M10915027 石成峰 HW1

[POA]

1. 每次只丟2段密文進行解密，逐一更改前面那段密文的每個byte使後面解密完能通過測試。
2. 最終後面那段解密完的明文與前密的密文進行XOR之後會得到80開頭後面皆為0的明文以通過測試。
3. 便可直接從前一段已知的密文推得後一段解密後的明文，即便不知道加密及解密方式。
4. 從後往前將每一段密文依上述方法求出明文，即可得到flag。

[COR]

1. 分析原始碼可以發現3個LFSR的狀態轉換是獨立的。
2. Getbit最後輸出的真值表可以分析出輸出狀態與l2和l3有75%的相關性。
3. 在l2和l3搜尋0~65535當作初始init時輸出會與目標有65~85%相關度的初始值。
4. 搜尋l1 0~65535已及第三部過濾過的l2和l3初始值試圖找出完全符合輸出序列的出值。
5. 非常幸運可以找到一組初值完全符合輸出，轉成字元後得flag。