## **分析与求解**

1. 根据题设，得到以下关系：

gift=lcm((p−1),(q−1))      gmpy2.lcm求最小公倍数gift=lcm((p−1),(q−1))      gmpy2.lcm求最小公倍数

n=p∗qn=p∗q

c=me mod nc=me mod n

1. 尝试直接将nn[分解](http://www.factordb.com/index.php" \t "https://www.cnblogs.com/vict0r/p/_blank)，无果。giftgift可以分解为

gift = 8 \* 11 \* 97 \* 9601 \* 26057167557433418766727399341516665922795024485718296827775927226598694152064298989740080209950805089159979564300359652085874056289167084685303669920341402021998569251561854184586912056788515477034039863935829715784489123437315798902409373317578932823488000322365526936227790036245092665207472438169954702748857842187299166976320465787901470261800372425345547560303561842376571751928531743505412746346436473024093575122041981043859827477404447458211341273671273506575488189374812217939984540494633634622813448773520886788206836310702581026986331011987344147901504555559723572981774237352245997308787165273589

1. 此外，根据我们小学五年级学过的知识，有：

最小公倍数(p,q) ∗ 最大公因数(p,q) = p∗q最小公倍数(p,q) ∗ 最大公因数(p,q) = p∗q

所以对于giftgift，我们有：

gift∗gcd(p−1,q−1)=(p−1)∗(q−1)=ϕ(n)gift∗gcd(p−1,q−1)=(p−1)∗(q−1)=ϕ(n)

1. 我们可以求出giftgift的二进制位数为2045

求法：**print(len(bin(gift)[2:]))**

1. 同时知道ϕ(n)=(p−1)∗(q−1)ϕ(n)=(p−1)∗(q−1)的位数为2048，因此gcd(p−1,q−1)gcd(p−1,q−1)占3bits，因此最大公因数的范围（十进制）为[4,8][4,8]
2. 在此范围内遍历最大公因数的值，然后与最小公倍数相乘得到ϕ(n)ϕ(n)的值，再有e, ϕ(n)e, ϕ(n)求得dd，然后就可求得明文
3. 但是这个时候发现一个[问题](https://blog.csdn.net/weixin_44110537/article/details/107592484" \t "https://www.cnblogs.com/vict0r/p/_blank)：ee值不是素数，分解可以得到

e=2∗27361e=2∗27361

所以，在计算时，需要将原先的ee值除以2才可以进行常规的解密操作。  
8. 值的变化可通过以下表达式体现

c=(m2)e2mod nc=(m2)e2mod n

所以解出的明文需要开根号再转为字节流