Propuesta de Trabajo Fin de Grado en Matemáticas (curso 2022-2023)

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:* Lucía Cano

Título del trabajo: Descripción y aspectos del criptoanálisis de la máquina Enigma
Tipología del trabajo (marcar una o varias de las siguientes casillas): ☐ Complementario de profundización ☐ Divulgación de las Matemáticas ☐ Docencia e innovación ☐ Herramientas informáticas ☐ Iniciación a la investigación
Materias del grado relacionadas con el trabajo: Álgebra II
Descripción y resumen de contenidos: La máquina Enigma es un dispositivo de cifrado y descifrado patentado por Scherbius & Ritter en 1918, y adoptada por las diferentes fuerzas armadas alemanas como principal herramienta de cifrado para las comunicaciones durante la Segunda Guerra Mundial. Es una máquina electromecánica cuya función de sustitución se implementa a partir de un conjunto de rotores junto con un cableado adicional. La descripción de la máquina Enigma puede hacerse matemáticamente mediante grupos de permutaciones del alfabeto, asociando una permutación a cada rotor y a cada reflector. De esta forma cada configuración de la máquina puede verse como una ecuación en un grupo de permutaciones. En este Trabajo de Fin de Grado, la estudiante estudiará las ecuaciones correspondientes y como pueden ser resueltas para simular el comportamiento de la máquina y para realizar ataques que permitan conocer los rotores, reflectores y configuraciones diarias, lo que permite conocer todos los mensajes cifrados. Dichos ataques se basan en el uso de mensajes estereotipos y en el conocimiento de partes del texto original.
Actividades a desarrollar: Estudio de las ecuaciones de la máquina Enigma.

Determinación del cableado frontal conocida la configuración de los rotores.
Determinación del cableado interno de los rotores.
Determinación de la configuración diaria.
Ataques de texto en plano conocido y las Bombas.
Ataques al criptograma.

Objetivos matemáticos planteados
Estudio de las ecuaciones de la máquina Enigma.
Determinación del cableado conocida la configuración de los rotores.
Determinación del cableado interno de los rotores.
Determinación de la configuración diaria.
Ataques de texto en plano conocido y las Bombas.
Ataques al criptograma.

Bibliografía para el desarrollo matemático de la propuesta:

N. P. Smart. Cryptography Made Simple. Springer, 2016.
D. W. Davies. The bombe a remarkable logic machine. Cryptologia, 23:2, 108-138. 1999.
D. W. Davies. Effectiveness of the diagonal board. Cryptologia, 23:3, 229-239. 1999.
M. Rejewski. An application of the theory of permutations in breaking the Enigma cipher. Applicaciones Mathematicae 16(4), 1980.

Otras referencias (si procede):

Firma del estudiante
(solo para trabajos propuestos por alumnos)

Firmado digitalmente por LOBILLO BORRERO FRANCISCO JAVIER - 30540852A
Fecha: 2022.05.25 10:02:45 +02'00'

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

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

En, Granada, a 24 de mayo de 2022