PONTIFICIA UNIVERSIDAD CATOLICA DE CHILE
ESCUELA DE INGENIERIA
DEPARTAMENTO DE CIENCIA DE LA COMPUTACION

Criptografía y Seguridad Computacional - IIC3253
Ayudantía 7
Alexander Pinto

RSA

1. Realice una demostración práctica del protocolo RSA, para ello considere $P = 29$, $Q = 37$ y $m = 125$.

2. Realice una demostración práctica del protocolo RSA, para ello considere:

   $P = 113863597804193638684746233303866275862959799351116319454932839076728438946896147861014045230382038476640030287985809455541219549331656514489547597100776866463781814271673557022224794131215064237956990930271588711457443015898310055178700526009643888726738585998120562566732806649886086397912653034050178893859$

   $Q = 115838909791943748922987753851050334560193343608838943167465762721872484238907283305609260452195433132247935218033024924981579405051273360371753983885753654957234722064446587754445946080621943088160497578956151867063126988652321672161448439688550488904372167035366626051841175064590746743483812434310620662793$

   $m = 123456789987654321$.

   ¿Qué inconvenientes espera encontrar en su demostración?

3. Una aplicación práctica de la criptografía asimétrica son las firmas digitales. La idea de una firma digital es dar autenticidad a un mensaje o documento. Para ello, un usuario A utiliza su clave privada para "firmar" un documento m, y cualquier otro usuario puede verificar que este documento realmente fue firmado por A utilizando la clave pública de A. En particular, en el protocolo de criptografía RSA se cumple la propiedad $m = Enc(P_A, Dec(S_A, m))$, útil para esta aplicación. Demuestre esta propiedad.

4. Investigue acerca del concepto de cifrado homomórfico. Luego demuestre que el protocolo de criptografía RSA sin *padding* es homomórfica en la multiplicación.