Super Agents

Необходимость засекречивать важные послания возникла еще в древности.

Со временем люди находили новые, все более сложные способы делать послания недоступными чужим глазам.

Какие типы шифрования вы знаете?

Шифрование — то есть сокрытие информации — появилось еще в древние времена. А уж когда возникли государства, армии, войны, разведка — то возникла необходимость тайно передавать какие-то сведения, чтобы, если вдруг они попадутся в руки врагу, тот ничего бы не понял.

Нужны были тайные знаки, чтобы узнавать своих.

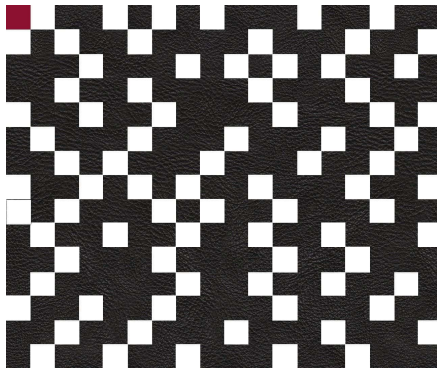
Например, разрезали на части монету.

Люди могли никогда друг друга не видеть, но если посланец предъявлял свою половинку, и при наложении обе части совпадали, значит, это свой.

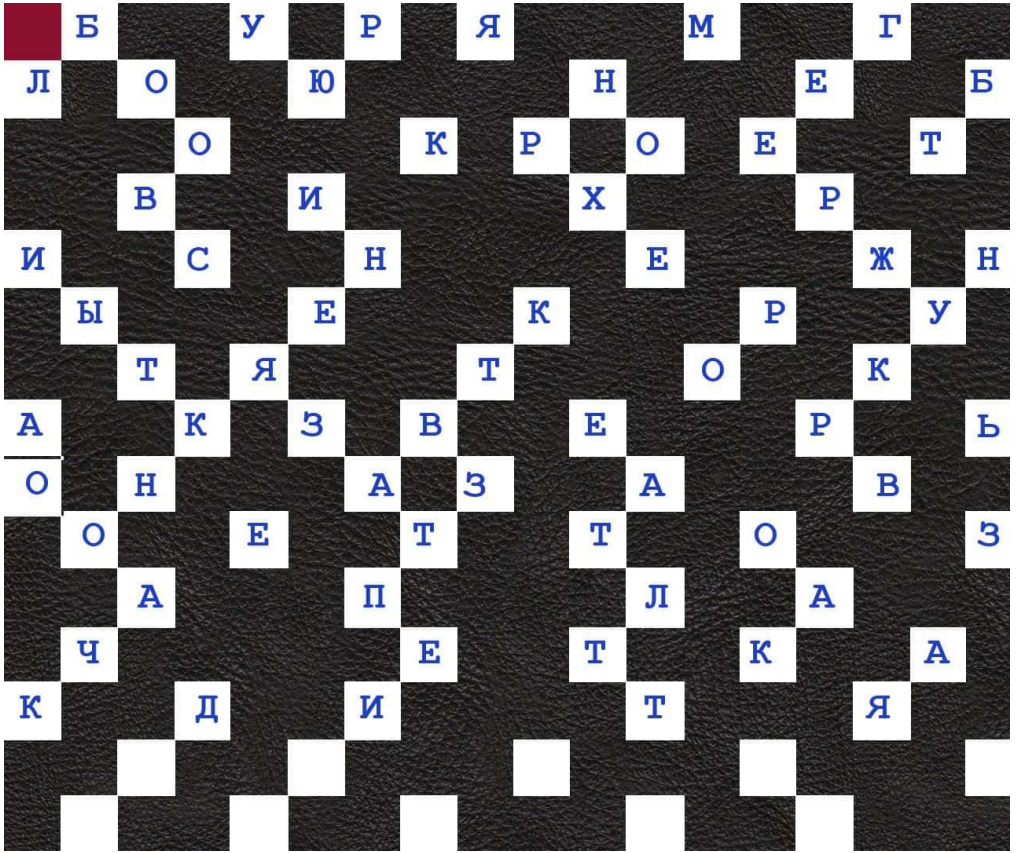
Криптография и стеганография

Есть два разных способа тайно передавать сообщение. Первый — это *криптография* (от греческого «криптос» — тайна и «графо» — пишу), в переводе на русский «тайнопись». Идея в том, что мы каким-то хитрым образом искажаем текст, который хотим скрыть, и кто этого способа не знает, не сможет его восстановить. Второй способ называется стеганография (от греческого «стеганос» — скрытый и «графо» — пишу). Здесь мы поступаем хитрее — никак не изменяем сам текст, который хотим передать, но прячем его среди ненужной информации.

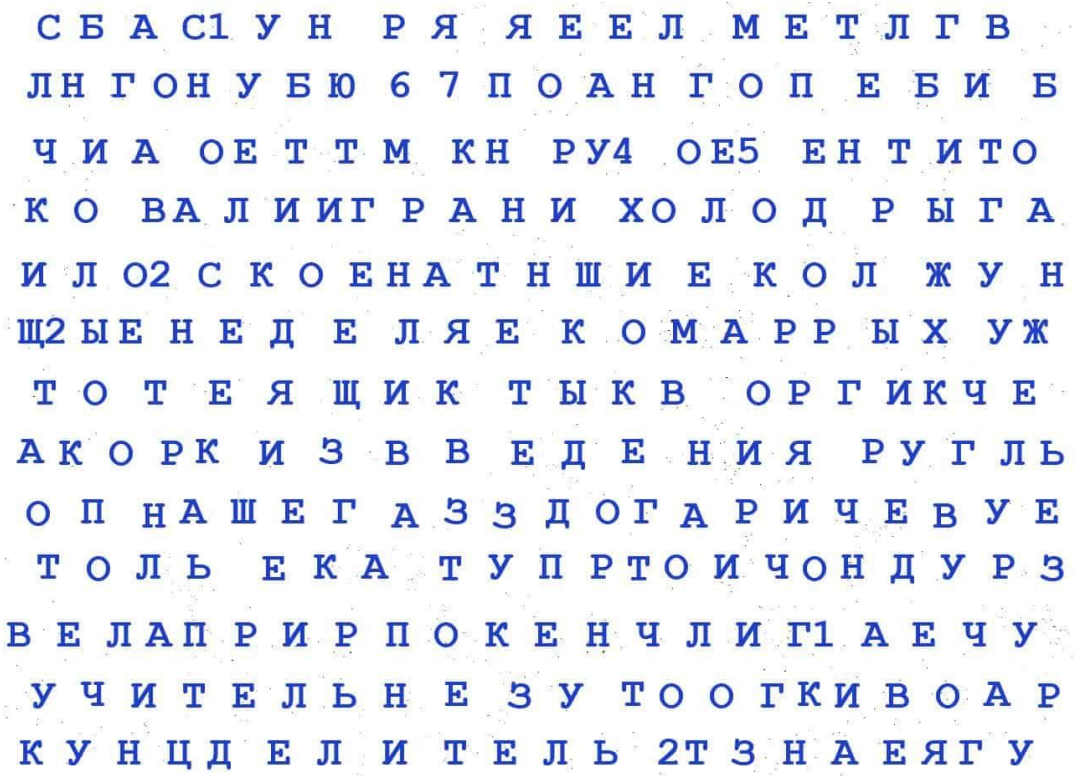
Например, используем так называемые *стеганографические решетки*. Это прямоугольные рамки, в которых хаотично прорезаны квадратики. Вот так:



Накладываем эту рамку на лист бумаги (так, чтобы цветной квадратик был в верхнем левом углу) и вписываем в прорези то сообщение, которое хотим спрятать. Без знаков препинания и без пробелов. Например:



Потом снимаем решетку и вписываем между букв нашего сообщения произвольные буквы и цифры. Например:



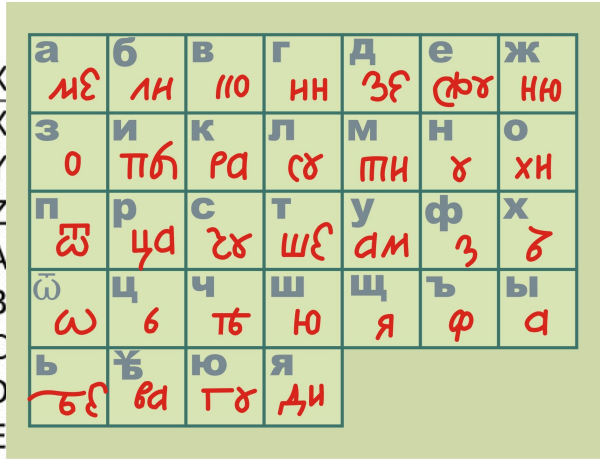
Совершенно бессмысленный текст, в котором нужное сообщение спрятано среди ненужного хлама.

Но у кого есть точно такая же решетка, может наложить ее на эту бумажку (выделенный квадратик — в левом верхнем углу) и прочитает те буквы, которые будут видны в прорезях.

По типам информации все доступные способы шифрования разделяются на:

- **симметричные**
- **ассиметричные**

	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
0	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X
1	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y
2	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z
3	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A
4	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B
5	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C
6	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D
7	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	W	X	Y	Z	A	B	C	D	E
8	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
9	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



1. К **симметричным** методам шифрования текста относятся системы шифрования с применением заранее разработанного ключа. Его должны знать только лица, ведущие между собой закрытую переписку. Для оперативного преобразования полученной информации ключ должен быть уже на руках или указан в самом сообщении.
2. Различие с симметричным методом шифрования заключается в ключах. Метод кодирования производится при помощи открытого кода. Он предоставляется в свободном доступе. Для раскодирования сообщения потребуется второй ключ. Он закрытый и знают его только участники переписки. Метод часто применяется в мессенджерах и почтовых службах.

Группы шифрования

Типы кодирования информации разделяются на алгоритмы и способы. Все они состоят из трех больших групп:

- замена;
- перестановка;
- комбинирование.

Transposition

Транспозиция / шифр перестановки

В транспозирующих шифрах буквы переставляются по заранее определенному правилу.

Например, если каждое слово пишется задом наперед, то из

«all the better to see you with» получается «lla eht retteb ot ees joy htiw». Другой пример — менять местами каждые две буквы. Таким образом, предыдущее сообщение станет «la tl eh eb tt re ot es ye uo iw ht».

hsilgnE

yadiloh

tnega repus

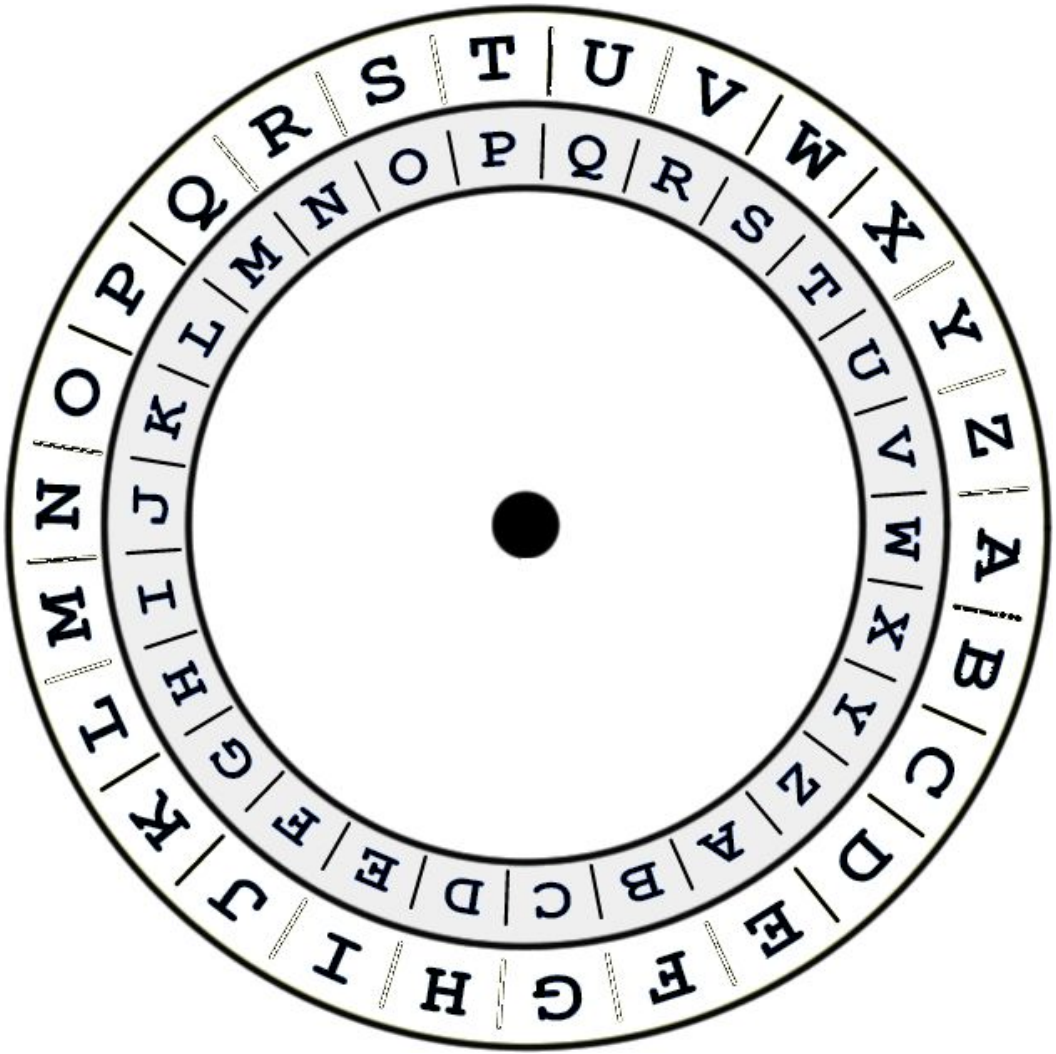
Let’s make a cypher!

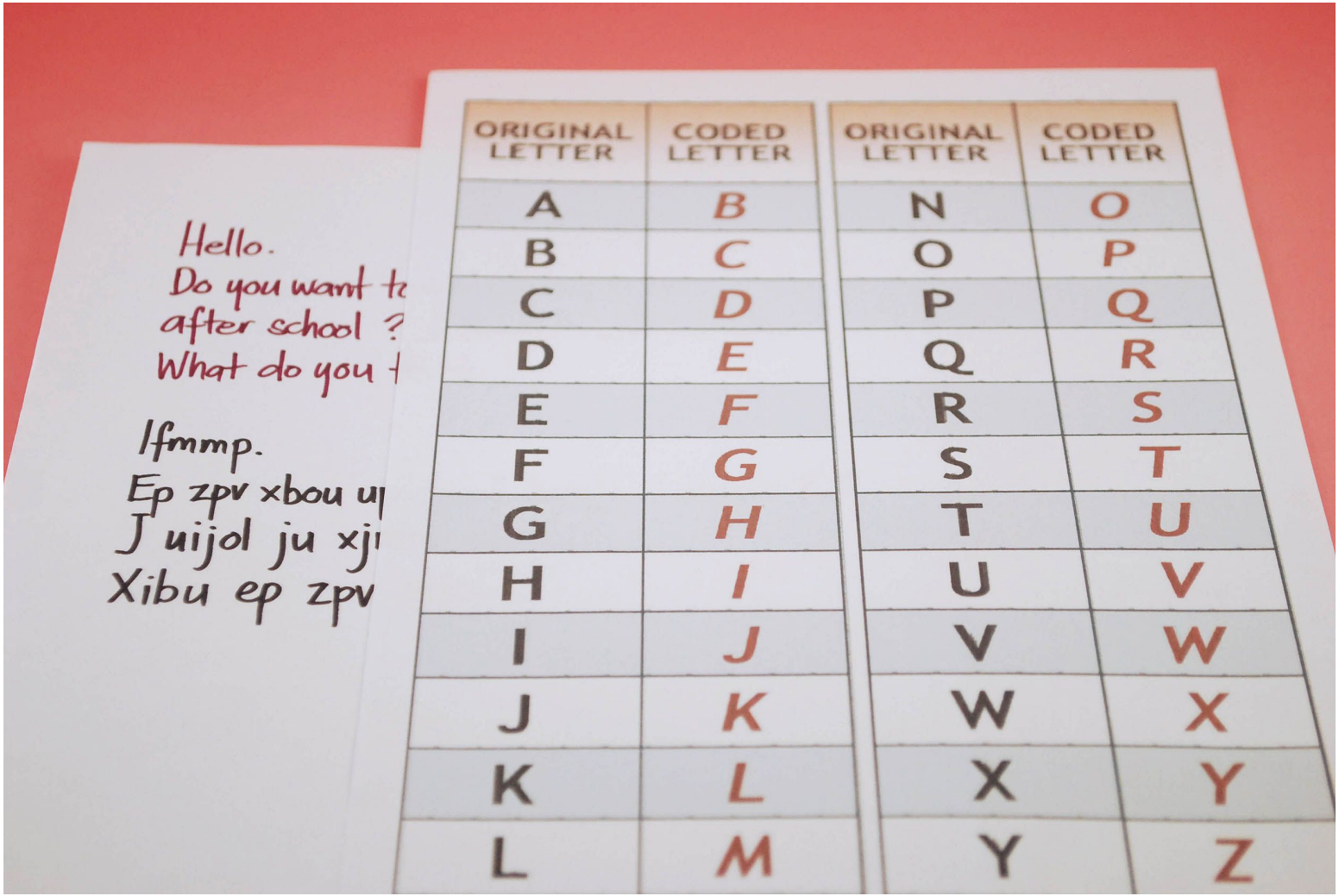
Давайте попробуем зашифровать слово!

Шифр Цезаря / Caesar cipher

Шифр Цезаря называется так, как ни странно, потому что его использовал сам Юлий Цезарь. На самом деле шифр Цезаря — это не один шифр, а целых двадцать шесть, использующих один и тот же принцип! Так, ROT1 — всего один из них.

Получателю нужно сказать, какой из шифров используется.


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
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 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 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 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 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 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 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 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 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 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 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 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 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


Hello.
Do you want t
after school ?
What do you
Ifmmp.
Ep zpv xbou u
J uijol ju xj
Xibu ep zpv
ORIGINAL LETTER
CODED LETTER
A B
B C
C D
D E
E F
F G
G H
H I
I J
J K
K L
L M
ORIGINAL LETTER
CODED LETTER
N O
O P
P Q
Q R
R S
S T
T U
U V
V W
W X
X Y
Y Z

ROT1

«ROTate 1 letter forward through the alphabet» *(англ. «сдвиньте алфавит на одну букву вперед»)*.

Сообщение **«I know what you did last summer»** станет **«J lopx xibu zpv eje mbtu tvnnfs»**.

Этот шифр весело использовать, потому что его легко понять и применять, но его так же легко и расшифровать. Из-за этого его нельзя использовать для серьезных нужд.

Let’s make a cypher!

Давайте попробуем зашифровать слово!

Polybius square / Квадрат Полибия

В Древней Греции был известен шифр, называемый "квадрат Полибия". Это устройство представляло собой квадрат 5x5, столбцы и строки которого нумеровали цифрами от 1 до 5.

В каждую клетку этого квадрата записывалась одна буква.

В греческом варианте одна клетка оставалась пустой, в латинском - в одну клетку помещали две буквы i и j.

Polybius Square Cipher Key

	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

Зашифруем слово “HAPPY”

Текст:

HAPPY

Шифротекст :

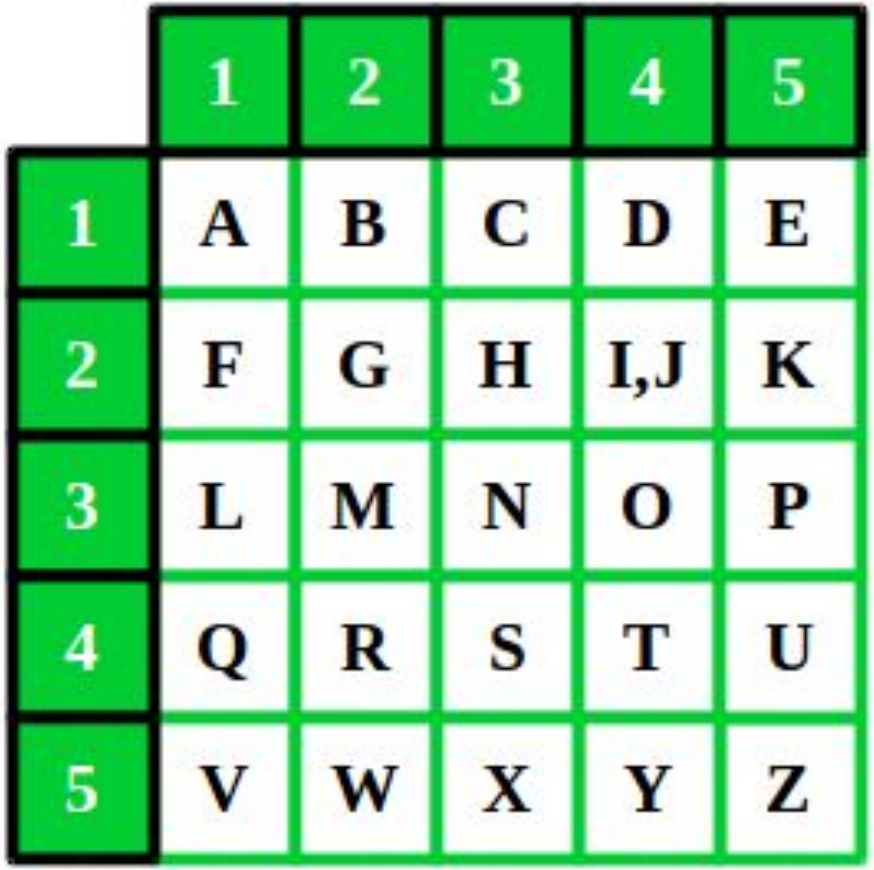
NFUUT

	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

Шифротекст:

RTHJFT

Какое слово зашифровано?



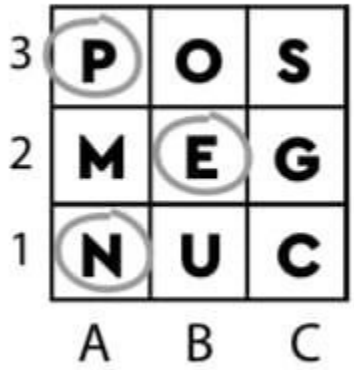
	1	2	3	4	5
1	A	B	C	D	E
2	F	G	H	I,J	K
3	L	M	N	O	P
4	Q	R	S	T	U
5	V	W	X	Y	Z

Let’s make a cypher!

Давайте попробуем зашифровать слово!

Шифровка английских слов по координатам

Пример:

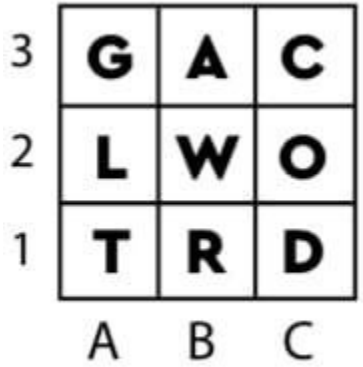


A3 B2 A1

p e n

Break the cypher!

Разгадайте шифр!



1) B1 B3 A1 .....

2) C3 B3 A1 .....

3) C1 C2 A3 .....

4) C3 C2 B2 .....

5) C2 B2 A2 .....

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

1) C3 E1 A5 A4 A2 D5 .....

2) C3 B4 C1 C1 E5 A5 .....

3) D3 B4 C2 B4 C1 A2 .....

4) E2 A4 A2 C2 E5 A5 .....

5) C3 E5 D3 C3 B3 A2 .....

Мы забыли про ребусы!

Now it’s your turn to create a cypher!

Теперь ваша очередь зашифровать слово или фразу!