

# Методы защиты информации

## Личный опыт

## Шифрование бывает двух видов :

Симметричное шифрование - метод шифрования , когда используют один и тот же ключ для зашифровывания информации и для ее расшифровывания.

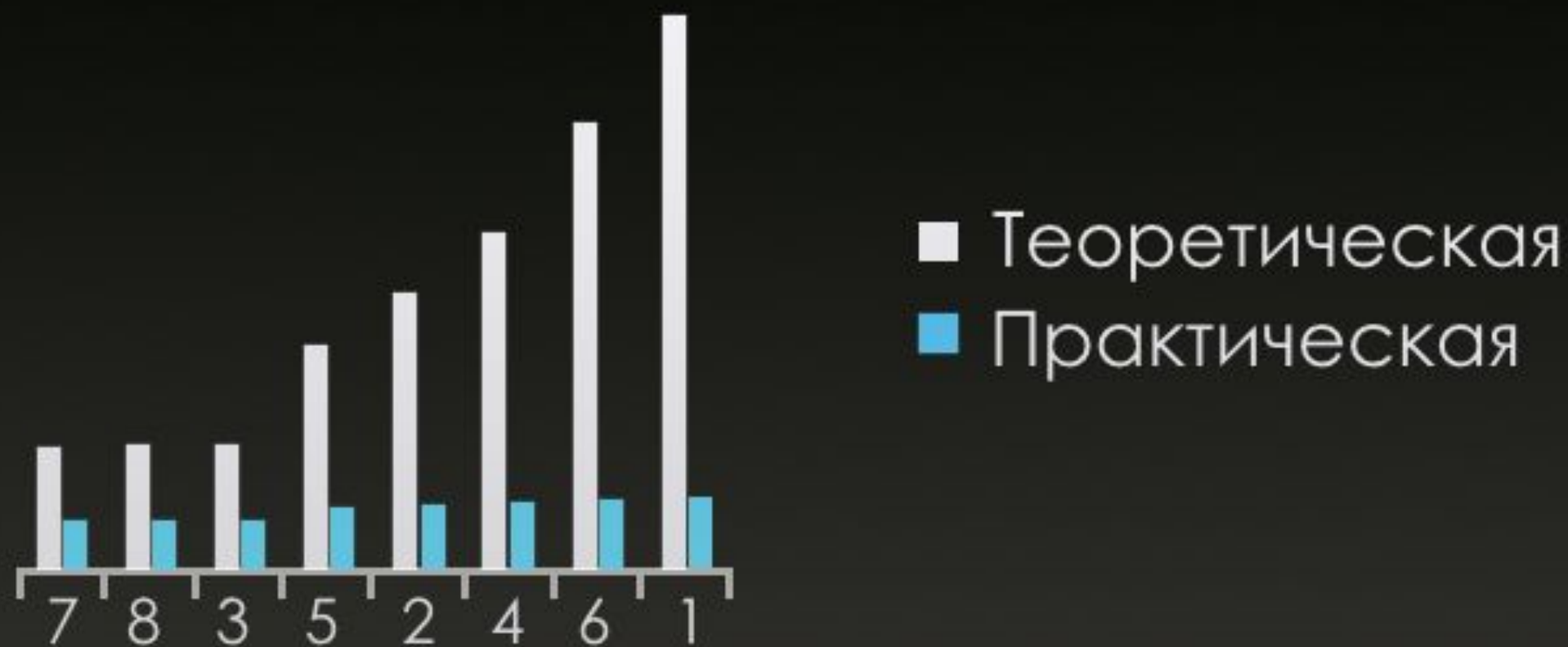
Асимметричное шифрование – метод шифрования, когда используют два ключа - один для зашифровывания, другой для расшифровывания.

Для шифрования какой-либо информации, обязательно нужен ключ.

## Популярные алгоритмы шифрования:

- 1) AES (Rijndael)
- 2) ГОСТ 28147-8
- 3) Blowfish
- 4) DES
- 5) RSA
- 6) CAST
- 7) XOR
- 8) Twofish

# Эффективность реализации различных криптографических алгоритмов



## Вывод

Для лучшей защиты информации , я предлагаю :

Использовать AES шифрование с 256 битным ключом  
+ дополнительно использовать Twofish алгоритм ,  
т.к на подбор ключа уйдёт много времени .

\* 77,000,000,000,000,000,000,000 лет.

Спасибо!