Propuesta de Trabajo Fin de Grado en Matemáticas (curso 2021-2022)

Responsable de tutorización: Francisco Javier Lobillo Borrero *Departamento:* Álgebra *Correo electrónico:* jlobillo@ugr.es
Responsable de cotutorización: *Departamento:* *Correo electrónico:*
(Rellenar sólo en caso de que la propuesta esté realizada a través de un estudiante) *Estudiante que propone el trabajo:* Claudia Rodriguez Vegas

Título del trabajo: Funciones Hash criptográficamente seguras
Tipología del trabajo (marcar una o varias de las siguientes casillas):
Materias del grado relacionadas con el trabajo: Álgebra I, Estadística Descriptiva e Introducción a la Probabilidad, Álgebra III, Teoría de Números y Criptografía.
Descripción y resumen de contenidos: Las funciones hash criptográficamente seguras son un elemento esencial en el diseño de algoritmos de firma digital. La seguridad radica en la dificultad de encontrar colisiones, segunda preimagen e imágenes inversas. Por ello es necesario estudiar la relación entre dichas dificultades, para ver qué elementos deben ser tenidos en cuenta en el diseño. Por otro lado, en vista de que una función Hash debe actuar sobre cadenas de bits de tamaño arbitrario, es conveniente disponer de construcciones como la de Merkle-Damgard que extienden las buenas propiedades criptográficas de funciones actuando sobre cadenas acotadas a cadenas arbitrarias. En este Trabajo de Fin de Grado se demostrará que la resistencia a colisiones implica las demás propiedades, así como que la construcción de Merkle-Damgard permite extender la resistencia a colisiones de funciones de compresión a funciones hash.
Actividades a desarrollar: Introducción a las funciones hash. Ataque del cumpleaños. Ejemplos relacionados con el logaritmo discreto. Construcción de Merkle-Damgard.

Familia SHA.

Objetivos matemáticos planteados
Demostrar las relaciones entre las propiedades de seguridad de las funciones hash.
Demostrar la eficacia del ataque del cumpleaños.
Relacionar la seguridad de una funnción hash a partir de su función de compresión mediante la construcción de Merkle-Damgard.

Bibliografía para el desarrollo matemático de la propuesta:

[1] N. P. Smart, "Cryptography Made Simple", Springer 2016.
[2] Joachim von zur Gathen, "CryptoSchool", Springer 2015.
[3] H. Delfs, H. Knebl, "Introduction to Cryptography", Springer 2015.

Otras referencias (si procede):

Firma del estudiante
(solo para trabajos propuestos por estudiantes)

CLAUDIA
RODRÍGUEZ
VEGAS
78944143R

Firma del responsable de tutorización
(solo para trabajos propuestos por estudiantes)

Firmado digitalmente por LOBILLO BORRERO FRANCISCO JAVIER - 30540852A
Fecha: 2021.05.17 06:37:45 +02'00'

Firma del responsable de cotutorización
(solo para trabajos propuestos por estudiantes)

En, Granada, a de de 2021