S & S

生活、學習、紀錄、分享

Pico2017ctf_ComputeRSA – 50 PTS

題目：RSA encryption/decryption is based on a formula that anyone can find and use, as long as they know the values to plug in. Given the encrypted number 150815, d = 1941, and N = 435979, what is the decrypted number?

這題沒有什麼特別的，就是數學運算

RSA的加密方法：

1. Obtains the recipient B's public key (n, e).先拿到收件人B的公鑰
2. Represents the plaintext message as a positive integer *m*, 1 < m < n
3. Computes the ciphertext $c = m^e \bmod n$.計算密文c
4. Sends the ciphertext *c* to B.將c寄給B

RSA的解密方法：

1. Uses his private key (n, d) to compute $m = c^d \bmod n$.用私鑰計算m
2. Extracts the plaintext from the message representative *m*.

由題幹：

m=

c=150815

d=1941

n=435979

有了公式，有了數值，接下來就只是計算的問題了，這邊使用python的數學函式：

```
> >>c=150815

>>> d=1941

>>>n=435979

>>>test = pow(c,d)

>>> answer=test%n

>>> print (answer)

133337
```

flag = 13337

Advertisements

分享此文：

Twitter Facebook G+ Google

★ 喜歡

Be the first to like this.