task4. Crypto Кристалл эха [easy]

cryptograpty

RSA (small e)

Условие уязвимости: маленькое e & сообщение m настолько мало, что m^e (e=3 например) < n.

n = 0x23d5092f21749af51e767497449f5a469f6f56161929fc043850e6fa184f645b2cd53a6b547df1c51d31f7feb74ca98ae00087f6c95323e09259cf6698c7bb4175342b033cc005f020f3194dad8e90d9

e = 3

c = 0x8d3ed016bb161359fa7907ab2f5aff90a27f32060e877c0efae498e858d09901c0dd8de408d2139cf5f7b978fd16103891f6480e5dac5c4e2b11e673f02a28975ccab1d83cb3459b1d477160965

решение:

m = gmpy2.iroot(c, e)[0]

print(bytes.fromhex(hex(m)[2:]).decode())

SSU{1ts\_sm4ll\_e\_cub3\_r00t}