# LABORATORIO #6

**Tema:** Cifrado asimétrico.

**Fecha de Entrega:** 26 de Abril a las 23:59 horas

**Objetivos:**

- Familiarizarse con algoritmos de cifrado asimétricos.
- Aplicar y ejercitar el intercambio de llaves de forma segura.

**Serie Única:**

El cliente quedó satisfecho con los algoritmos Caesar, pero teme que transmitir la palabra clave de Caesar sea inseguro. Por lo que le pide que se le pide transmitir la clave de forma segura. Para ello debe crear el API "/cipher/caesar2/" el cual deberá utilizar uno de estos algoritmos.

- RSA
- Diffie-Hellman

En ambos casos, debe generar una llave pública que va a compartir y almacenar la llave privada. Debe crear un API para intercambiar las llaves "/cipher/getPublicKey", este API devolverá la llave pública y qué algoritmo se estará usando.

- cipher: "rsa" | "diffie"
- key: <la llave pública>

Para el caso que decidan usar Diffie-Hellman, se acordará usar g = 43 y p = 107. Adicional, deberá enviar su llave como un parámetro.

- key: <su llave pública>

**Entregable:**

Enlace hacia github ( https://github.com/ ) en donde contenga la aplicación. Se estará revisando que dentro del manejador de versiones existan varios *commits* y que no se suba solamente la versión final.