

## Pasamos el mensaje y las claves por el RSA

```
Console X
<terminated> RsaEcdsaInteractive [Java Application] C:\Users\niels\p2\pool\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64_22.0.2.v20240802-1626\jre\bin\javaw.exe (
== RSA / ECDSA interactivo ==
Elija la operación:
  1 - RSA cifrar/descifrar (RSA/OAEP SHA-256)
  2 - ECDSA firmar/verificar (secp256r1 / SHA256withECDSA)
> 1

--- RSA: cifrar/descifrar (OAEP SHA-256) ---
¿Deseas GENERAR claves nuevas o PEGAR claves existentes?
  G - Generar
  P - Pegar claves en Base64
> p

Introduce la clave pública RSA en Base64 (X.509). Si no deseas proporcionarla deja en blanco y pulsa ENTER:
(Pega el texto, luego pulsa ENTER y otra línea vacía para terminar.)
MIIBIjANBgkqhkiG9w0BAQEFAAOCAQ8AMIIBCgKCAQEA1pH50EnwAYrncaYISFQE3qYyx331ZkRI8mg17CWGvJJGQPyhccY9zXTpy05SAglpsd0TGwed5g9qC12pvRcvtgYwnZ

Clave pública cargada.

Introduce la clave privada RSA en Base64 (PKCS#8). Si no deseas proporcionarla deja en blanco y pulsa ENTER:
(Pega el texto, luego pulsa ENTER y otra línea vacía para terminar.)
MIIEvQIBADANBgkqhkiG9w0BAQEFAASCBCcwggSjAgEAAoIBAQCWkdLQSFABiudxpghIVATepjLHfeVmREgGaCXsJYa8kkZA/KFxxj3Nd0nI71ICDwmx3RMBB53mD2oLXam9Fy

Clave privada cargada.

¿Qué quieres hacer?
  1 - Cifrar (necesita la clave pública)
  2 - Descifrar (necesita la clave privada)
> 2

Introduce el texto cifrado en Base64 (RSA/OAEP):
(Pega el texto, luego pulsa ENTER y otra línea vacía para terminar.)
ISQ/bh1jHc67OXTLQnt45yhNAQLj2kxLC8smCqab2oZhmkTQ+JjPkFHBW2tQXw10DUPKz0wIqfX3r7yM4YVoaqrkWEcX1effevq/KzEaLdGR/3Tq6YTcBBR3dJXc0tqHB9uJKn

Descifrado (UTF-8):
r1/gU0rQcuV3k6Wk+n81WyYveV9BCs0adnrrc3z47duIv+S0Yx3SkIDhLL1U4jQdTNzt9d30tiGdSLM/RtLbqrxXWYwGxcQnDd10
```

## El resultado que nos da el RSA lo metemos en el AES y nos da el mensaje final

```
Console X
<terminated> AesGcmDemo [Java Application] C:\Users\niels\p2\pool\plugins\org.eclipse.justj.openjdk.hotspot.jre.full.win32.x86_64_22.0.2.v20240802-162
Original: Esto es un mensaje cifrado
Cifrado (Base64) generado: v03mWQuVZaAinPag+H8nTjk40BxHHMwaZnyx6b7aWo/zF5/yfxCAeg86

Pega aquí un mensaje cifrado en Base64 para descifrar (o deja vacío para usar el generado arriba) y pulsa ENTER:
r1/gU0rQcuV3k6Wk+n81WyYveV9BCs0adnrrc3z47duIv+S0Yx3SkIDhLL1U4jQdTNzt9d30tiGdSLM/RtLbqrxXWYwGxcQnDd10
Usando el Base64 introducido por el usuario.
Descifrado: Tarea de asignatura optativa, felicidades por su descifrado
```