M10915027 石成峰 HW2

[COM]

1. 用輾轉相除法求出n1和n2的質因數後分解n1。
2. 知道e和n的p, q後用RSA的公式求出私鑰d。
3. 用d解密c得出flag。

[STE]

1. 從generate.py中可以得知明文m的高位元皆為ff，加密用的e只有3。
2. 將這些資訊帶入sage的求解多項式中解出m後即可得出flag。

[RSA]

1. 從generate.py中可以得知質因數p與n的關係大約為12\*p^3=n。
2. 將p初值設為pow(n / 12, 1 / 3)。
3. 再由原本產生n的方式產生出假設的n。
4. 計算誤差後除掉p ^ 2當作預計誤差delta。
5. 不停將p加上0.01delta迭代到完全等於n及可得出p並分解n。
6. 使用RSA的公式求出私鑰後解密得出flag。

[LSB]

1. 將密文乘上 3^ 65537後送入解密。
2. 透過餘數的方式縮減明文的可能範圍。
3. 不停重複乘上3^65537，將明文的可能範圍不斷除3。
4. 最終得出唯一可能的明文及可得到flag。