**Descripción**:

implemente RSA de la mejor manera posible, seguir todas las instrucciones y buenas prácticas ;) https://es.wikipedia.org/wiki/RSA

aunque... algo no funciona, no puedo descifrar los mensajes que cifro, algo anda mal podrías ayudarme a descifrar mi bandera?

Esto no puede ser tan fácil o ¿sí?

creo que alguien de una compañía importante ya había encontrado algo parecido.

**Writeup**:

Revisando el código fuente del reto debería ser un poco obvio la mala implementación de la generación de llaves. Una condición importante en RSA es que el valor de la función de Euler del modulo debe ser coprimo al exponente público, en otras palabras, que el máximo común divisor entre **phi(n)** y **e** sea igual a 1. Cuando esta condición no se cumple simplemente no se podrá recuperar la llave privada incluso teniendo los valores factorizados de N.

Texto

Descripción generada automáticamente con confianza media

A pesar de poseer los dos factores primos **P** y **Q** no es posible recuperar la llave privada ya que esta no cumplirá con la propiedad necesaria para invertir la exponenciación con el exponente público.

Esta vulnerabilidad o “bug” en la generación de llaves RSA fue descubierta por Microsoft y esta afectaba a ciertas versiones de Windows 10. Los detalles de esta vulnerabilidad y los algoritmos para recuperar un texto claro cifrado pueden ser consultados en esta publicación oficial: **https://eprint.iacr.org/2020/1059.pdf**

El autor igual tiene sus propias implementaciones, y pueden ser encontradas en su repositorio oficial: **https://github.com/danshumow-msft/FixBadRsaEncryption**

Este reto pude ser resuelto usando implementaciones propias o reutilizando los scripts del propio autor.

Con los scripts se puede resolver el reto de forma relativamente facil solo se requiere realizar un par de modificaciones para que se encuentre la flag:

Texto

Descripción generada automáticamente

Ejecutando el script modificado de RSAMath se puede recuperar la flag.

Texto

Descripción generada automáticamente

La dificultad del reto esta en identificar la mala implementación de RSA en el código fuente, una vez identificada es necesario investigar este bug para llegar a la publicación oficial de Microsoft donde está la teoría necesaria para entender como usar los scripts del autor.