

Основные сведения

Математическая модель

$$E(x) = ((m-1)x + (m-1)) \bmod m$$

$$E(x) = ((m-1)(x+1)) \bmod m$$

$$D(x) = E(x) \quad x \quad m$$

Авторы

Криптоанализ

Источники

1. Leuchter, Mark. "Jeremiah's 70-Year Prophecy and the מק בל/שש Atbash Codes." *Biblica*, vol. 85, no. 4, 2004, pp. 503–22. JSTOR, <http://www.jstor.org/stable/42614548>. Accessed 18 Dec. 2023.
 2. <https://www.geeksforgeeks.org/implementing-atbash-cipher/>
-

Исторические сведения

Шифр Атбаш - один из самых древних алгоритмов шифрования. Слова, зашифрованные этим шифром, встречаются в еврейской Библии (Танахе). Например, в книге пророка Иеремии в предложении «А царь Шешаха будет пить последним» слово «Шешах» (ивр. ששח) является криптограммой слова «Вавилон» (ивр. בבל) (Книга пророка Иеремии, глава 25, стих 26). Эта же криптограмма встречается в другом месте этой книги, а именно, в главе 51, стих 41. А в предложении «Подниму Я против Вавилона, против жителей Лев-Камая, ветер гибельный!» слово «Лев-Камай» (ивр. לבקמי) является криптограммой слова «Халдея» (ивр. כשדים) (Книга пророка Иеремии, глава 51, стих 1). Главы этой книги писались в период примерно с 626 по 580 год до н.э. Название шифра Атбаш (אלבאש) составлено из букв «алеф» א, «тав» ת, «бет» ב, «шин» ש. Это первая, последняя, вторая и предпоследняя, соответственно, буквы еврейского алфавита (еврейские буквы пишутся справа — налево). Т.е. в самом названии шифра отражен принцип шифрования: первая буква алфавита заменяется на последнюю букву алфавита, вторая буква на предпоследнюю, и т.д. Темура (ивр. תמורה)

Церуф (ивр. צירוף)

тав	ת	א	алеф
шин	ש	ב	бет
реш	ר	ג	гимель
куф	ק	ד	далет
цади	צ	ה	хе
пе	פ	ו	вав
аин	ע	ז	заин
самех	ס	ח	хет
нун	נ	ט	тет
мем	מ	י	йуд
ламед	ל	כ	каф
каф	כ	ל	ламед
йуд	י	מ	мем
тет	ט	נ	нун
хет	ח	ס	самех
заин	ז	ע	аин
вав	ו	פ	пе
хе	ה	צ	цади
далет	ד	ק	куф
гимель	ג	ר	реш
бет	ב	ש	шин
алеф	א	ת	тав

Пример реализации на языке Python

Код:

```
# Python program to implement Atbash Cipher
# This script uses dictionaries to lookup various alphabets
lookup_table = {'A' : 'Z', 'B' : 'Y', 'C' : 'X', 'D' : 'W', 'E' : 'V',
                'F' : 'U', 'G' : 'T', 'H' : 'S', 'I' : 'R', 'J' : 'Q',
                'K' : 'P', 'L' : 'O', 'M' : 'N', 'N' : 'M', 'O' : 'L',
                'P' : 'K', 'Q' : 'J', 'R' : 'I', 'S' : 'H', 'T' : 'G',
                'U' : 'F', 'V' : 'E', 'W' : 'D', 'X' : 'C', 'Y' : 'B', 'Z' : 'A'}

def atbash(message):
    cipher = ""
    for letter in message:
        # checks for space
        if(letter != ' '):
            #adds the corresponding letter from the lookup_table
            cipher += lookup_table[letter]
        else:
            # adds space
            cipher += ' '
    return cipher

# Driver function to run the program
def main():
    #encrypt the given message
    message = 'GEEKS FOR GEEKS'
    print(atbash(message.upper()))

    #decrypt the given message
    message = 'TVVPH ULI TVVPH'
    print(atbash(message.upper()))

# Executes the main function
if __name__ == '__main__':
    main()
```

Результат:

```
TVVPH ULI TVVPH
GEEKS FOR GEEKS
```

Атбаш (ивр. אַתבּשׁ)

Моноалфавитные шифры подстановки Группа 1



■ Шифры подстановки

■ Моноалфавитные шифры подстановки

■ Аффинные шифры

The ATBASH Cipher

א ב ג ד ה ו ז ח ט י כ ל ם נ ס ע פ צ ק ר ש ת
 ת ש ר ק צ פ ע ס נ ם ל כ י ט ח ו ז ה ד ג ב א