Ejercicio Primer Parcial Practic...

Juandf03

Seguridad de la Información

3º Grado en Ingeniería Informática

Escuela Técnica Superior de Ingeniería Informática
Universidad de Málaga

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 ►