

Crypto-11 Секрет командного блока

Исследуя морской данж, ты находишь странный командный блок, светящийся красным светом. Рядом стоит табличка:

"Я создал этот командный блок для защиты своих самых ценных ресурсов, используя криптографический алгоритм RSA..."

На дисплее командного блока отображаются три числа:

- n (какое-то большое число)
- e (публичный ключ)
- c (зашифрованная команда)

Сможешь ли ты найти уязвимость в этой защите и активировать командный блок?

Рекомендуемые утилиты: python

Цель работы: Расшифровать сообщение и получить флаг

Критерий оценки: Предоставление правильного флага

Решение

Нам даны параметры RSA - n, e, c . Так как n мал, его можно быстро разложить на простые p и q , затем вычислить экспоненту d и расшифровать $m = c^d \pmod{n}$, получить флаг из байтов.

Вспомним основной алгоритм RSA:

- $n = p \cdot q$.
- $\phi(n) = (p - 1)(q - 1)$.
- $d \equiv e^{-1} \pmod{\phi(n)}$
- $m \equiv c^d \pmod{n}$.

Тогда этапы решения:

1. Разложить n - для маленьких n
2. Посчитать $\phi(n)$ и d .
3. Возвести c в степень d по модулю n .
4. Преобразовать число m в байты и строку - получаем флаг.

Скрипт

```
from Crypto.Util.number import long_to_bytes
from sympy.ntheory import factorint

c = 408114776764409099690169640113227
n = 2347332715134999472660100244460421
e = 65537

p, q = factorint(n).keys()
phi = (p - 1) * (q - 1)
d = pow(e, -1, phi)
m = pow(c, d, n)

print("vsosh{" + long_to_bytes(m).decode() + "}")
```

Флаг

vsosh{c0mm4nd_b10ck5}