UNIVERSIDAD DE GRANADA

FACULTAD DE CIENCIAS

**Propuesta TFG.** Curso 2026/2027

**GRADO:** Grado en Matemáticas

**CÓDIGO DEL TFG:** 270-010-2026/2027

## 1. DATOS BÁSICOS DEL TFG:

**Título:** Nociones de seguridad en Criptografía

**Descripción general (**resumen y metodología):

Históricamente, la seguridad en un criptosistema estába ligada a la unidireccionalidad, invertir una función criptográfica era "computacionalmente" difícil sin el conocimiento de cierta información adicional (trapdoor). Realizar un análisis formal de qué es ser computacionalmente difícil conduce a inferir qué recursos de cómputo tiene el atacante en relación a los recursos de los demás participantes. En ese sentido se entiende que un criptosistema es perfectamente seguro si un atacante con ilimitada capacidad de cálculo es incapaz de obtener información. Este escenario es poco realista, por lo que se propone la noción de seguridad semántica, en la que los recursos del atacante están polinomialmente acotados por los resursos de los participantes. La dificultad de demostrar que un criptosistema es semánticamente seguro conduce al concepto de seguridad polinomial o indistinguibilidad, mucho más accesible matemáticamente.
En este TFG se estudiarán estas nociones de seguridad y las relaciones entre ellas en distintos escenarios de ataque. como ataques pasivos, ataque de texto en claro conocido/escogido, ataques de criptograma conocido/escogido adaptativo o no.
Los resultados pasan por acotar la probabilidad de éxito de un ataque a partir de la probabilidad de éxito de un ataque en un escenario distinto.

**Tipología:** Estudio de casos, teóricos o prácticos, relacionados con la temática del Grado.

**Objetivos planteados:**

- Definir y relacionar las distintas nociones de seguridad: Unidireccionalidad e Indistinguibilidad.
- Definir los distintos escenatios de ataque: pasivo, texto en claro conocido/escogido, criptograma conocido/escogido.
- Relacionar las distintas nociones y escenarios.
- Diseño de mecanismos de encapsulamiento de clave indistinguibles a partir de criptosistemas asimétricos unidireccionales.

**Bibliografía básica:**


1. Nigel P. Smart. Cryptography Made Simple. Springer International Publishing Switzerland 2016. DOI 10.1007/978-3-319-21936-3
2. Joachim von zur Gathen. CryptoSchool. Springer-Verlag Berlin Heidelberg 2015. DOI 10.1007/978-3-662-48425-8
3. Daniel J. Bernstein and Edoardo Persichetti. Towards KEM Unification. Cryptology Archive, Paper 2018/526. https://eprint.iacr.org/2018/526


**Recomendaciones y orientaciones para el estudiante:**

**Plazas:** 1

## 2. DATOS DEL TUTOR/A:

**Nombre y apellidos:** FRANCISCO JAVIER LOBILLO BORRERO

**Ámbito de conocimiento/Departamento:** ÁLGEBRA

**Correo electrónico:** jlobillo@ugr.es

**3. COTUTOR/A DE LA UGR (en su caso):**

**Nombre y apellidos:**

**Ámbito de conocimiento/Departamento:**

**Correo electrónico:**

**4. COTUTOR/A EXTERNO/A (en su caso):**

**Nombre y apellidos:**

**Correo electrónico:**

**Nombre de la empresa o institución:**

**Dirección postal:**

**Puesto del tutor en la empresa o institución:**

**Centro de convenio Externo:**

**5. DATOS DEL ESTUDIANTE:**

**Nombre y apellidos:** Marta Maldonado Galdeano

**Correo electrónico:** martamalgal@correo.ugr.es