the most basic ECDLP problem, mainly in the hope that the contestants will know the basic concept of elliptic curve and the usage of sage.

Since the plaintext is very small (< 1048575), use the discrete\_log function in sage can directly solve the problem. or written some function manually. BruteForce recovery will be slow.

|  |
| --- |
| N = 2\*\*256-2\*\*32-2\*\*9-2\*\*8-2\*\*7-2\*\*6-2\*\*4-1  E = EllipticCurve(GF(N), [0, 7])  xG = 0x79be667ef9dcbbac55a06295ce870b07029bfcdb2dce28d959f2815b16f81798  yG = 0x483ada7726a3c4655da4fbfc0e1108a8fd17b448a68554199c47d08ffb10d4b8  G = E(xG,yG)  c0 = E(76950424233905085841024245566087362444302867365333079406072251240614685819574 , 85411751544372518735487392020328074286181156955764536032224435533596344295845)  c1 = E(42965775717446397624794967106656352716523975639425128723916600655527177888618 , 32441185377964242317381212165164045554672930373070033784896067179784273837186)  c2 = E(26540437977825986616280918476305280126789402372613847626897144336866973077426 , 1098483412130402123611878473773066229139054475941277138170271010492372383833)  print(hex(G.discrete\_log(c0)))  print(hex(G.discrete\_log(c1)))  print(hex(G.discrete\_log(c2)))  '''babe  ecc1  3c001''' |