	ENSENYAMENT: MASTER DE ENGINYERIA DE PROGRAMARI LLIURE		
	ASSIGNATURA: Criptografia i Codis amb Sage, CCSAGE. (Codi: 11537) **Curso 2009-10**		
	PROFESSOR/A RESPONSABLE: Ramiro Moreno Chiral		
	CURS: Segundo (1º cuatrimestre)	**CRÈDITS: 6**	**TIPUS: Optativa**

1. OBJECTIUS

Esta asignatura CCSAGE, que se ofrece por primera vez este curso en el MEPL, se asienta en el estudio y uso del calculador matemático **Sage**, creado por William Stein en Harvard en enero de 2005. Así pues vamos a tratar con un sistema reciente que, además, evoluciona rápidamente. Pretendemos iniciarnos en el manejo de una herramienta compleja al tiempo que atacamos algunos problemas *criptográficos* y de *códigos correctores* de errores de canal. Tangencialmente habrá que formalizar y ver com se tratan en **Sage** algunos conceptos del, digamos, bagage matemático básico.

Ni que decir tiene que Sage es "software" libre: empaqueta "software" libre ya creado y usa *python* como lenguaje básico. Pero dejemos que lo diga el propio Stein: "*Sage is the **only** project whose goal is to create a viable open source alternative to all of Mathematica, Maple, Matlab and Magma. It is the analogue of Star Office or Firefox, as alternatives to Microsoft Office or Internet Explorer.*"

2. ESTRUCTURA

CCSAGE se impartirá en el primer cuatrimestre de este curso 2009-10, como asignatura optativa de la titulación del Master de Enginyeria de Programari Lliure. Tiene 6 créditos: de esos 6, 4'5 son presenciales, equivalen a 45 horas de clase, y dedicaremos 2 a clases de teoría y 2'5 créditos a clases de laboratorio.

La he pensado en tres partes, a saber,

1. **Introducción**: Revisaremos y "actualizaremos" el bagage matemático básico (algebraico, fundamentalmente) desarrollando esos conceptos con las '*Sage work sheets*' (en adelante, sws).
1. **Proyecto Crypto**: Se desarrollará un sistema criptográfico en **Sage**.
2. **Proyecto ECC** (ECC: por "error correcting codes"): Un segundo proyecto con **Sage**, sobre algún sistema de corrección de errores de canal.

3. PROGRAMA

Parte I. Introducción

Lección 1: Fundamentos matemáticos

1.1 Grupos, anillos y cuerpos: revisión y complementos.
1.2 Cuerpos finitos.
1.3 Espacios vectoriales.
1.4 Anillos de polinomios: complementos.

LAB Sesiones 1 y 2: Introducción al **Sage** con ejercicos sws sobre la Lección 1

Parte II. Proyecto Crypto

Lección 2: Somera introducción a la criptografía.

2.1 Criptografía clásica.
2.2 El problema de la factorización de enteros, IFP.
2.3 El problema del logaritmo discreto, LDP
2.4 Otros problemas computacionalemente difíciles.
2.5 Criptoanálisis.

LAB Sesión 3: Cripto clásica.

LAB Sesión 4: Los IFP y LDP.

Lección 3: Introducción a los criptosistemas sobre curvas elípticas (ECCs).

3.1 Curvas elipticas (ECs) sobre cuerpos finitos.
3.2 Propiedades relevantes.
3.3 El ECLDP.
3.4 ECCs tipo ElGamal y ECDSA.

LAB Sesión 5: ECs sobre cuerpos finitos

LAB Sesión 6: El ECDLP.

LAB Sesión 7: Proyectos ECCs

Parte III. Proyecto ECC

Lección 4. Códigos lineales y cíclicos.

4.1 Códigós lineales. Conceptos básicos
4.2 Decodificación.
4.3 Códigos cíclicos.
4.4 Códigos BCH y Reed-Solomon (RS)

LAB Sesión 8: Introducción a los códigos.

Lección 5. Proyecto ECC: códificación de los CDs de audio.

5.1 Simulación de canales con ruido.
5.2 Códigos RS recortados.
5.3 Decodificación FFT.
5.4 Decodificación Gao.

LAB Sesión 9: Proyecto ECC.

4. MATERIALS DE L'ASSIGNATURA I PROGRAMARI

- **Clases teóricas**: desarrolladas con la ayuda de la pizarra y transparencias.
- **Clases de proyectos**: en laboratorio, usando las sws de **Sage**.

5. BIBLIOGRAFIA

General

- La documentación sobre **Sage** se puede encontrar en http://www.sagemath.org/help.html. El 'Tutorial', el 'Sage for newbies' y al menos los capítulos correspondientes a crypto, ECs y ECC, del 'Reference manual' estarán disponibles en Sakai.

- *Codificación de la Información*. Juan Munuera y Juan Tena, Manuales y textos Universitarios, nº 25. Ciencias. Universidad de Valladolid, 1997.

- *Comunicación Digital, Teoría Matemática de la Información. Codificación Algebraica. Criptología*. Josep Rifá y Llorenç Huguet, Masson, Barcelona, 1991.

Parte II: Proyecto Crypto

- *Handbook of Applied Cryptography*. A. J. Menezes, P. C. van Oorschot y S. A. Vanstone , Fifth Printing (August 2001), que está disponible en http://www.cacr.math.uwaterloo.ca/hac/, por cortesía de CRC Press. Manual muy completo del tema.

- *Elliptic Curve Public Key Cryptosystems*, A. J. Menezes, Kluwer Academic Publishers,1993. Ya un tanto antiguo pero muy manejable.

- *Handbook of elliptic and hyperelliptic curve cryptography*, H. Cohen, G. Frey et alt., CRC Press, 2005. El "otro" gran manual de criptografía

Parte III: Proyecto ECC

- *Informació i codis*. Josep M. Brunat y Enric Ventura, Col. Politext, Edicions UPC, 2001. Libro base para la parte III de la asignatura, con casi todo lo necesario también para la **Parte I: Introducción**.

- *Coding and Information Theory*. Steven Roman, Graduate Texts in Mathematics. Springer-Verlag, New York, 1992. Muy buen manual, especialmente serio en la teoría de los códigos correctores.

- *A First Course in Coding Theory*. Raymond Hill, Oxford Applied Mathematics and Computing Science Series. Clarendon Press, 1993. Un libro "fácil" de Teoría de Códigos.

6. AVALUACIÓ

La evaluación se realizará según dos modelos:

1. *Continuada*. Consistirá en la realización de una serie de 5 *Actividades Complementarias,* ACs, (una por cada capítulo del programa) con una valoración del 40% de la calificación y de dos Proyectos: uno de Crypto y otro de ECC, que representarán el 60% de la calificación final.
2. *Examen global*. Consistirá en un examen sobre 10 puntos de todos los contenidos de la asignatura. Ambos modelos de evaluación son excluyentes.

Como no hay convocatoria en septiembre, obviamente
NO HABRÁ EVALUACIÓN EN SEPTIEMBRE.