



ИТ-класс
В МОСКОВСКОЙ ШКОЛЕ

Из опыта реализации модуля «Информационная безопасность» в ИТ-классах

Четверов Алексей Владимирович
Эксперт МГПУ ИРПО

Примеров киберугроз



Вирусы и
вредоносное ПО (малвари).



Фишинг.



Сайты с
неподходящим контентом



Онлайн-троллинг
Кибербуллинг

Триада информационной безопасности

Конфиденциальность

Как секрет между друзьями, некоторая информация должна быть известна только определенным людям



Триада информационной безопасности

Целостность

Подобно написанному вами письму, информация не должна быть изменена без разрешения



Триада информационной безопасности

Доступность

Как любимая видеоигра, информация должна быть доступна,
когда она нужна



Как защититься?

Представьте, что кто-то притворяется вами в интернете. Он может отправлять сообщения вашим друзьям, публиковать что-то от вашего имени, или даже потратить ваши деньги, если получит доступ к вашим банковским данным в интернете. Это называется украденной личностью, и это может произойти, если мы не будем осторожны и не будем защищать свою личную информацию..

Как защититься?

Вы когда-нибудь сталкивались с компьютерным вирусом? Так же, как простуда может заставить вас чувствовать себя больными и неспособными делать то, что вам нравится, компьютерный вирус, который является типом вредоносного ПО, может замедлить работу вашего компьютера, удалить ваши файлы или даже полностью сломать ваш компьютер. Если мы случайно загрузим вредоносное ПО, это может вызвать множество проблем.

Как защититься?

Иногда люди используют интернет, чтобы говорить грубые вещи о других или заставить их чувствовать себя плохо. Это называется кибербуллингом. Если мы не будем осторожны с тем, с кем мы общаемся в интернете, и как мы относимся к другим, мы можем стать жертвами кибербуллинга, или мы даже можем навредить другим, не осознавая этого.

Превентивный Контроль



Превентивные щиты, такие как брандмауэры, антивирусные программы и обучение пользователей, действуют как первая линия обороны в Cyberia, блокируя потенциальные угрозы до того, как они смогут проникнуть в систему и нанести ей вред.

Детективный Контроль



Детективные щиты, такие как системы обнаружения вторжений, мониторинг журналов и регулярные аудиты, служат бдительными глазами для Киберии, выявляя и предупреждая нас о любой несанкционированной активности или нарушениях в системе.

Корректирующий Контроль



Корректирующие щиты, включающие процедуры резервного копирования и восстановления, управление патчами и план реагирования на инциденты, представляют собой группу ремонта и реагирования Киберии, устраняющую любой ущерб, нанесенный киберугрозами, и укрепляющую систему против будущих атак.



Вторжение в частную жизнь

Несанкционированный доступ и использование личной информации без согласия являются этическим и юридическим нарушением..



Нарушение авторских прав

Использование охраняемых авторским правом материалов без разрешения является нарушением законов и проявлением неуважения к правам создателей.



Кража

Использование взломанного программного обеспечения является кражей чужого труда, нарушает законы об авторском праве.



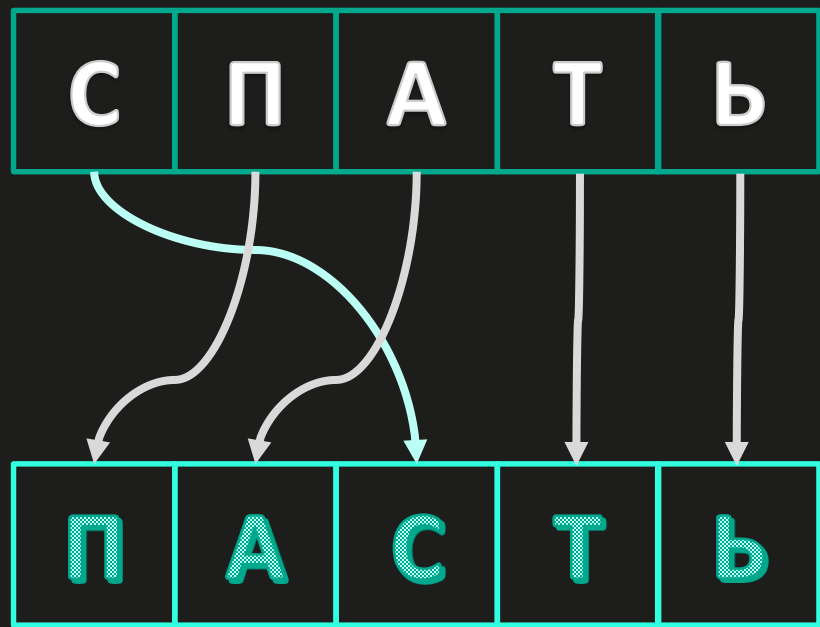
Несанкционированный доступ

Доступ к системе или данным без разрешения нарушает права владельца



Распространение вредоносного ПО

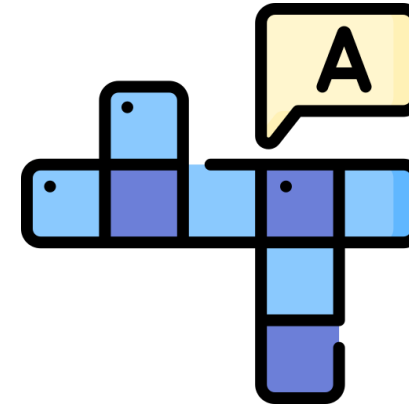
Использование накопителя с вредоносным ПО приводит к его распространению, что является нарушением закона.



нЖиьз отэ онс опд йноул.

Шифр

Перед вами зашифрованное сообщение АНАГРАММА



Расшифровка

Переставьте буквы в каждом слове так, чтобы получилось осмысленное предложение

Cesar

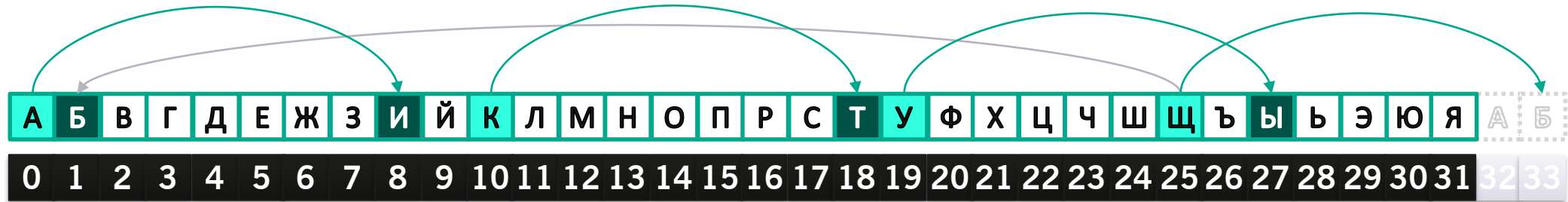
КиберХранитель на встрече с Цезарем

Где-то тут

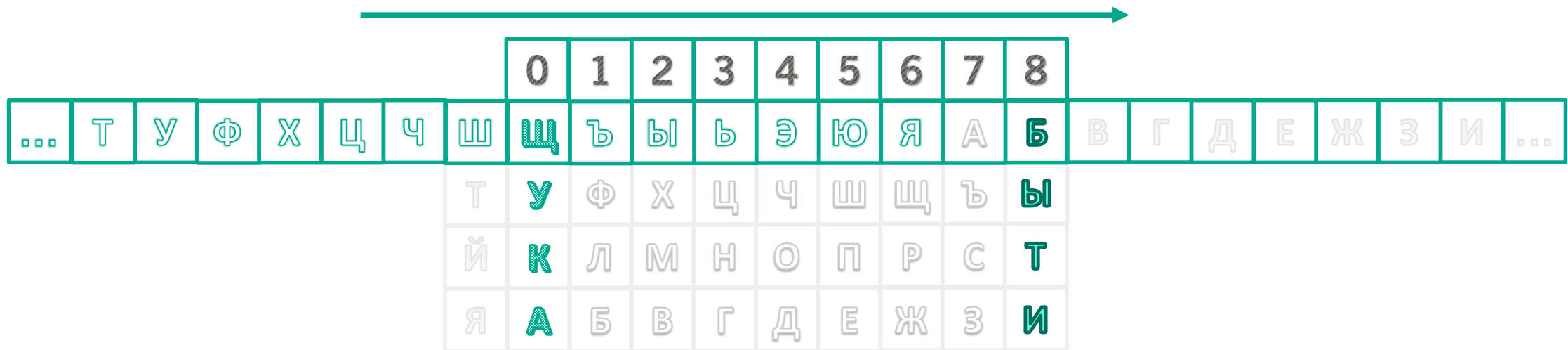
Цезарь, блестящий полководец, планировал масштабную кампанию. Однако перед ним встала проблема. Ему нужно было отправлять приказы своим генералам на огромные расстояния, но он знал, что вражеские шпионы, подобно нашей подслушивающей Еве, всегда таятся, готовые перехватить его сообщения.

Киберхранитель

Gaius Iulius Caesar



Выполняем сдвиг по ключу = 8

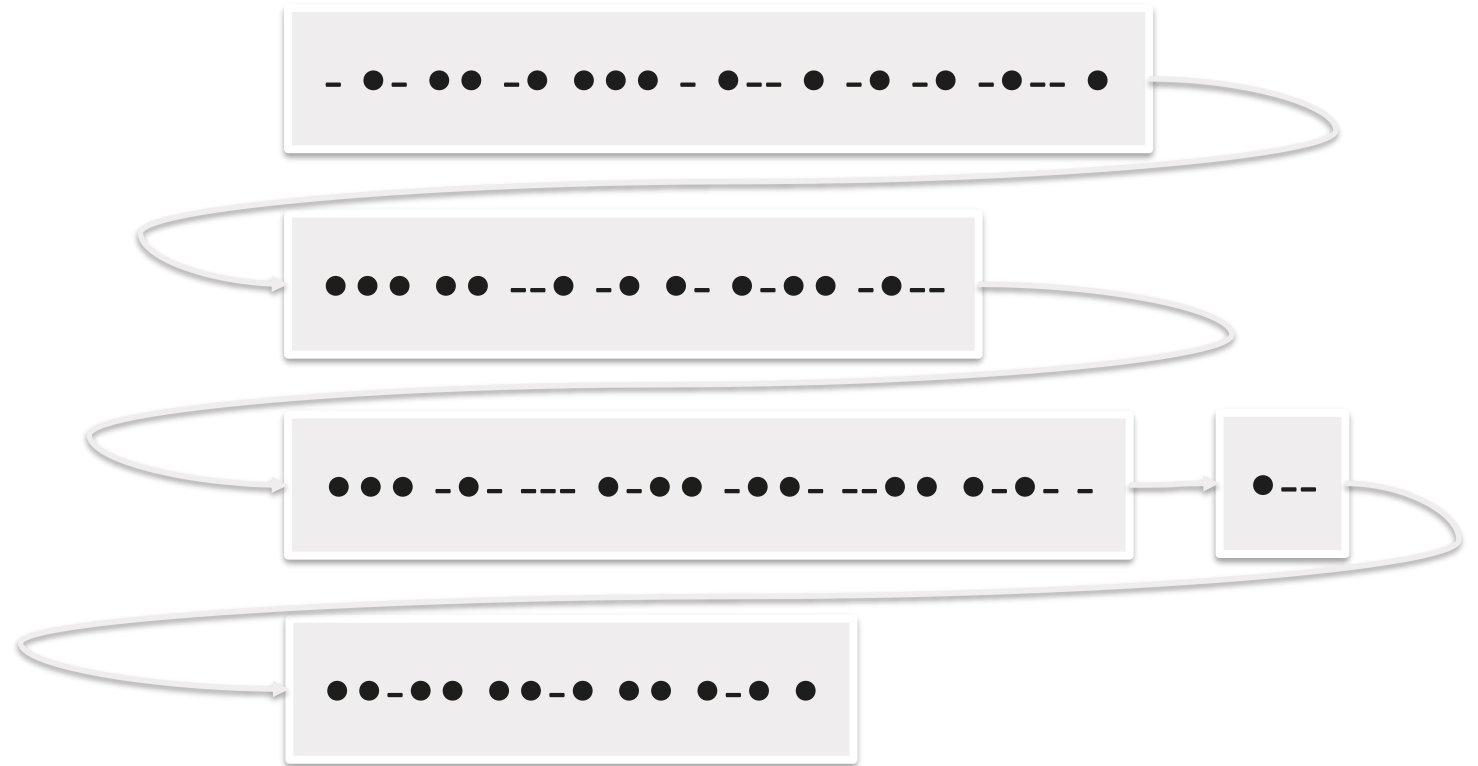


Выполняем сдвиг по алфавиту на значение ключа.

Таким образом слово ЩУКА шифруется в БЫТИ

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

Таинственные сигналы скользят в эфире



Заменяем каждую букву на последовательность точек и тире согласно ключу. Ключ это таблица

Morze

— • • • • — — • • — — • • • — — • — — • — —

Шифр

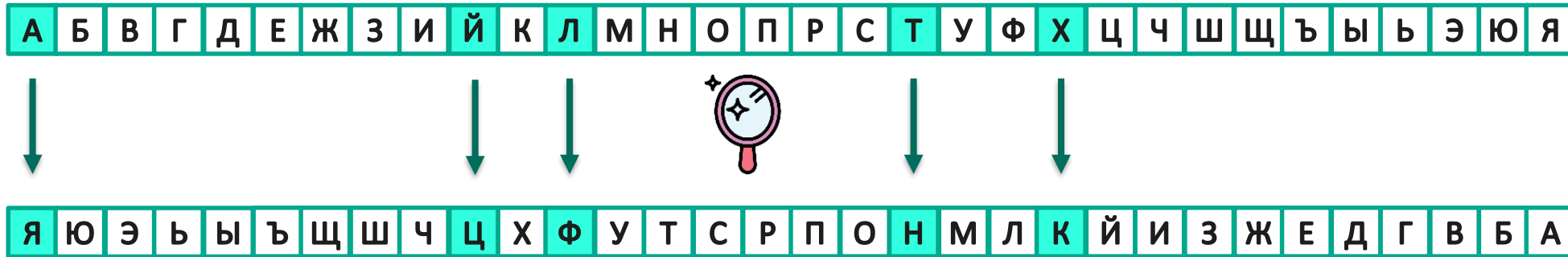
Перед вами зашифрованное сообщение переданное по телеграфу

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

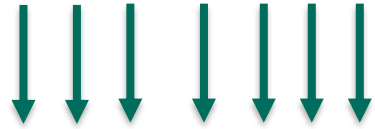
18

Расшифровка

Последовательности точек и тире должны быть заменены на соответствующие им буквы согласно таблице-ключу



Хай Лайт!



Кяц Фяцн!

Мазаль тов



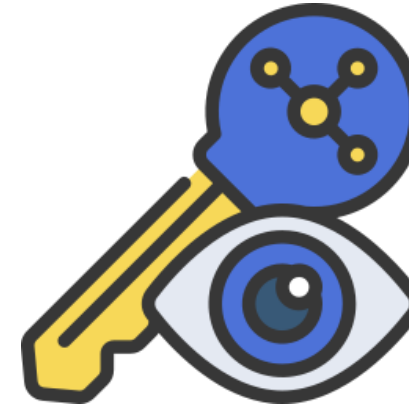
Уяшяфг нсю

Выполняем замену буквы на противоположную согласно ключу. На букву имеющую тот же порядок в зеркальном алфавите

זיאפסו חכיופ

Шифр

Перед вами зашифрованное сообщение АТБАШ



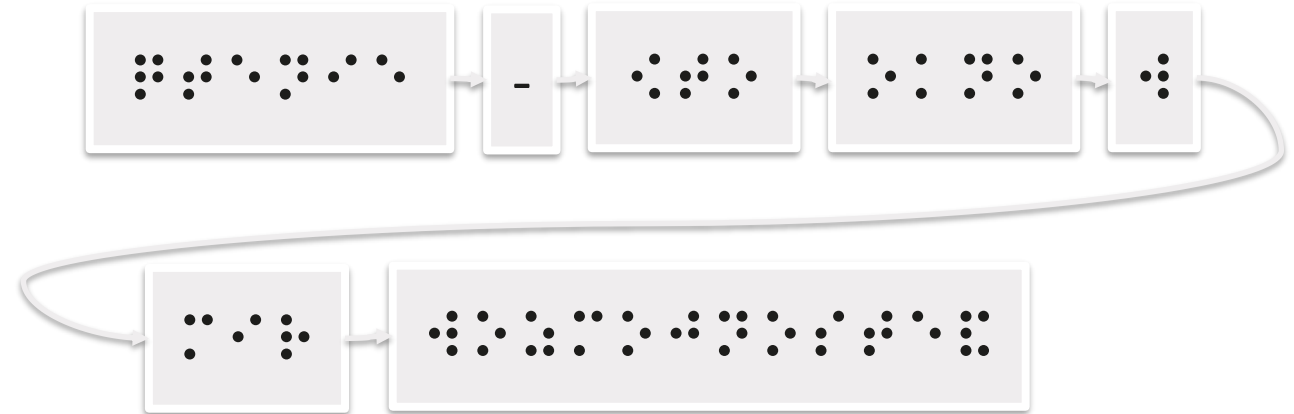
Расшифровка

Каждая буква должна быть заменена на другую из противоположного алфавита

А	Б	В	Г	Д	Е	Ж	З	И	Й	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	Й	И	З	Ж	Е	Д	Г	В	Б	А

⠁	⠃	⠉	⠎	⠙	⠅
⠚	⠵	⠇	⠊	⠏	⠌
⠓	⠈	⠋	⠎	⠕	⠔
⠠	⠶	⠒	⠡	⠼	⠢
⠨	⠰	⠒	⠠	⠴	⠠
⠩	⠱	⠒	⠠	⠴	⠠
⠪	⠳	⠒	⠠	⠴	⠠
⠫	⠴				

Чтение – это окно в мир возможностей



Заменяем каждую букву на последовательность точек согласно ключу. Ключ это таблица



Шифр

Перед вами сообщение записанное шрифтом Брайля

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

Расшифровка

Последовательности точек должны быть заменены на соответствующие им буквы согласно таблице-ключу

ДОСОБАСАВЛЕСЕНИСИЕСЕ
ШУСУМАСА

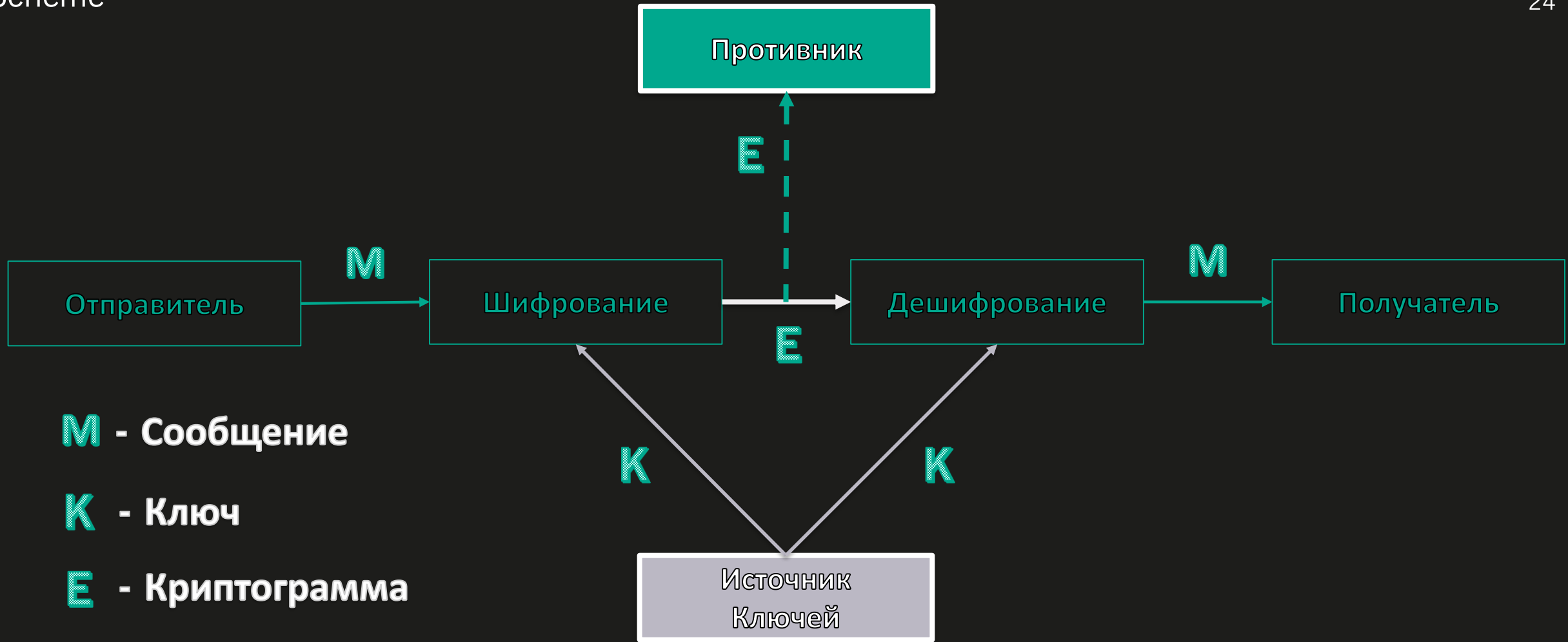
Шифр

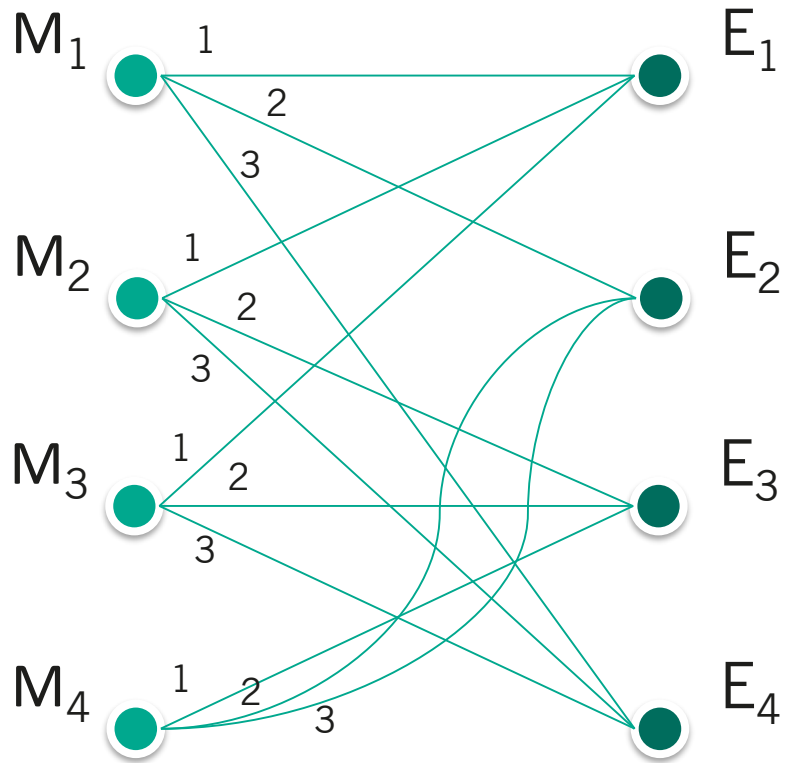
Перед вами зашумленное
сообщение



Расшифровка

Уберите весь лишний шум,
выполните роль фильтрующего
элемента по известному алгоритму





Замкнутая система

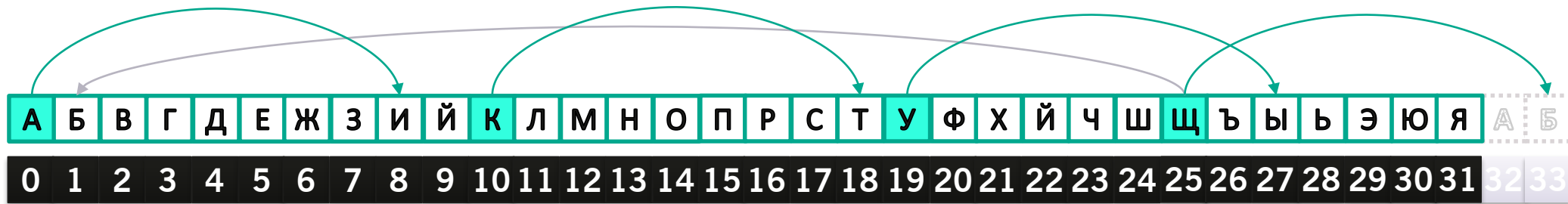
Возможные сообщения представлены точками слева, а возможные криптограммы точками справа. Вес связи это номера ключей

$$M = m_1 m_2 m_3 m_4 \dots$$

$$E = e_1 e_2 e_3 e_4 \dots = f(m_1) f(m_2) f(m_3) f(m_4) \dots$$

$f(m)$ - имеет обратную функцию

$$f(m) = (m + k) \bmod n$$



m – исходное сообщение

k – ключ

n – мощность используемого множества символов
языка

ЩУКА \rightarrow БЫТИ

$k = 8$

$$f(25) = (25 + 8) \% 32 = 1$$

$$f(19) = (19 + 8) \% 32 = 27$$

$$f(10) = (10 + 8) \% 32 = 18$$

$$f(0) = (0 + 8) \% 32 = 8$$

$$f(m_i) = (m_i + k_i) \bmod n$$

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31
0	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
1	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А
2	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
3	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
4	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
5	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
6	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
7	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
8	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
9	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И

$$f(25) = (25 + 8) \% 32 = 1 \quad f(10) = (10 + 5) \% 32 = 18$$

$$f(19) = (19 + 6) \% 32 = 25 \quad f(0) = (0 + 4) \% 32 = 8$$

m – исходное сообщение

k – ключ

n – мощность используемого множества символов языка

ЩУКА → БЩПД
 8 6 5 4

	0	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	
0	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	
1	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
2	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
3	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
4	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
5	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
6	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж
7	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З
8	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И
9	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й
10	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К
11	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л
12	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М
13	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н
14	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О
15	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П
16	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р
17	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
18	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
19	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
20	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
21	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
22	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
23	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
24	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
25	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
26	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
27	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
28	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
29	Э	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
30	Ю	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
31	Я	А	Б	В	Г	Д	Е	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

$$f(m_i) = (m_i + ki + 1) \bmod n$$

m – исходное сообщение

k – ключ. +1 т.к. ROT1

n – мощность используемого множества символов языка

$$f(25) = (25 + 31 + 1) \% 32 = 25 \quad f(10) = (10 + 11 + 1) \% 32 = 22$$

$$f(19) = (19 + 17 + 1) \% 32 = 5 \quad f(0) = (0 + 8 + 1) \% 32 = 9$$

ЩУКА → ЩЕЦЙ
Я С Л И

Code sample

29

```
a = [1, 2, 3] # списки
```

```
f = open("file.name", "r", encoding="utf-8") # работа с файлами  
data1 = f.readlines()  
f.close()
```

```
with open("file.name", "r", encoding="utf-8") as f: # работа с файлами  
    data2 = f.readlines()
```

```
f = "привет как дела".split() # работа со строками
```

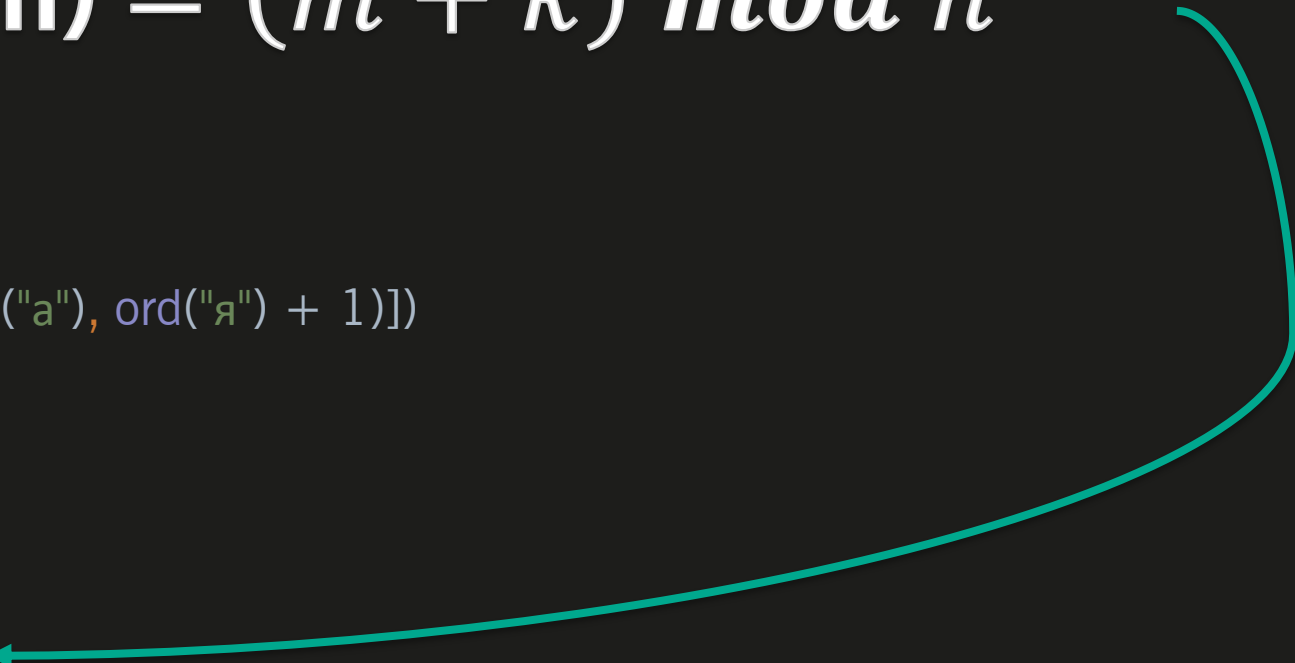
```
print(cesarEncrypt("код", 3))
```

```
i = input() # получить данные на стандартный вход
```

$$f(m) = (m + k) \bmod n$$

```
# -*- coding: utf-8 -*-
```

```
def cesarEncrypt(message, key):  
    alphabet = "".join([chr(i) for i in range(ord("a"), ord("я") + 1)])  
    n = len(alphabet)  
    newMessage = ""  
    for character in message:  
        if character in alphabet:  
            position = alphabet.find(character)  
            newPosition = (position + key) % n  
            newCharacter = alphabet[newPosition]  
            newMessage += newCharacter  
        else:  
            newMessage += character  
    return newMessage
```



Code sample

$$f(m) = (m + k) \bmod n$$

31

```
# -*- coding: utf-8 -*-
```

```
def cesarEncrypt(message, key):  
    n = ord("я") - ord("a") + 1  
    newMessage = ""  
    for character in message:  
        if ord("a") <= ord(character) <= ord("я"):  
            position = ord(character)  
            newPosition = (position - ord("a") + key) % n  
            newCharacter = chr(newPosition + ord("a"))  
            newMessage += newCharacter  
        else:  
            newMessage += character  
    return newMessage
```





ИТ-класс
В МОСКОВСКОЙ ШКОЛЕ

Спасибо за внимание

Четверов Алексей Владимирович
Эксперт МГПУ ИРПО

<https://kids.kaspersky.ru/metodic/>

