

# Ejercicio Primer Parcial Practic...



**Juandf03**



**Seguridad de la Información**



**3º Grado en Ingeniería Informática**



**Escuela Técnica Superior de Ingeniería Informática  
Universidad de Málaga**



La mejor escuela de negocios en energía, sostenibilidad y medio ambiente de España.

Más información  
[www.eoi.es](http://www.eoi.es)

Formamos  
**talento** para un futuro  
**Sostenible**



**100% Empleabilidad**



**Modalidad: Presencial u online**



**Programa de Becas,  
Bonificaciones y Descuentos**

24/10/23, 13:21

PP1 - Subgrupo A1 (página 15 de 15)



campusvirtual  
E.T.S. de Ingeniería Informática



[EVL](#) | [Aulas TIC](#) | [Programación Docente](#) | [Idioma](#) | [Contacta](#)

[UMA](#) / [CV](#) / [E.T.S. de Ingeniería Informática](#) / [Mis asignaturas en este Centro](#) / [Curso académico 2023-2024](#)

/ [Grado en Ingeniería Informática. Plan 2010](#)

/ [Seguridad de la Información \(2023-24, Grado en Ingeniería Informática. Plan 2010 Grupos A,B y Grado en Matemáticas + Ingeniería Informática. Plan 2019 Grupos A,B\)](#)

/ [Exámenes teóricos / prácticos](#) / [PP1 - Subgrupo A1](#)

### Pregunta 15

No respondida aún

Valor: 1,00

Sea el siguiente código, asumiendo que los elementos utilizados han sido definidos anteriormente, indica si es correcto o no, y la razón por la que es correcto / incorrecto.

```
# Paso 2) T->B: KBT(K1, Nonce_Replay) en AES-GCM
```

```
cifrado = socket.recibir()
```

```
cifrado_mac = socket.recibir()
```

```
cifrado_nonce = socket.recibir()
```

```
# El método descifrar_K1_Nonce obtiene k1 (clave simétrica) y t_nonce_destino (campo de defensa contra ataques replay) a partir de la información enviada por T
k1, t_nonce_destino = descifrar_K1_Nonce(cifrado, cifrado_mac, cifrado_nonce)
```

```
if (cifrado_nonce != t_nonce_destino):
```

```
    exit()
```



◀ [Pertenezco al Grupo A1 para los parciales prácticos](#)

[Saltar a...](#)

[Tema 1 - Fundamentos de Seguridad ▶](#)

**X**  
**SIBUYA**  
URBANSUSHIBAR

Hay rollos y rollos... Me vas a comparar tu rollo de ayer  
con un Hot Roll, claramente el sushi está más bueno

HAZ CLIC PARA HACER TU

**RESERVA**



WUOLAH