# Шифрование

# Определение

Шифрование – это технология кодирования и раскодирования данных

# Определение

Это математический процесс преобразования сообщения в вид, нечитаемый для всех, кроме того человека или устройства, у которого имеется **ключ** для «расшифровки» этого сообщения обратно в читаемый вид.

# Примеры

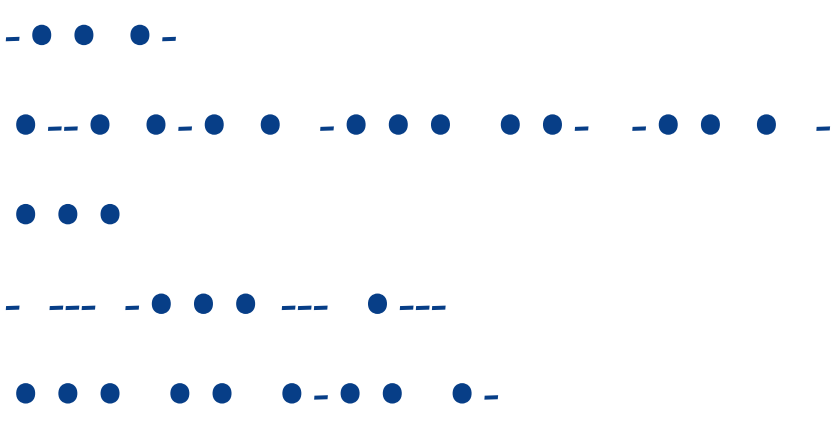
| | | | |
|---|---|---|---|
| А •– | И •• | Р •–• | Ш –––– |
| Б –••• | Й •––– | С ••• | Щ ––•– |
| В •–– | К –•– | Т – | Ъ •––•–• |
| Г ––• | Л •–•• | У ••– | Ы –•–– |
| Д –•• | М –– | Ф ••–• | Ь –••– |
| Е • | Н –• | Х •••• | Э ••–•• |
| Ж •••– | О ––– | Ц –•–• | Ю ••–– |
| З ––•• | П •––• | Ч –––•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

# Примеры

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

Азбука Морзе

# Азбука Морзе



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

# Азбука Морзе

Да

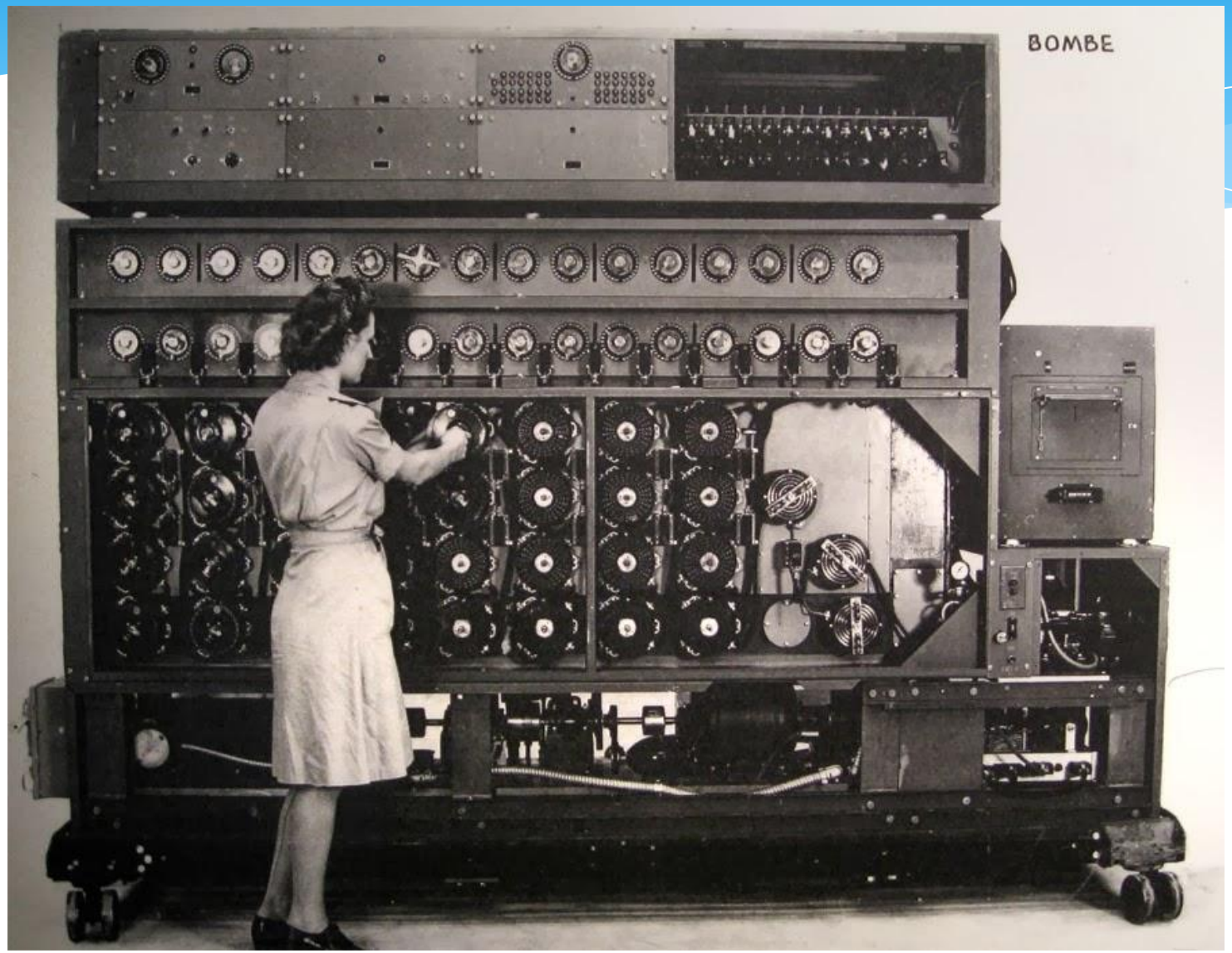
Пребудет

С

Тобой

Сила

# Шифр Энигмы



# Шифр A1Z26

ABCDEFGHIJKLMNOPQRSTUVWXYZ

23-1-11-5  21-16, 19-1-13-16-18-1-9

# Шифр A1Z26

ABCDEFGHIJKLMNOPQRSTUVWXYZ

23-1-11-5 21-16, 19-1-13-16-18-1-9

Wake up , samurai

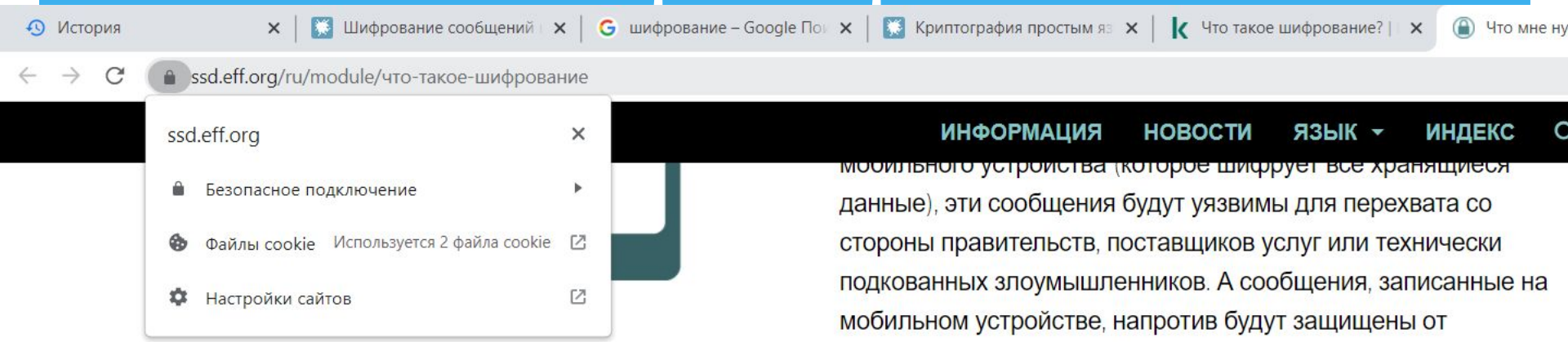
# ASCII

| Dec | Hex | Oct | Char | Dec | Hex | Oct | Char | Dec | Hex | Oct | Char | Dec | Hex | Oct | Char |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 0 | 0 | 0 | | 32 | 20 | 40 | [space] | 64 | 40 | 100 | @ | 96 | 60 | 140 | ` |
| 1 | 1 | 1 | | 33 | 21 | 41 | ! | 65 | 41 | 101 | A | 97 | 61 | 141 | a |
| 2 | 2 | 2 | | 34 | 22 | 42 | " | 66 | 42 | 102 | B | 98 | 62 | 142 | b |
| 3 | 3 | 3 | | 35 | 23 | 43 | # | 67 | 43 | 103 | C | 99 | 63 | 143 | c |
| 4 | 4 | 4 | | 36 | 24 | 44 | $ | 68 | 44 | 104 | D | 100 | 64 | 144 | d |
| 5 | 5 | 5 | | 37 | 25 | 45 | % | 69 | 45 | 105 | E | 101 | 65 | 145 | e |
| 6 | 6 | 6 | | 38 | 26 | 46 | & | 70 | 46 | 106 | F | 102 | 66 | 146 | f |
| 7 | 7 | 7 | | 39 | 27 | 47 | ' | 71 | 47 | 107 | G | 103 | 67 | 147 | g |
| 8 | 8 | 10 | | 40 | 28 | 50 | ( | 72 | 48 | 110 | H | 104 | 68 | 150 | h |
| 9 | 9 | 11 | | 41 | 29 | 51 | ) | 73 | 49 | 111 | I | 105 | 69 | 151 | i |
| 10 | A | 12 | | 42 | 2A | 52 | * | 74 | 4A | 112 | J | 106 | 6A | 152 | j |
| 11 | B | 13 | | 43 | 2B | 53 | + | 75 | 4B | 113 | K | 107 | 6B | 153 | k |
| 12 | C | 14 | | 44 | 2C | 54 | , | 76 | 4C | 114 | L | 108 | 6C | 154 | l |
| 13 | D | 15 | | 45 | 2D | 55 | - | 77 | 4D | 115 | M | 109 | 6D | 155 | m |
| 14 | E | 16 | | 46 | 2E | 56 | . | 78 | 4E | 116 | N | 110 | 6E | 156 | n |
| 15 | F | 17 | | 47 | 2F | 57 | / | 79 | 4F | 117 | O | 111 | 6F | 157 | o |
| 16 | 10 | 20 | | 48 | 30 | 60 | 0 | 80 | 50 | 120 | P | 112 | 70 | 160 | p |
| 17 | 11 | 21 | | 49 | 31 | 61 | 1 | 81 | 51 | 121 | Q | 113 | 71 | 161 | q |
| 18 | 12 | 22 | | 50 | 32 | 62 | 2 | 82 | 52 | 122 | R | 114 | 72 | 162 | r |
| 19 | 13 | 23 | | 51 | 33 | 63 | 3 | 83 | 53 | 123 | S | 115 | 73 | 163 | s |
| 20 | 14 | 24 | | 52 | 34 | 64 | 4 | 84 | 54 | 124 | T | 116 | 74 | 164 | t |
| 21 | 15 | 25 | | 53 | 35 | 65 | 5 | 85 | 55 | 125 | U | 117 | 75 | 165 | u |
| 22 | 16 | 26 | | 54 | 36 | 66 | 6 | 86 | 56 | 126 | V | 118 | 76 | 166 | v |
| 23 | 17 | 27 | | 55 | 37 | 67 | 7 | 87 | 57 | 127 | W | 119 | 77 | 167 | w |
| 24 | 18 | 30 | | 56 | 38 | 70 | 8 | 88 | 58 | 130 | X | 120 | 78 | 170 | x |
| 25 | 19 | 31 | | 57 | 39 | 71 | 9 | 89 | 59 | 131 | Y | 121 | 79 | 171 | y |
| 26 | 1A | 32 | | 58 | 3A | 72 | : | 90 | 5A | 132 | Z | 122 | 7A | 172 | z |
| 27 | 1B | 33 | | 59 | 3B | 73 | ; | 91 | 5B | 133 | [ | 123 | 7B | 173 | { |
| 28 | 1C | 34 | | 60 | 3C | 74 | < | 92 | 5C | 134 | \ | 124 | 7C | 174 | \| |
| 29 | 1D | 35 | | 61 | 3D | 75 | = | 93 | 5D | 135 | ] | 125 | 7D | 175 | } |
| 30 | 1E | 36 | | 62 | 3E | 76 | > | 94 | 5E | 136 | ^ | 126 | 7E | 176 | ~ |
| 31 | 1F | 37 | | 63 | 3F | 77 | ? | 95 | 5F | 137 | _ | 127 | 7F | 177 | |

# Примеры

* Сайты финансовых, правительственных, образовательных и торговых организаций обычно шифруют ваши данные, чтобы **защитить их от краж и мошенничества**. На то, что веб-формы защищены и что ваши данные будут зашифрованы, вам укажет следующее:
* - Адрес веб-страницы начинается с "http**s**": это означает, что ваши данные будут зашифрованы и переданы с использованием защищенного протокола.
* - В нижнем левом или нижнем правом углу окна браузера расположен значок в виде замка. Если вы кликните на значок блокировки, вы увидите сведения о безопасности сайта.

# Примеры




мобильного устройства (которое шифрует все хранящиеся данные), эти сообщения будут уязвимы для перехвата со стороны правительств, поставщиков услуг или технически подкованных злоумышленников. А сообщения, записанные на мобильном устройстве, напротив будут защищены от злоумышленников, имеющих физический доступ к устройству, но не знающих пароля.

И наоборот, если вы отправляете сообщение с использованием сквозного шифрования (шифру передающиеся данные) на устройство, не использующее шифрование (не шифрующее хранящиеся на нём данные), эти сообщения будут недоступны для шпионов в сети. Однако есл кто-либо получит физический доступ к этому мобильному устройству, то он получит доступ к сообщению и сможет его прочитать.

Учитывая приведённые примеры, идеальным способом защиты от широкого круга угроз станет шифрование данных, как хранящихся на устройстве, так и передаваемых в сети.

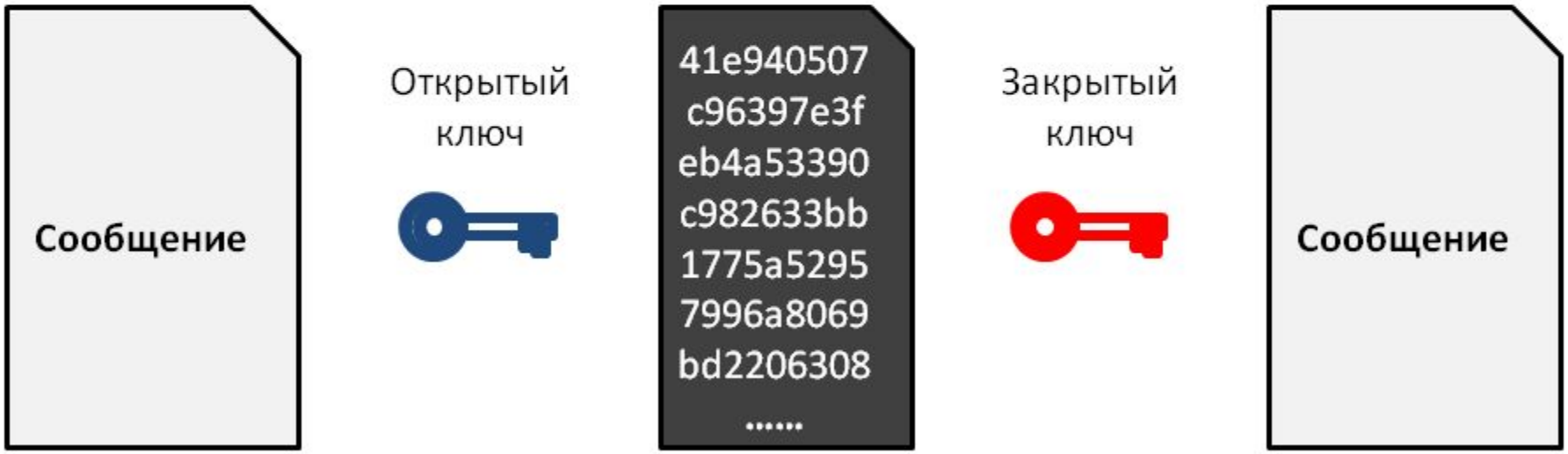
Для получения более подробной информации по использованию шифрования обратитесь к нашему руководству «Ключевые концепции шифрования».

# Симметричное шифрование

# Симметричное шифрование

Слабым местом симметричного шифрования является ключ шифрования, точнее его доставка до адресата. Если во время доставки ключ будет скомпрометирован, стороннее лицо легко раскодирует сообщение. Сильной стороной симметричного шифрования является его скорость, что дает возможность кодировать большие объемы данных.

# Асимметричное шифрование



# Асимметричное шифрование

https://youtu.be/sGFbM-X6W_4

# Асимметричное шифрование

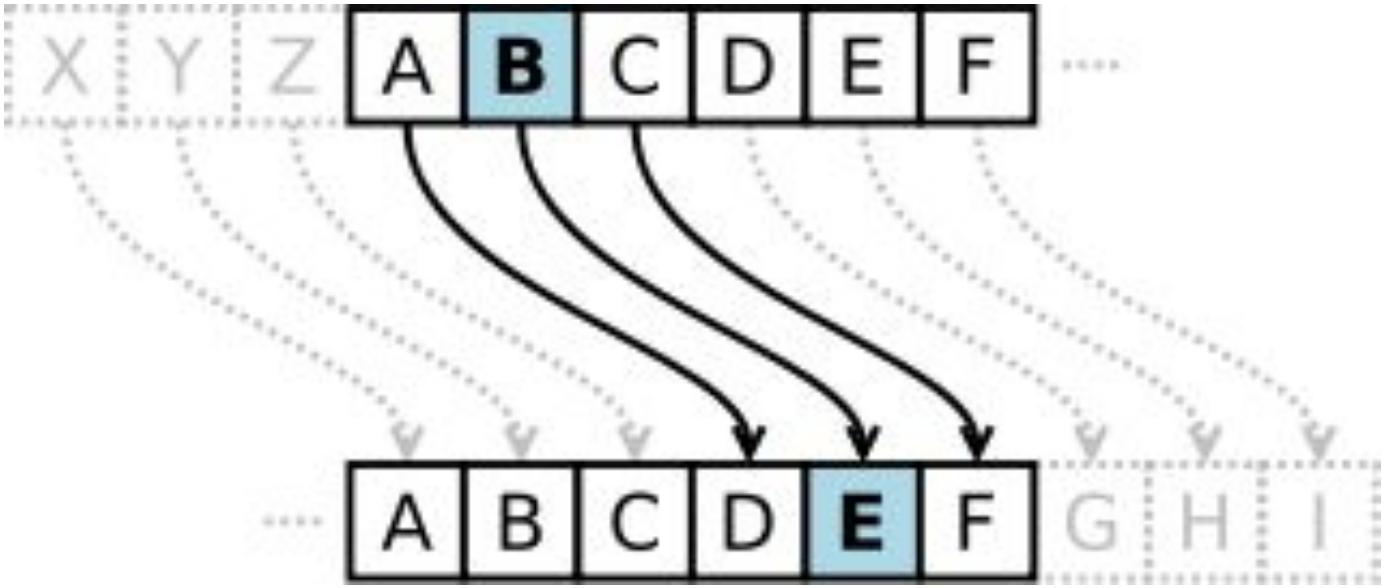
* адресат отправляет ОТКРЫТЫЙ ключ отправителю;
* отправитель кодирует сообщение при помощи полученного открытого ключа. При этом, раскодировать сообщение можно теперь только закрытым ключом;
* при получении зашифрованного сообщения адресат раскодирует его ЗАКРЫТЫМ ключом (который был сгенерирован в паре с открытым).

# Шифр Цезаря

https://youtu.be/pi58jcbs09k

# Шифр Цезаря

Сдвиг в исходном алфавите на величину **шага**



# Шифр Цезаря
# Шаг = 7

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

# Шифр Цезаря
# Шаг = 7

| 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 |
|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|---|
| 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 |

# Исходные данные

Что необходимо создать в начале ?

# Исходные данные

Алфавит

alfavit_EU = 'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

alfavit_RU = 'АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ'

# Исходные данные

Задать шаг смещения:

offset = …

# Исходные данные

Задать шаг смещения:

```
offset = int(input('Шаг шифрования: '))
```

# Исходные данные

Задать исходное сообщение:

message=…

# Исходные данные

Задать исходное сообщение:

```
message = input("Сообщение для шифровки: ")
```

# Исходные данные

Задать исходное сообщение (*с поправкой на алфавит*):

alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

message = input("Сообщение для шифровки: ")

*Что необходимо сделать с исходным сообщением ?*

# Исходные данные

Задать исходное сообщение (*с поправкой на алфавит*):

```
alfavit_EU =  'ABCDEFGHIJKLMNOPQRSTUVWXYZ'

message = input("Сообщение для шифровки: ").upper()
```

# Исходные данные

Создать переменную для итога:

itog = …

# Исходные данные

Создать переменную для итога:

itog =''

# Алгоритм работы

1. Ввести шаг шифрования
2. Ввести исходное сообщение
3. Выбрать язык (RU/EN)
4. Зашифровать шифром Цезаря исходное сообщение (2) с шагом (1) использую алфавит (3)
5. Вывести зашифрованное сообщение

# Хеширование