2023 암호분석경진대회

3번문제

RSA 복호화 과정은 암호문 C와 개인키 d, 공개키 n에 대해 $C^d \bmod n$의 연산을 통해 평문 M을 계산한다.
대학원생인 김철수는 1024-bit 공개키 n과 암호문 C에 대한 복호화 연산을 수행하여 정상적인 평문 M을 다음과 같이 얻을 수 있었다.

C = 37401583471056104381034405113413 5

n = 98639350158287747956171614024858003106737929785723376047985588489903225031675238942280563373940905701931651170379361219551278894213021434648783114473246721338107200738833103695814346217200966617698677137725683746838186561756004241774294434212453862492176950276330700287348945941127494562176214125995218765677

M = 86843456369086866983830587539305158453762160744919050956253860389213163768459050969489741842800371583977732099203915296497845749069857544504773500146103562220031272124661691355221692794922319549625101446769098920958838190576063519649356189104686925724356580485663786964929657082417372715796601952630784727 51

하지만, 위와 같은 C, n에 대해 복호화 연산을 반복해서 160번 수행하는 도중 d의 최하위 k개의 비트를 모두 0으로 셋팅하는 오류주입 공격이 수행되었다. 160번의 복호화 연산과정에서 오류가 주입된 위치는 다음과 같다. (예를 들어, 오류가 주입된 위치가 30일 때, d의 최하위 30비트는 모두 0으로 변경되어 $C^d \bmod n$의 연산이 수행되었다.)

[5, 11, 18, 24, 30, 37, 43, 51, 57, 63, 70, 78, 84, 90, 98, 105, 112, 120, 125, 131, 137, 144, 150, 156, 161, 169, 176, 180, 187, 193, 201, 205, 212, 220, 228, 235, 239, 246, 252, 258, 265, 269, 277, 283, 290, 295, 301, 307, 311, 318, 326, 330, 337, 345, 353, 360, 365, 370, 377, 383, 389, 397, 405, 409, 413, 421, 429, 433, 441, 446, 454, 461, 468, 476, 483, 490, 497, 504, 510, 517, 524, 531, 538, 546, 551, 559, 562, 569, 577, 584, 590, 596, 599, 606, 609, 617, 624, 631, 638, 642, 648, 653, 658, 662, 670, 676, 681, 689, 693, 700, 708, 716, 723, 730, 738, 746, 753, 758, 763, 769, 778, 784, 790, 796, 804, 812, 819, 826, 831, 838, 844, 850, 858, 865, 869, 876, 883, 890, 897, 903, 910, 917, 925, 932, 939, 945, 950, 954, 959, 963, 969, 976, 983, 989, 993, 998, 1005, 1010, 1016, 1021]

오류가 주입되어 연산된 160개의 평문 값이 순차적으로 fault_message.txt에 기록되었을 때, 개인키 d를 찾으시오.