# RSA

Canek García (kaan.ek@ciencias.unam.mx)

# Proyecto 2

# Especificaciones:

Elaborar **un** programa con **tres métodos principales**, utilizando el criptosistema RSA:

1. Uno método que **genere** las llaves: pública y privada.
2. Otro método que **cifre** utilizando las llaves generadas en el punto 1.
3. Otro método que **descifre**, utilizando las llaves generadas en el punto 1.
4. Pueden agregar todos los métodos auxiliares que ustedes requieran.

- La función relacionada con **generar** las llaves, deberá buscar números primos primos **p** y **q** distintos y aleatorios de al menos **100 dígitos**. (en clase hemos utilizado tipos de datos BigInteger que son capaces de manipular estos números).
- La función relacionada con **cifrado**, puede recibir como parámetros **N** y **e** (generado en el punto anterior) y el texto que se va a cifrar **m**. (Aquí pueden utilizar estrategias de ustedes para el manejo del texto o pueden transformar el texto a bytes como se vio en clase).
- La función relacionada con **descifrado**, puede recibir como parámetros **N**, **d** y el **texto cifrado** en el punto anterior.
- Recuerden incluir un **método main** (método principal del programa) con pruebas a estas funciones e imprimir en pantalla el texto en claro después de aplicar el algoritmo de descifrado.

# Notas adicionales

El programa debe ser entregado en un lenguaje **distinto** a Java (puede ser Python o C/C++).

Desarrollar el proyecto en equipos de dos integrantes (**que no se pueden repetir en proyectos futuros**). **NO SE RECIBIRÁN PROYECTOS INDIVIDUALES**.

La entrega del código es el día **8 de mayo de 2019**.

El proyecto debe ser enviado por **ambos** integrantes del equipo a través de la plataforma **ClassRoom**. (sin importar que se duplique la entrega, lo importante es que la entrega este registrada por ambos)

Documentar el código fuente de **todos** los métodos e incluir el **nombre completo** de ambos integrantes en el método **main** del programa.