Cifrar y descifrar con clave clave secreta AES que se ha transmitido mediante cifrado asimetrico RSA en Java

```
import java.security.*;
import javax.crypto.*;
public class AesRsa {
        public static void main(String args[]) {
                try {
                        // SE CREA EL PAR DE CLAVES pública y
privada
                                KeyPairGenerator keyGen =
KeyPairGenerator.getInstance("RSA");
                        keyGen.initialize (1024);
                                        KeyPair  par  =
keyGen.generateKeyPair();
                                    PrivateKey clavepriv =
par.getPrivate();
                        PublicKey clavepub = par.getPublic();
                        // SE CREA LA CLAVE SECRETA AES
                                        KeyGenerator  kg  =
KeyGenerator.getInstance("AES");
                        kg.init (128);
                                SecretKey clavesecreta =
kg.generateKey();
                        // SE ENVUELVE LA CLAVE SECRETA CON LA
RSA PÚBLICA
                                                Cipher  c  =
Cipher.getInstance("RSA/ECB/PKCS1Padding");
                        c.init(Cipher.WRAP_MODE, clavepub);
                                  byte claveenvuelta[] =
c.wrap(clavesecreta);
                        // CIFRAMOS TEXTO CON LA CLAVE SECRETA
                                                        c  =
Cipher.getInstance("AES/ECB/PKCS5Padding");
                                c.init(Cipher.ENCRYPT_MODE,
```

```
clavesecreta);
                        byte textoPlano[] = "Esto es un Texto
Plano".getBytes();
                                    byte textoCifrado[] =
c.doFinal(textoPlano);
                         System.out.println("Cifrado: "+ new
String(textoCifrado));
                        // SE DESENVUELVE LA CLAVE SECRETA CON
LA CLAVE RSA PRIVADA
                                                Cipher c2 =
Cipher.getInstance("RSA/ECB/PKCS1Padding");
                            c2.init(Cipher.UNWRAP_MODE,
clavepriv);
                                    Key clavedesenvuelta=
c2.unwrap(claveenvuelta, "AES", Cipher.SECRET_KEY);
                         // DESCIFRAMOS TEXTO CON LA CLAVE
DESENVUELTA
                                                        c2 =
Cipher.getInstance("AES/ECB/PKCS5Padding");
                            c2.init(Cipher.DECRYPT_MODE,
clavedesenvuelta);
                                    byte desencriptado[] =
c2.doFinal(textoCifrado);
                        System.out.println("Descifrado: "+ new
String(desencriptado));

                } catch (Exception e) {
                        e.printStackTrace();
                }
        }
}
```