BBB

defkit

November 14, 2022

Abstract

Every 5 year child in Russia knows quadratic equations. DTRUSH BBB writeup

1 Introduction

We can choose b for function $x^2 + ax + b$. We need to recover flag. As we can see, the flag encrypted many times, so we just need to receive enough data to solve crt. As you can see, we only have 5 attemps with public exponent greater than 10 and length of encrypted data is not greater than 116 bytes and the length of public modulus for every encryption is 2048 bits. Okay, let imagine, that we have 5 times encrypted flag with exponent 11, to crt we need:
$\frac{11 bitlength(flag)}{5} < 2048$
and we exactly have
$\frac{11 bitlength(flag)}{5} = 2041.6$
, so if we find the way, to encrypt flag 5 times with exponent 11, we can solve the task.

2 Way to encrypt flag with the same exponent

First step is to find such b:
$y(x) = x^2 + ax + b \ mod \ p$ and $y(11) = 11$
Its simple. We just compute $b = 11 - 11^2 - 11a \ mod \ p$.
Second step. We cannot send the same seed, but in task, $e = y(e)$ computes from 1 to 100 times, so we just need to find such seed:
$y(y(seed)) = 11$
, so seed is the root of the equation $y(seed) = A$, whereas A is the second root of equation $y(x) = 11$ and so on.