# Основные сведения

Математическая модель

$$E(x) = ((m-1)x + (m-1)) \operatorname{mod} m$$

$$E(x) = ((m-1)(x+1)) \operatorname{mod} m$$

$$D(x) = E(x)$$

$$\mathbf{x}$$

Авторы

# Криптоанализ

#### Источники

- 1. Leuchter, Mark. "Jeremiah's 70-Year Prophecy and the ימק בל/ךשש 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. ¬шш) является криптограммой слова «Вавилон» (ивр. сст (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 (אתבש) составлено из букв «алеф» к, «тав» л, «бет» д, «шин» у. 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	Х	алеф
шин	w	ב	бет
реш	٦	ړ	гимель
куф	ק	7	далет
цади	Z	ה	xe
пе	Đ	١	вав
аин	ע	7	заин
самех	۵	Π	хет
нун	נ	ט	тет
мем	מ	,	йуд
ламед	ל	٥	каф
каф	כ	ל	ламед
йуд	,	מ	мем
тет	ט	נ	нун
хет	Π	٥	самех
заин	7	ע	аин
вав	١	Ð	пе
xe	ה	צ	цади
далет	7	7	куф
гимель	٦	٦	реш
бет	ב	w	шин
алеф	х	ת	тав

### Программная реализация

#### 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__':
```

Результат:

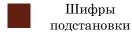
TVVPH ULI TVVPH GEEKS FOR GEEKS

main()

# Атбаш (ивр. אתבש )

Моноалфавитные шифры подстановки

Группа 1





Моноалфавитные шифры подстановки



Аффинные шифры



# The ATBASH Cipher

אבג רה ו וחטיכל מנסעפצקרשת תשר קצפ עסנמל כיטחוו הרגב א