

Аннотация

Среда программирования: Visual Studio Code

Язык программирования: Python 3

Процедуры для запуска программы: \$ python3 <имя_файла>.py

Пословица-тест: Красивыми словами пастернак не помаслишь

Текст для проверки работы: Вот пример статьи на тысячу символов. Это достаточно маленький текст, оптимально подходящий для карточек товаров в интернет или магазинах или для небольших информационных публикаций. В таком тексте редко бывает более двух или трёх абзацев и обычно один подзаголовок. Но можно и без него. На тысячу символов рекомендовано использовать один или два ключа и одну картину. Текст на тысячу символов это сколько примерно слов? Статистика показывает, что тысяча включает в себя сто пятьдесят или двести слов средней величины. Но, если злоупотреблять предлогами, союзами и другими частями речи на один или два символа, то количество слов неизменно возрастает. В копирайтерской деятельности принято считать тысячи с пробелами или без. Учет пробелов увеличивает объем текста примерно на сто или двести символов именно столько раз мы разделяем слова свободным пространством. Считать пробелы заказчики не любят, так как это пустое место. Однако некоторые фирмы и биржи видят справедливым ставить стоимость за тысячу символов с пробелами, считая последние важным элементом качественного восприятия. Согласитесь, читать слитный текст без единого пропуска, никто не будет. Но большинству нужна цена за тысячу знаков без пробелов.

Интерфейс: #в разработке#

ОБМЕН КЛЮЧАМИ

- Обмен ключами по алгоритму Diffie–Hellman

Код программы:

```
def main():
    a = int(input("Введите число a: "))
    n = int(input("Введите число n, n должно быть больше a: "))
    ka = int(input("Введите число ka: "))
    Ya = a**ka % n
    print ("Ваш Ya = ", Ya)
    Yb = int(input("Введите число Yb, которое прислал собеседник: "))
    K = (a**(Ya*Yb))%n
    print ("Ваш общий ключ: ", K)

if __name__ == "__main__":
    main()
```

Тестирование:

```
PS C:\Users\xiaomi\Desktop\cryptography_ciphers\lab_11\dh> python3 dh.py
Введите число a: 5
Введите число n, n должно быть больше a: 9
Введите число ka: 20
Ваш Ya = 7
Введите число Yb, которое прислал собеседник: 15
Ваш общий ключ: 8
```