Writeup

首先先求n，已知：

$$(enc+d)^{e_1} \equiv \ c_1 \ mod \ n$$
$$(enc+d)^{2e_1} \equiv \ c_2 \ mod \ n$$
$$(enc+d)^{3e_1} \equiv \ c_3 \ mod \ n$$

根据等差的性质：

$$c_1 * c_3 - c_2^2 = k_1 n$$
$$c_2 - c_1^2 = k_2 n$$

求gcd即可得n

求得n后：

$$c_4 \equiv \ (enc+2d)^D \ mod \ n$$
$$c_4^{e_2} \equiv \ enc+2d \ mod \ n$$
$$(c_4^{e_2} - 2d)^{e_2} \equiv \ m \ mod \ n$$

又

$$c_5 \equiv d^5 \ mod \ n$$

于是可以把上面的式子展开，得到关于d的四次方程，然后对这个四次方程作2，3，4次幂，加上本身一共四个方程，把d消掉得到关于m的四次方程，而m很小，用coppersmith求小值根得到flag