实验报告4

陈旻 SA18225036

1 具体思路

分解第一个和第二个数时安装题目里的公式做就行

$$A = \lfloor \sqrt{N} \rfloor$$

由于A是p和q的中点，所以存在一个x使得$p = A - x$以及$q = A + x$。又因为$N = pq = (A - x)(A + x) = A^2 - x^2$，因此$x = \sqrt{A^2 - N}$。现在，根据$x$和$A$，你可以找到$N$的$p$和$q$。于是已经分解出了$N$。

要注意的是gmpy2模块的精度要取得足够大，否则sqrt()函数的参数为mpfr型时，即使该参数的平方根也是整数，得出的结果可能是很趋近那个平方根的浮点数，导致最终结果错误，所以计算x值时要注意确认设定的精度可以得到正确的x。程序中精度取的是1200(gmpy2.get_context().precision = 1200)。

分解第三个数时，要注意$A = (3p + 2q)/2$，即A是3p和2q的中点，并且3p是奇数，2q是偶数，所以A一定不是整数，并且因为除以2，A的小数部分是0。通过公式的推导，可以知道 A和$\sqrt{6N}$差距小于$1/(8 * \sqrt{6})$，所以A的值等于 $\lfloor \sqrt{6N} \rfloor - 0.5$,取得A值后，计算$x = \sqrt{a^2 - 6N}$，计算出x后，A-x可能为3p或2q，判断一下A-x是否被3除尽就可确定。

最后一个问题是RSA解密，通过对N的分解因式可以计算 ，然后可以计算出私钥，解密的结果是很长一串数，将其转换成16进制编码的字符串，decode('hex')以后就是PKCS1编码后的明文，分隔符之后的就是原始信息。