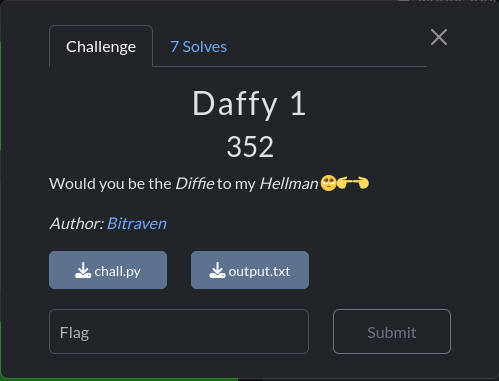
**Daffy 1**



Like daffy 2 same deal use this python script below copy paste and then execute:

from sympy.ntheory import discrete\_log

from Crypto.Util.number import long\_to\_bytes

from Crypto.Cipher import AES

from Crypto.Util.Padding import pad, unpad

# Given values

p = 335828589845279

g = 11

A = 105184740584178

B = 257292025029694

enc = bytes.fromhex('ab624c529eb96fe0b9ece0d7e646c7d6e9e6e49f026d579d42f1a85b7ec67525c620c4d5a2124ae57e638eef84fbf985')

# Calculate private\_key\_b using discrete logarithm

private\_key\_b = discrete\_log(p, B, g)

# Compute the shared secret S

S = pow(A, private\_key\_b, p)

# Derive the AES key from the shared secret S

key = pad(long\_to\_bytes(S), 16)[:16]

# Decrypt the ciphertext using the shared secret S

cipher = AES.new(key, AES.MODE\_ECB)

decrypted = cipher.decrypt(enc)

try:

    decrypted = unpad(decrypted, 16)

    print(decrypted.decode())

except ValueError:

    print("Error: Incorrect padding.")

boooooooooommmmmmmmmm soldier here’s your flag ☺

