PROPUESTA DE TRABAJO DE FIN DE MÁSTER
MÁSTER EN MATEMÁTICAS AVANZADAS

Director(es): Ignacio Luengo Velasco

Tutor UCM: (sólo en caso de que no haya ningún director de la UCM)

Alumno(a): Jaime Miguel Zapata

Curso: Máster en Matemáticas Avanzadas

Título: Criptografía con Códigos Goppa

Resumen: Los llamados "Códigos Correctores" son algoritmos que detectan y corrigen errores en la transmisión o el almacenaje de la información. La idea es añadir redundancias a la información de forma óptima para poder corregir el mayor número de errores ocupando la menor memoria posible.

Dichos algoritmos pueden usarse también como herramientas de encriptación: si queremos transmitir un mensaje m, le añadimos un "error" e y enviamos $m+e$. Un algoritmo corrector recuperará después el mensaje original m. Con esta idea se puede llegar a construir un sistema de encriptación de clave pública.

En este trabajo se hará una introducción a los mencionados Códigos Correctores, focalizándonos en un tipo concreto: los "Códigos Goppa". Posteriormente, se analizará el "Criptosistema de McEliece", sistema de clave pública basado en códigos Goppa.

La bibliografía básica será:

- **"Applied Abstract Algebra", de R. Lidl y G. Pilz**
- **"Introduction to Coding Theory", de J.H van Lint**