這種題目通過某種方法提供一個解密機，但是只會返回解密後明文的最後一比特位，既返回解密出明文的奇偶。我們可以用 $log(N)$ 的覆雜度確定 m，舉例如下：

1. 我們可以得到 n, e, c，`c` 通常是 `encflag`，要注意到 n 是奇數，因為他是兩個質數相乘而來。
2. 我們可以傳入 c，`server` 算出 $m = c^d \bmod n$ 並返回 m 的奇偶性。

`server` 計算出 $m' = (c * 2^e)^d \bmod n = 2m \bmod n$，

1. 如果 $2m < n$，那麼 m' 會是個偶數
2. 如果 $2m \geq n$，那麼 $m' = 2m - n$，那麼 m' 會是個奇數。

我們現在已經可以通過一次查詢把 m 的範圍縮小到了 $n/2$，我們是否可以通過二分法確定 m 的準確的值？以數學歸納法的思想，我們現在已經完成了第一步的證明，現在要完成的是對之後部分的證明。

假設現在已經把m的範圍確定到了 $\frac{xn}{2^i} \leqslant m < \frac{(x+1)n}{2^i}$，那麼下面我們查詢$c * 2^{(i+1)e} \bmod n$，服務器會返回給我們 $m' = 2^{(i+1)} m \bmod n = 2^{(i+1)} m - kn$，那麼：

$$0 \leqslant 2^{(i+1)} m - kn < n$$
$$\frac{kn}{2^{(i+1)}} \leqslant m < \frac{(k+1)n}{2^{(i+1)}}$$

並且考慮到初始條件：

$$\frac{xn}{2^i} \leqslant m < \frac{(x+1)n}{2^i}$$
$$\frac{(2x)n}{2^{(i+1)}} \leqslant m < \frac{(2x+2)n}{2^{(i+1)}}$$

因為 x 和 k 都是整數，要滿足原先的條件， k 只能取 $2x$ 或 $(2x+1)$。

$2^{(i+1)}$ 是偶數， n 是奇數。所以當 m' 是奇數的時候， $2^{(i+1)} - kn$ 是奇數， k 必然是奇數；反之，如果 $2^{(i+1)} - kn$ 是偶數， k 必然是偶數。

如果 k 是奇數， k 只能取 $(2x+1)$，m 被約束到 $\frac{(2x+1)n}{2^{(i+1)}} \leqslant m < \frac{(2x+2)n}{2^{(i+1)}}$；

如果 k 是偶數， k 只能取 $2x$，m 被約束到 $\frac{(2x)n}{2^{(i+1)}} \leqslant m < \frac{(2x+1)n}{2^{(i+1)}}$。

這樣二分下去直到上下界只差小於 `1.`