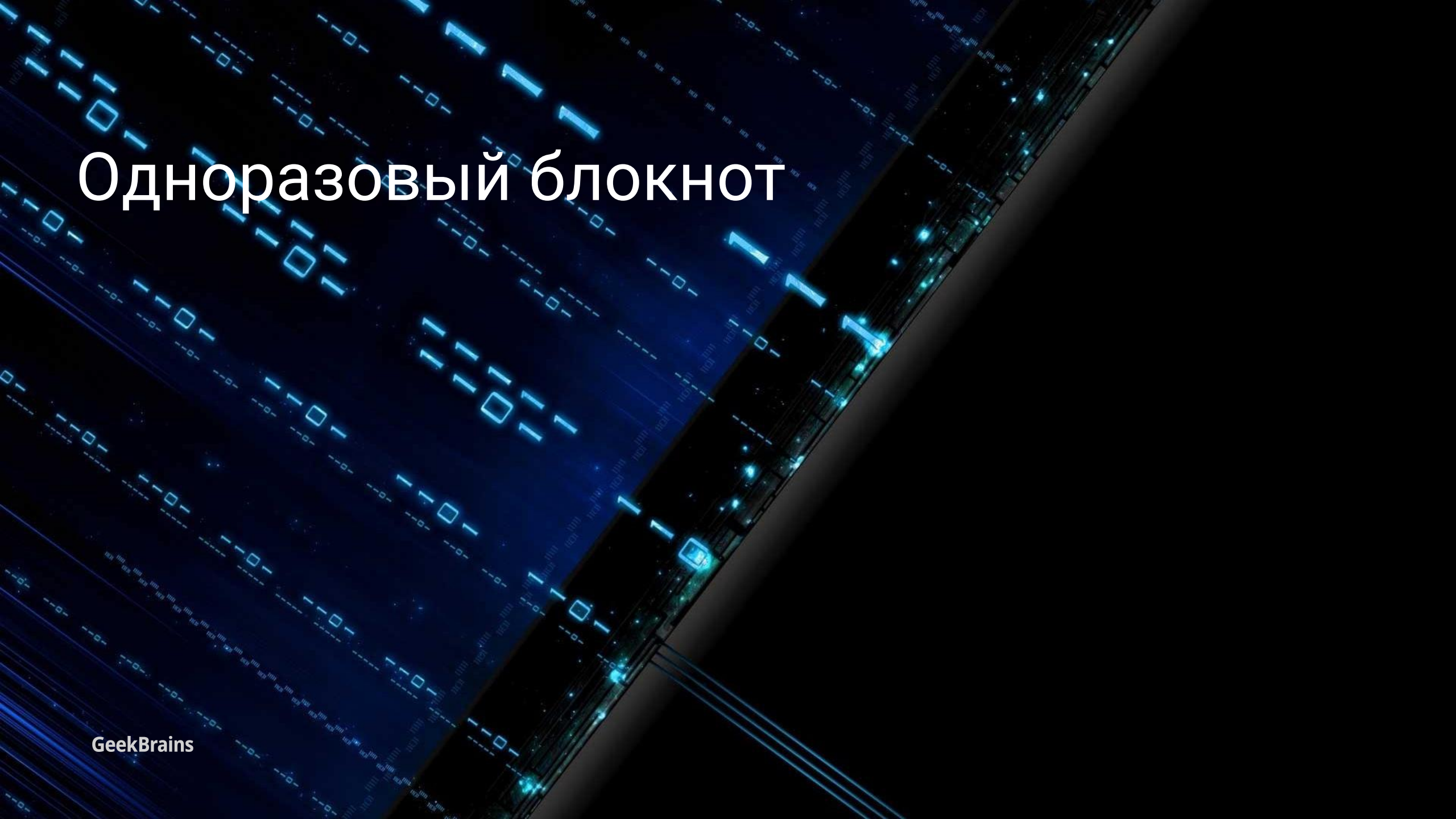
Открытый текст:

P = HELLO SIMPLE SUB CIPHER

Зашифрованный текст:

C = SURRZ FJGNRU FXT RJNSUV

Одноразовый блокнот



GeekBrains

Одноразовый блокнот

Исходное сообщение

```
this is a secret message we have to transfer it to a receiver without being read by any third person
```

+

Одноразовый блокнот

```
you can be anything you want to be just turn yourself into anything you think that you could ever be
```

>>

Криптограмма

```
rvcs if b seppxa zksqoae wr htje xo njtnlzve gh kg l rmpxwvee ppbuuur vebuo betk uy ohy hbtud kiisp
```

+

Одноразовый блокнот

```
you can be anything you want to be just turn yourself into anything you think that you could ever be
```

<<

Исходное сообщение

```
this is a secret message we have to transfer it to a receiver without being read by any third person
```

Итоги

Рассмотрели:

- Шифр Цезаря
- Шифр Виженера
- Простой подстановочный шифр
- Одноразовый блокнот