

Writeup – Secret Message

Challenge Description

We are given RSA parameters:

- $n=3233$
- $e=17$
- $c=1306$

We need to decrypt the ciphertext and find the original plaintext.

Flag format: `FLAG{plaintext}`

Step 1 – Factoring nn

RSA security depends on the difficulty of factoring nn .

Here, $n=3233$ is small, so I used an **online factorization tool**.

It gave:

$$3233 = 61 \times 53$$

Search	Sequences	Report results	Factor tables	Status	Downloads	API	Login
<div>3233</div>						<div>Factorize!</div>	
Result:							
status (2)		digits	number				
FF		4 (show)	$3233 = 53 \cdot 61$				

Step 2 – Using an RSA Calculator

Instead of calculating everything by hand, I used a simple **RSA calculator tool** where I entered:

- $p=61$
- $q=53$
- $e=17$
- $c=1306$

The tool handled the math and gave me the decrypted message:

RSA Calculator

This module demonstrates step-by-step encryption with the RSA Algorithm to ensure authenticity of message. The sender encrypt the message with its private key and the receiver decrypt with the sender's public key.

No provisions are made for high precision arithmetic, nor have the algorithms been encoded for efficiency when dealing with large numbers.

Step 1. Calculate N which is a product of two distinct prime numbers p and q

$p =$

$q =$

Calculate N $53 * 61 = 3233$

Step 2. Find $\phi(N)$ which is $(p-1) * (q-1)$

$\phi(N) =$ $(53-1) * (61-1) = 3120$

Step 3. Select e such that $\gcd(\phi(N), e) = 1$ and $1 < e < \phi(N)$

Possible Values of e

7, 11, 17, 19, 23, 29, 31, 37, 41, 43, 47, 49, 53, 59, 61, 67, 71, 73, 77, 79, 83, 89, 97, 101, 103, 107, 109, 113, 119, 121, 127, 131, 133, 137, 139, 149, 151, 157, 161, 163, 167, 173,

Enter e

Step 4. Calculate d such that $d * e \bmod \phi(N) = 1$

$d =$

Step 3 – Submitting the Flag

So the final flag is:

FLAG{1337}