



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:

$P = 1138635978041936386847462333038662758629597993511163194549328390767284389468$
 $961478610140452303820384766400302879858094555412195493316565144895475971007768664$
 $637818142716735570222247941312150642379569909302715887114574430158983100551787005$
 $26009643888726738585998120562566732806649886086397912653034050178893859$

$Q = 1158389097919437489229877538510503345601933436088389431674657627218724842389$
 $072833056092604521954331322479352180330249249815794050512733603717539838857536549$
 $572347220644465877544459460806219430881604975789561518670631269886523216721614484$
 $39688550488904372167035366626051841175064590746743483812434310620662793$

$m = 123456789987654321$.

¿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 es homomórfico en la multiplicación.