

TetCTF 2021 - Unimplemented

Орлов Михаил, Уткин Артем

June 2023

В чем состоит наша задача?

Автор задания использовал особый вид шифрования, основанный на криптосистеме RSA, где вместо простых чисел используются гауссовы целые числа, а модуль N рассчитывается как P^2Q^2 вместо PQ . Наша задача состоит в том, чтобы воспроизвести процесс дешифрования сообщения, зашифрованного именно таким способом, имея закрытый ключ и, собственно, само сообщение.

Как мы решим задачу?

Как и в RSA, расшифровка при данном методе шифрования производится следующим образом:

- $\phi(N)$
- $d = \frac{1}{e} \bmod \phi(N)$
- $m = c^d \bmod N$

Формулу для $\phi(x)$

$$\phi(x) = p_1^{r_1-1}(p_1 - 1)p_2^{r_2-1}(p_2 - 1)\dots p_k^{r_k-1}$$

можно переписать в виде

$$\phi(x) = x(1 - \frac{1}{p_1})(1 - \frac{1}{p_2})\dots(1 - \frac{1}{p_k})$$

и тогда

$$\phi(N) = \phi(P^2 Q^2) = \phi(P^2)\phi(Q^2) = P^2(1 - \frac{1}{P})Q^2(1 - \frac{1}{Q})$$

и... это не правильно

Мы имеем дело не с простыми целыми числами, а с гауссовыми целыми числами (с мнимой частью, равной 0).

Используем функцию $\eta(\alpha) = a^2 + b^2$, где a и b - целая и мнимая части числа α соответственно. Получаем

$$\phi(x^k) = \eta(x)^k \left(1 - \frac{1}{\eta(x)}\right)$$

$$\phi(P^2) = \eta(P)^2 \left(1 - \frac{1}{\eta(P)}\right)$$

$$\phi(Q^2) = \eta(Q)^2 \left(1 - \frac{1}{\eta(Q)}\right)$$

$$\phi(N) = \phi(P^2)\phi(Q^2) = \eta(P)^2 \left(1 - \frac{1}{\eta(P)}\right) \eta(Q)^2 \left(1 - \frac{1}{\eta(Q)}\right)$$

Находим


$$\phi(N) = (P^4 - P^2)(Q^4 - Q^2)$$

А теперь напомним функцию?

Теперь, используя формулу, мы можем написать функцию дешифровки на Python

```
def decrypt(private_key, ciphertext):  
    (p, q) = private_key  
    n = (p ** 2) * (q ** 2)  
    c = Complex(  
        int.from_bytes(ciphertext[:len(ciphertext) // 2], "big"),  
        int.from_bytes(ciphertext[len(ciphertext) // 2:], "big")  
    )  
    e = 65537  
    phi = (p ** 4 - p ** 2) * (q ** 4 - q ** 2)  
    d = pow(e, -1, phi)  
    m = complex_pow(c, d, n)  
    return unpad(m.re.to_bytes((n.bit_length() + 7) // 8, "big")  
        + m.im.to_bytes((n.bit_length() + 7) // 8, "big"))
```

Программа расшифровала текст и в нем оказался флаг. результат после ввода - положительный.

 Unimplemented (TETCTF) 18 Solves • 0 Solutions


A new public key encryption algorithm is being invented, but the author is not quite sure how to implement the decryption routine correctly. Can you help him?

Challenge contributed by **NDH**

Challenge files:

- **output.txt**
- **source.py**

You have solved this challenge!

 import numpy as MT (Zh3r0 CTF V2) 5 Solves

<https://github.com/OrlovMlc/Unimplemented>