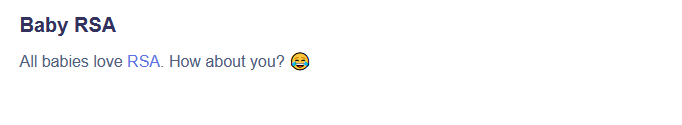
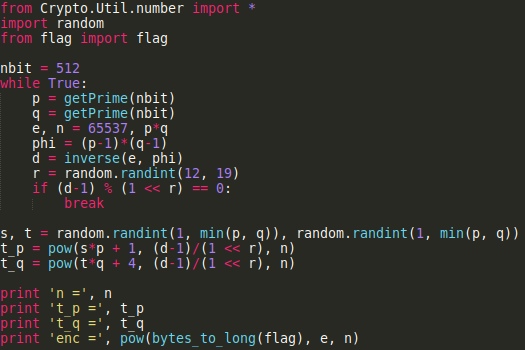
**Task**

****

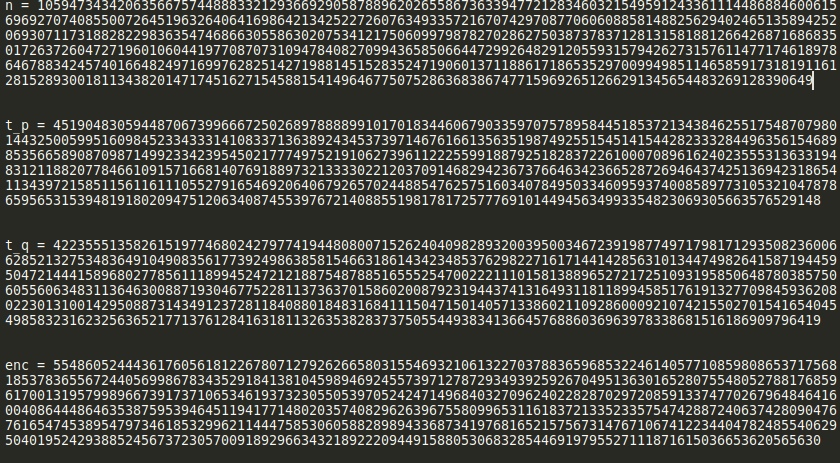
**Solution**

После распаковки приложенного архива получаем 2 файла: baby\_rsa.py и output.txt.

Первый содержит реализацию алгоритма RSA с выводом n, зашифрованного сообщения, а также некоторых дополнительных значений t\_p и t\_q:



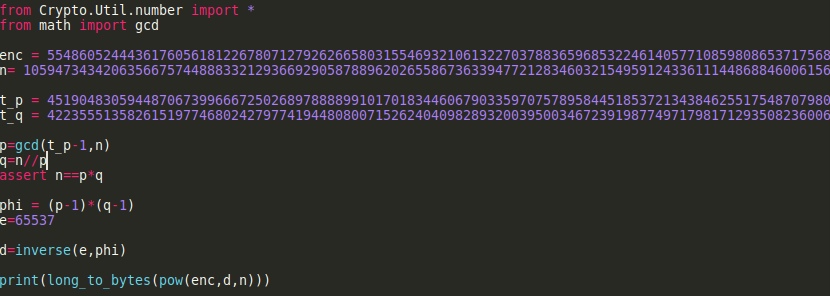
Output.txt содержит эти выводы для искомого флага:



Исходя из способа расчёта значения *t\_p*, можно сделать вывод о том, что *t\_p-1* делиться на *p*. *n* также делится на *p*, так как *n=p\*q*, следовательно, мы можем найти *p*, как НОД между *t\_p* и *n*.

После нахождения *p* с помощью функции *gcd()*, находим *q, phi* и *d*, с помощью которого расшифровываем сообщение.

Скрипт:



Результат:

https://sun9-8.userapi.com/3VJPwY-Nw-LXIz4wm3xRR-FJ47EeRP3EE1ASqA/ky-mv9DOKvU.jpg

**Флаг:**

ASIS{baby\_\_\_RSA\_\_\_f0r\_W4rM\_uP}