Portafolio como herramienta educativa en Ciberseguridad: Aprendizaje por aproximación en Criptografía.

Noemí DeCastro-García,
Research Institute of Applied Sciences in Cybersecurity (RIASC),
Departamento de Matemáticas
Universidad de León,
ncasg@unileon.es

Adriana Suárez Corona,
Research Institute of Applied Sciences in Cybersecurity (RIASC),
Departamento de Matemáticas
Universidad de León,
asuac@unileon.es

***Resumen*—En el contexto educativo actual, los programas de formación en Ciberseguridad incluyen la Criptografía como disciplina fundamental. En esta materia, se presentan las técnicas y protocolos criptográficos utilizados en la seguridad de las comunicaciones, así como las tendencias emergentes en el campo. Sin embargo, los estudios realizados mediante las encuestas de calidad docente de la materia, muestran que el desarrollo de competencias se encuadra en un marco matemáticamente demasiado abstracto, que implica dificultades en los procesos de enseñanza y aprendizaje. En este artículo, se desarrolla una propuesta metodológica basada en el uso del portafolio como herramienta educativa, que nos permite aproximarnos a la Criptografía desde el Aprendizaje basado en Proyectos. El diseño se ha llevado a la práctica en estudios de postgrado en Ciberseguridad, y la experiencia se ha evaluado mediante diferentes cuestionarios y estadísticas, cuyos resultados son positivos, y muestran que el aprendizaje es más eficaz y significativo.**

***Index Terms*—Ciberseguridad, Criptografía, Portafolio, Innovación docente, Formación.**

Tipo de contribución: *Formación e innovación educativa.*

I. Introducción.

Actualmente, la especialización en Ciberseguridad es uno de los perfiles profesionales más demandados por empresas e instituciones públicas. Sin embargo, no hay suficientes egresados con formación específica en el área como para poder cubrir todas las vacantes existentes. Por este motivo, los currículos de estudios universitarios han comenzado a incluir en los programas de grado y/o postgrado, la especialidad en Ciberseguridad.

Una de las materias incluidas en la mayoría de los programas de formación en Ciberseguridad es la Criptografía. En esta asignatura se presentan las técnicas y protocolos criptográficos necesarios para garantizar la privacidad y la autenticidad e integridad de los datos, así como los resultados y herramientas matemáticas necesarias para comprender su funcionamiento.

En las últimas décadas, la Criptografía se ha convertido en una disciplina fundamental para las telecomunicaciones y todas aquellas plataformas que las soportan. Además, las últimas tendencias en Big Data requieren arquitecturas tecnológicas cuya seguridad y privacidad supone nuevos desafíos de investigación, veáse [1] ó [2]. En ese escenario, la Criptografía aporta herramientas que sirven para proteger la confidencialidad y autenticación de los datos. Sin embargo, los esquemas tradicionales de clave privada o pública pueden tener limitaciones cuando el conjunto de datos es grande y complejo. Por lo tanto, es necesario el uso de otro tipo de esquemas como los de cifrado homomórfico o aquellos que permiten el control de acceso basado en credenciales, veáse [3] y [4]. Además, la necesidad de almacenar, migrar y procesar datos en la nube conlleva grandes ventajas computacionales, pero presenta serias amenazas en la seguridad de dicha información, pudiendo acabar en manos de usuarios no deseados. Se precisan, por tanto, otro tipo de herramientas criptográficas, veáse [5], [6], [7], [8] o [9], entre otros.

Por otra parte, la aparición del ordenador cuántico supone un serio peligro para la seguridad de los protocolos criptográficos más utilizados en la actualidad, incluyendo RSA y esquemas basados en curvas elípticas [10]. Por este motivo, es necesario el estudio de esquemas que resistan este tipo de ataques, la llamada criptografía post cuántica [11].

Por lo tanto, un programa de formación en Ciberseguridad no sería del todo completo si la materia de Criptografía no estuviera incluida. Es más, la impartición de este curso es requisito necesario en los criterios que determinan la excelencia académica en ciber defensa por la NSA [12].

Desde el punto de vista didáctico, el desarrollo de competencias en la materia de Criptografía se encuadra en un potente marco abstracto. Es necesario tener presente que no podemos prescindir de la base matemática que se esconde detrás de este tipo de conocimiento, ya que la finalidad educativa de los programas de Ciberseguridad ha de estar enfocada a la generación de expertos que no sólo sean capaces de aplicar protocolos criptográficos, sino de determinar cuáles son más adecuados para cada situación, reconocer e identificar vulnerabilidades, e incluso romper algunos esquemas criptográficos que se les puedan presentar. Sin embargo, habitualmente los estudiantes de los programas de especialización en Ciberseguridad son graduados en ingeniería cuya formación en matemáticas está enfocada al estudio de la materia como herramienta utilitaria, relegando a un segundo plano el desarrollo y comprensión del conocimiento teórico matemático. Por este motivo, el formalismo y rigor abstracto inherente al aprendizaje eficaz de la Criptografía, supone que, en determinadas ocasiones, los estudiantes desconozcan o no comprendan la necesidad, funcionalidad y aplicabilidad de los contenidos teóricos de-

sarrollados.

En particular, es conveniente crear situaciones activas de enseñanza y aprendizaje de la Criptografía que estén relacionadas con contextos cotidianos de seguridad informática. Sin embargo, encontrar situaciones reales de aprendizaje no es, a priori, una tarea sencilla, ya que algunos de los escenarios reales más actuales y emergentes relacionados con la Criptografía, como los descritos con anterioridad, requieren un conocimiento matemático abstracto de alto nivel cuyo dominio resulta prácticamente inabarcable en una única asignatura de Criptografía.

La propuesta metodológica desarollada en este artículo se basa en la experiencia docente en la materia de Criptografía impartida en el Máster de Investigación en Ciberseguridad de la Universidad de León [13]. Tras varias ediciones del título universitario, se han detectado algunas deficiencias en los procesos de enseñanza y aprendizaje de la materia relacionados con la aplicabilidad de los contenidos, la relación con problemas criptográficos reales, las pruebas de evaluación y el proceso de aprendizaje de los estudiantes. Por ello, con el fin de solventar este problema, en el curso 2016/2017, se ha introducido el portafolio como herramienta de aprendizaje y evaluación de los alumnos.

La experiencia se ha evaluado mediante la realización de un cuestionario sobre la nueva herramienta, así como la realización de una encuesta basada en los estándares SEEQ (Students' Evaluation of Educational Quality) [14] y [15].

El artículo está organizado de la siguiente manera: en la Sección II presentamos la contextualización de la experiencia, detallamos los aspectos más relevantes del programa de formación en el que se ha llevado a cabo, así como las características principales de la asignatura de Criptografía. En la Sección III, se desarrollan los motivos que nos llevaron a realizar esta experiencia de innovación docente. En la Sección IV se describe la propuesta metodológica, así como la evaluación realizada. En las secciones V y VI se desarrollan los resultados obtenidos y la discusión. Finalmente, se encuentran las conclusiones, referencias y material suplementario.

II. Contextualización.

El Máster universitario de Investigación en Ciberseguridad es un título oficial de postgrado de la Universidad de León, cuya primera edición se ha realizado en el curso escolar 2016 / 2017. Consta de dos cursos de 60 ECTS cada uno y se imparte en lengua inglesa. Este programa tiene su origen en el Máster Profesional en Tecnologías de la Seguridad de la Información (veáse [16]), cuya duración era de un año con una carga de 60 ECTS. El título propio se ha impartido entre los años 2008 y 2016 en la Universidad de León, en coordinación con el Instituto Nacional de Ciberseguridad (INCIBE).

En las últimas dos ediciones del título propio, se tuvo una matrícula de 18 alumnos cada año. Como hemos mencionado, en el curso 2016/2017, el Máster de Investigación en Ciberseguridad de la Universidad de León se ha convertido en un título oficial cuya duración es de dos años escolares. En el curso actual, hay 15 alumnos, 7 alumnos matriculados en el primer curso y 8 alumnos en el segundo curso, que provienen, en su mayoría, de Grados en Ingeniería Informática e Ingeniería de Telecomunicaciones.

En particular, la materia de Criptografía ha sido una asignatura obligatoria en los dos tipos de titulación. En el programa de formación oficial, la materia *Mathematics for Cybersecurity I: Cryptography*, de 6 ECTS se incluye en el primer curso. En el título propio, la asignatura Criptografía constaba de 4 ECTS. A lo largo de las tres últimas ediciones, el equipo docente implicado en la asignatura se ha mantenido constante, estando compuesto por profesores del Departamento de Matemáticas de la Universidad de León.

Los contenidos que se imparten en esta materia se basan en una aproximación histórica de la Criptografía, desde los principales hitos alcanzados hasta los nuevos desafíos que plantean los escenarios más innovadores y actuales. Los alumnos pueden acceder al material didáctico a través de Moodle, la plataforma virtual de aprendizaje utilizada por la Universidad de León. Con el fin de dar una panorámica global de la Criptografía, el programa actual de la asignatura incluye los siguientes bloques de contenidos:

1) Fundamentos matemáticos y Criptografía clásica: aritmética modular, principales criptosistemas clásicos, etc.
2) Combinatoria: repaso de contenidos básicos y aplicación al cálculo de cardinales de espacios de claves, etc.
3) Fundamentos de Teoría de la Información: introducción a los conceptos fundamentales, seguridad perfecta, etc.
4) Criptografía simétrica y asimétrica: cifrado en flujo, cifrado en bloque, RSA, ElGamal, firma digital, intercambio de clave, etc.
5) Compresión de datos: funciones hash, etc,
6) Generadores de números pseudoaleatorios y
7) Nuevas tendencias en criptografía: criptografía cuántica y post-cuántica, criptomonedas, etc.

Debido a la ampliación de horas lectivas que ha supuesto la conversión del título propio hacia el programa oficial de investigación, se han completado los contenidos de la materia de la manera descrita en la Tabla I.

TABLE I
Contenidos de la asignatura Criptografía en los distintos programas.

Bloque	Master oficial	Título propio
Fundamentos matemáticos y criptografía clásica	✓	✓
Combinatoria	✓	
Fundamentos de Teoría de la Información	✓	
Criptografía simétrica y asimétrica	✓	✓
Compresión de datos	✓	
Generadores de números pseudoaleatorios	✓	✓
Nuevas tendencias en criptografía.	✓	✓

El instrumento de evaluación utilizado durante las ediciones de 2014/2015 y 2015/2016, consistió en una prueba escrita, cuyo peso era el 100 % de la calificación, y en la que el alumnado disponía del material didáctico utilizado durante la asignatura. En esta prueba, se evaluaron los contenidos y competencias que los alumnos habían adquirido, correspondientes a todos los bloques temáticos descritos en la Tabla I, salvo el relativo a nuevas tendencias.

Durante el curso escolar 2015/2016, el programa de Criptografía se ha planificado según los plazos descritos en la Tabla II, ajustándonos a la duración establecida por los créditos universitarios del Espacio Europeo de Educación Superior (60 horas que incluyen sesiones presenciales y pruebas de evaluación).

TABLE II
CRONOGRAMA DE LA ASIGNATURA CRIPTOGRAFÍA EN EL CURSO ESCOLAR 2016 / 2017.

Bloque	Temporalización
Fundamentos matemáticos y criptografía clásica	10 horas
Combinatoria	2 horas
Fundamentos de Teoría de la Información	6 horas
Criptografía simétrica y asimétrica	30 horas
Compresión de datos	4 horas
Generadores de números pseudoaleatorios	2 horas
Nuevas tendencias en criptografía.	4 horas

III. MOTIVACIÓN / JUSTIFICACIÓN.

La calidad de la formación impartida en el título propio del Master Profesional de Seguridad en Tecnologías de la Información, se ha medido, desde el curso escolar 2014/2015, mediante encuestas de evaluación basadas en los estándares SEEQ [14]. Esta encuesta incluye preguntas mediante las que los estudiantes valoran aspectos como su aprendizaje, satisfacción, pruebas de evaluación propuestas, metodología y material didáctico proporcionado. Los resultados han mostrado que la mayoría de las asignaturas del Máster obtuvieron una buena puntuación, superior a 4 sobre 5. Sin embargo, la asignatura de Criptografía ha sido la peor valorada durante dos años consecutivos.

Como podemos ver en la *Fig. 1*, los ítems con una valoración más baja son las pruebas de evaluación, los trabajos, el aprendizaje y la organización, resultando especialmente críticos los tres primeros. Por este motivo, en el curso 2015/2016, se realizó una entrevista abierta con todos/as los/as estudiantes para comprender los motivos que les habían llevado a dar esa puntuación a la materia. Los resultados de dicho análisis se desarrollan en [17] y se dirigen hacia el descontento con el enfoque principalmente teórico y matemático de la asignatura, y el desconocimiento de la funcionalidad y aplicabilidad de la materia.

IV. DISEÑO METODOLÓGICO.

Por los motivos descritos en la Sección III, se ha realizado una propuesta metodológica de mejora para la asignatura de Criptografía del primer curso del Máster de Investigación en Ciberseguridad de la Universidad de León en el curso 2016/2017. El diseño parte del aprendizaje basado en proyectos, y hace especial énfasis en el desarrollo de los aspectos prácticos de la materia, sus aplicaciones, la relación de la asignatura (de manera concreta) con problemas en escenarios reales, y la relevancia e importancia de la comprensión de los contenidos matemático - teóricos. Además, básandonos en los resultados de la encuesta estandarizada SEEQ ([18]), hemos enfocado la innovación hacia la mejora en los bloques de Aprendizaje, Pruebas de evaluación y Trabajos.

En concreto, hemos considerado oportuno el uso del portafolio como herramienta de aprendizaje e instrumento complementario de evaluación. El concepto de portafolio implica la elaboración de una carpeta o dossier de evidencias de aprendizaje, en la que los estudiantes muestran su trabajo, y el proceso que han seguido para conseguirlo. Entre las ventajas de su utilización nos encontramos con que el portafolio ayuda al alumnado a hacerse más responsable de su propio aprendizaje, potencia la organización y fomenta la reflexión, veáse [19].

Por otra parte, las nuevas metodologías educativas implican una reflexión hacia una nueva concepción de los instrumentos y procedimientos de evaluación, convirtiendo a ésta en un proceso más personalizado y centrado en el alumno. El uso del portafolio como instrumento de evaluación ha sido validado en numerosas ocasiones en diferentes cursos de nivel universitario, veáse [19], [20], [21] o [22], [23], entre otros.

El portafolio propuesto a los estudiantes ha consistido en varios proyectos prácticos relacionados con los diferentes bloques de contenidos de la asignatura, y un proyecto final en el que se pone de manifiesto la relación entre los distintos temas del curso en un contexto real. Para establecer los proyectos, nos hemos basado en [21], donde se propone una taxonomía innovadora para el aprendizaje de alto nivel, que nos permite diseñar experiencias de aprendizaje eficaces y activas. La experiencia, por tanto, se enmarca dentro de un contexto de aprendizaje basado en proyectos y aprendizaje por aproximación. Este tipo de metodología nos permite aproximarnos a los tópicos criptográficos de una manera más activa, promoviendo que el estudiante construya su propio conocimiento, y no sea un mero receptor de contenidos. Debido al número de alumnos, se pudo realizar un seguimiento de la evolución y el trabajo de los estudiantes, así como resolver posibles dudas y/o dificultades durante algunas horas lectivas. Estas sesiones de seguimiento presenciales se habían preestablecido en el cronograma de la programación didáctica de la asignatura.

Se ha utilizado el portafolio como recurso didáctico de manera pre-instruccional para introducir la necesidad de estudio de los tópicos teóricos de Criptografía para resolver problemáticas reales de seguridad. De esta manera, se motiva al alumnado proporcionando situaciones en las que puede descubrir, por sí mismo, aquellos escenarios en los que la Criptografía es esencial, fomentando un aprendizaje significativo y evitando el aplicacionismo ([24]). También se ha hecho uso del portafolio como herramienta co-instruccional, para que los/las estudiantes pudieran resolver el proyecto, a medida que aplican los contenidos aprendidos en el aula.

Los objetivos planteados en esta experiencia se describen a continuación:

1) Generales:
   - Mejorar el proceso de enseñanza y aprendizaje de la materia de Criptografía en los programas específicos de formación en Ciberseguridad.
   - Familiarizar al alumnado con aquellos contextos reales de seguridad que requieran de conocimiento experto en protocolos criptográficos, para que sean capaces de reconocerlos en el ámbito futuro profesional.
   - Profundizar y desarrollar la competencia para saber aplicar, crear y mejorar los contenidos criptográficos adquiridos en la formación impartida.

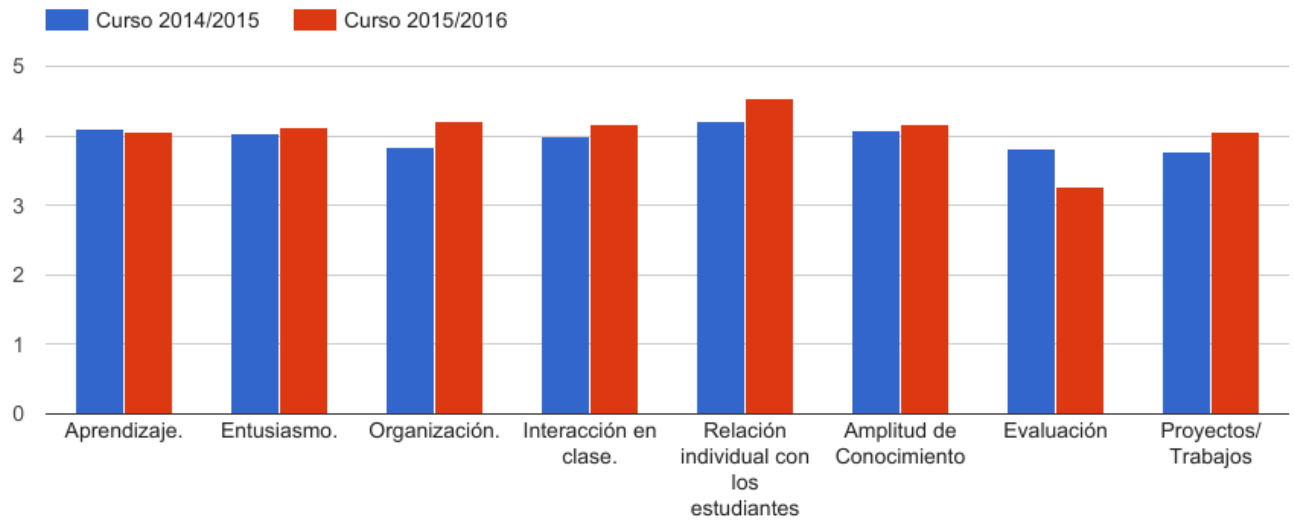

Fig. 1. Resultados de Criptografía en la encuesta SEEQ.

- Fomentar la adquisición de actitudes positivas hacia las matemáticas. En particular, hacia los contenidos teóricos implicados en la disciplina de Criptografía.
- Introducir al alumnado en algunas herramientas informáticas útiles para la implementación de esquemas criptográficos y criptoanálisis.
- Introducir el portafolio como herramienta educativa que nos permita trabajar determinados contenidos conceptuales, procedimentales y actitudinales en diferentes materias. En particular, en Criptografía.
- Estimular situaciones activas de aprendizaje.
- Fomentar la resolución de problemas dentro del área de seguridad informática y de las comunicaciones.

2) Transversales:

- Estimular la capacidad de elaboración y defensa de argumentos científicos ante lectores especializados.
- Establecer mecanismos e instrumentos de evaluación que permitan al alumnado desarrollar competencias de aprendizaje de forma autónoma.
- Desarrollar la capacidad de gestionar el tiempo y el trabajo autónomo.
- Integrar diferentes conocimientos.

A continuación, se enumeran los diferentes proyectos que conformaban el portafolio final. Todos los proyectos están relacionados de manera jerárquica: es decir, la elaboración de los primeros era necesaria para una comprensión y elaboración significativa del Proyecto final. Para una descripción más detallada, veáse Sección VIII de *Material Suplementario*.

1) **Proyecto I: Fundamentos matemáticos y criptografía clásica.** En este proyecto los alumnos realizaron el criptoanálisis de un texto cifrado con un criptosistema clásico en el que debían establecer y resolver ecuaciones en congruencias adecuadas, una vez realizado un análisis de frecuencias. Se propuso el uso de la herramienta interactiva [25].
2) **Proyecto II: Criptografía de clave pública.** En este proyecto los estudiantes utilizaron Maxima para generar pares de claves públicas y privadas para los esquemas RSA y ElGamal ([26]). Publicaron sus claves en un directorio público y cifraron mensajes para sus compañeros con el posterior descifrado de los mensajes recibidos.
3) **Proyecto III: Autenticación y Criptoanálisis.** Esta tarea consistió en realizar, usando una librería de Pari [27], el cifrado con firma utilizando RSA y el intento de criptoanalizar textos cifrados de otros compañeros cuando los parámetros utilizados no han sido adecuados.
4) **Proyecto final: Descifrar la información sobre la conexión segura de una página web.** Para repasar los conocimientos adquiridos a lo largo del curso, los alumnos analizaron la información proporcionada por una página web sobre cómo se realiza la conexión segura, indicando todos los protocolos utilizados y argumentando el motivo de uso de esos protocolos específicos.

Además, se ha utilizado el portafolio como instrumento de evaluación de la asignatura, complementando la prueba escrita habitual. La evaluación ha sido sumativa y continua. El deadline de entrega de cada tarea, así como el peso de cada prueba en la calificación final, se encuentran en la Tabla III.

TABLE III
DEADLINE DE CADA PROYECTO.

Proyecto	Peso en la calificación	Deadline
Proyecto I	10 %	30/11/2016
Proyecto II	10 %	22/12/2016
Proyecto III	10 %	12/1/2017
Proyecto final	20 %	10/2/2017
Prueba escrita	50 %	7/2/2017

Debido al carácter sumativo de la evaluación, no se dieron a conocer las calificaciones hasta que la prueba escrita no había sido realizada.

A. *Evaluación de la propuesta.*

La evaluación de la experiencia se ha llevado a cabo desde dos perspectivas diferentes: la valoración de la calidad

docente, y el proceso de aprendizaje de los estudiantes.

En el primer caso, para analizar el grado de satisfacción de los estudiantes con el profesorado, así como con la metodología utilizada en la asignatura de Criptografía, entre otros, se ha realizado la encuesta de calidad basada en SEEQ que se había implementado en ediciones anteriores.

Por otra parte, y con el objetivo de evaluar el portafolio como herramienta de aprendizaje, se ha elaborado un cuestionario específico sobre el mismo. Este cuestionario (basado en [22], [23]), contenía 22 afirmaciones que los estudiantes tenían que valorar en escala tipo Likert, de 1 a 5 donde 1= nada de acuerdo y 5= totalmente de acuerdo. Las cuestiones estaban referidas a cinco bloques que describimos a continuación:

1) **El portafolio como herramienta de aprendizaje** (9 afirmaciones): en el que valoraron la utilidad del portafolio para mejorar su proceso de aprendizaje en Criptografía. Aspectos como el reconocimiento de fortalezas y debilidades, identificación de contenidos más relevantes, gestión del trabajo para conseguir los objetivos de aprendizaje planteados o utilidad para preparar la prueba escrita.
2) **Funcionalidad de los contenidos teóricos** (3 cuestiones): en el que evaluaron la capacidad del portafolio para mejorar la comprensión de los aspectos teóricos estudiados, entender sus aplicaciones prácticas y reconocer su necesidad en situaciones del mundo real.
3) **Desarrollo del portafolio** (6 cuestiones): en el que han valorado aspectos relativos a la manera en la que han trabajado (consulta de bibliografía y/o material didáctico proporcionado), la reflexión y el esfuerzo realizado.
4) **Aspectos transversales** (4 cuestiones): en este bloque se han valorado ítems como la motivación, la mejora en la comunicación escrita en lengua inglesa, el interés, el desarrollo personal y profesional, así como la propuesta para la inclusión del uso del portafolio en otras materias, y su utilización en un programa de formación en Ciberseguridad.

Ambos instrumentos de evaluación se llevaron a cabo de manera anónima y voluntaria, obteniendo un 100% de los participación. Además, los cuestionarios se ofrecieron y cumplimentaron en el momento en el que las calificaciones de la asignatura de Criptografía ya estaban cerradas, evitando la situación en la que los estudiantes pudieran sentirse coaccionados por la posibilidad de que los resultados de las encuestas influyeran en su calificación.

V. Resultados.

En la *Fig. 2*, se incluye la valoración global de los estudiantes en la asignatura de Criptografía en la encuesta de calidad estandarizada SEEQ que se ha realizado en las últimas tres ediciones.

En particular, en la *Fig. 3*, se muestra al detalle la evolución en la valoración media obtenida en los bloques que motivaron la realización de esta experiencia.

En la *Fig. 4*, se incluyen los resultados obtenidos en el cuestionario sobre el portafolio como herramienta didáctica para Criptografía.

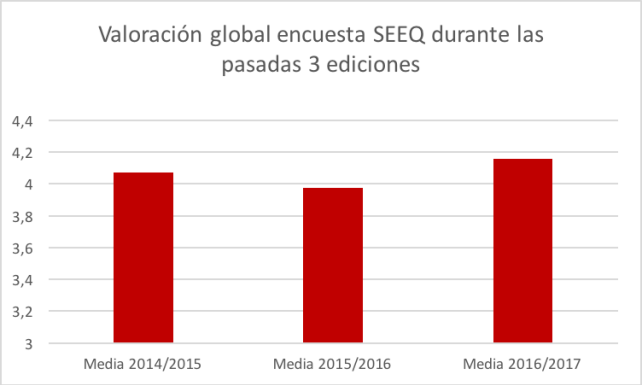

Fig. 2. Comparativa medios globales de la encuesta SEEQ en Criptografía.

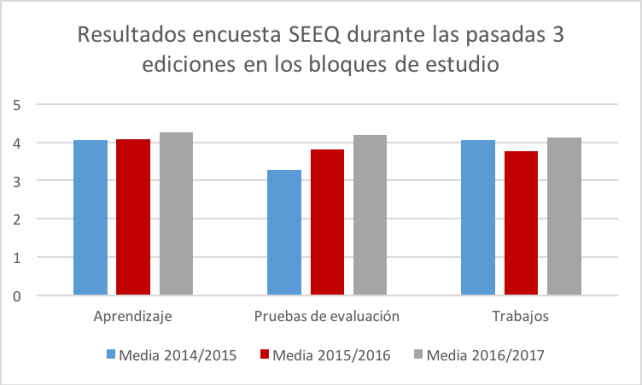

Fig. 3. Evolución de valoración en los bloques objeto de estudio.

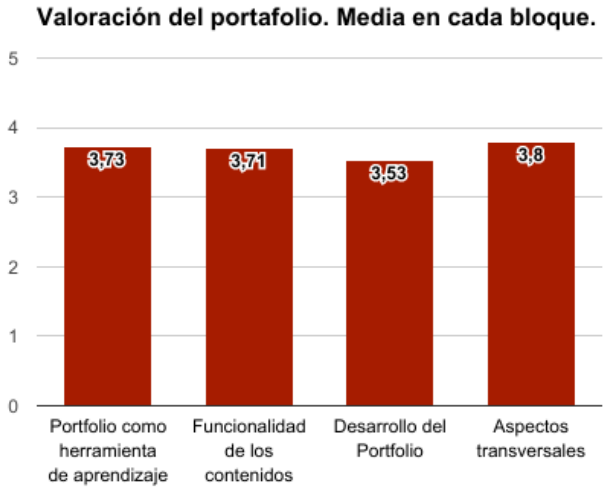

Fig. 4. Resultados del cuestionario sobre el Portafolio por bloques.

En la Tabla IV se encuentran las afirmaciones del Bloque de Aspectos transversales que obtuvieron las puntuaciones más altas.

Se detalla, en la *Fig. 5*, el desglose de las valoraciones recibidas en el bloque de Funcionalidad del aprendizaje.

TABLE IV
ÍTEMS MEJOR VALORADOS EN EL BLOQUE DE ASPECTOS TRANSVSERSALES.

Ítem	Media sobre 5
Me gustaría escribir el portafolio en otras asignaturas.	4.28
Escribir el portafolio debería ser parte de un programa de Ciberseguridad.	4
Escribir el portafolio ha aumentado mi interés en la asignatura.	4

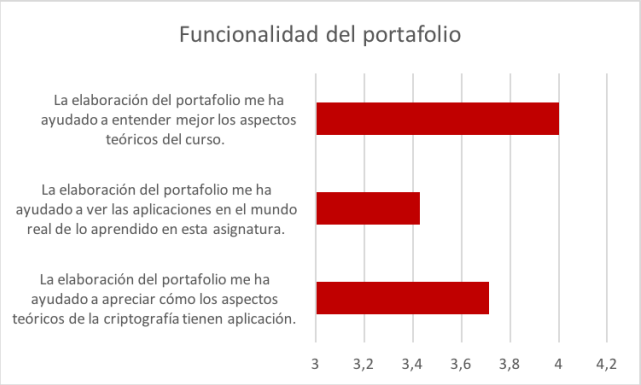

Fig. 5. Resultados del Bloque de Funcionalidad.

VI. Discusión.

Como podemos ver en las *Fig. 2 y 3*, la valoración global de los estudiantes ha mejorado con respecto a la pasadas ediciones. En particular, la puntuación obtenida en los bloques que habían motivado la realización de esta experiencia, ha aumentado. Como aspecto a destacar, el portafolio ha implicado una mejora en el aprendizaje, y ha supuesto una evolución positiva en el ítem de pruebas de evaluación.

Uno de los objetivos principales del uso del portafolio durante esta experiencia, era que el aprendizaje de los estudiantes fuera más significativo. Como se puede observar en la *Fig. 4*, la puntuación media de todos los bloques en la evaluación del portafolio ha estado por encima de 3.5 / 5. Estos resultados nos muestran que la experiencia ha sido efectiva en la consecución de los objetivos propuestos. Aunque hemos obtenido una valoración por encima de 3 sobre 5 en todos los bloques, la interpretación de los resultados requiere un análisis más profundo y en detalle, que nos permita seguir buscando el planteamiento didáctico más efectivo que incluya el uso del portafolio en el aula. La puntuación más alta se ha obtenido en el Bloque de Aspectos Transversales. Cabe destacar, veáse Tabla IV, que los ítems mejor valorados están relacionados con la opinión positiva por parte de los estudiantes de la inclusión del portafolio en las propuestas metodológicas en los programas de formación en Ciberseguridad. Sin embargo, el bloque de Desarrollo del portafolio ha obtenido la media más baja. Por lo tanto, se ha de reflexionar sobre la estimulación del uso de los materiales didácticos que se aportaron al alumnado y la autoreflexión.

En esta experiencia, la comprensión de la importancia de los contenidos téoricos de Criptografía, y la aplicabilidad de éstos a situaciones reales de seguridad, por parte del alumnado, ha sido un desafío docente prioritario. Si observamos la valoración que ha obtenido este bloque, *Fig. 5*, podemos comprobar que el portafolio se presenta como una solución efectiva. Sin embargo, el uso de escenarios reales es una línea en la que se ha de seguir trabajando en el futuro.

Por otra parte, y realizando un análisis más detallado, se han identificado algunos aspectos a mejorar en futuras experiencias. Por ejemplo, se plantea elaborar más diversidad de proyectos para que la calificación del portafolio pueda ser más discriminante para la evaluación del alumnado. Además, si el número de alumnos es el adecuado, se plantearán proyectos en equipo que nos permitan fomentar el aprendizaje cooperativo. En futuros cursos se fomentará el uso del e-portafolio, [20], con proyectos más complejos en los que intervengan diferentes etapas de dificultad de aplicación de contenidos. Esta herramienta nos permitirá realizar un seguimiento más continuado y profundo del trabajo y evolución de los estudiantes, así como poder ofrecer un feedback más apropiado. En el caso de utilizar este tipo de portafolio interactivo mediante aprendizaje colaborativo, se utilizarán e-rúbricas (veáse [28]), y herramientas para la evaluación del trabajo en equipo, [29].

VII. Conclusiones.

La calidad en los programas educativos del Espacio Europeo de Educación Superior se dirige hacia la utilización de metodologías innovadoras y diversos procedimientos de evaluación, que impliquen una mejora constante en los procesos de enseñanza y aprendizaje, así como el desarrollo de competencias profesionales que ayuden a los estudiantes universitarios a introducirse en el mercado laboral en las mejores condiciones posibles.

La experiencia realizada y descrita en este artículo, en la asignatura de Criptografía, nos ha permitido comprobar que el uso del portafolio, enmarcado en una metodología de aprendizaje por proyectos, ha mejorado la valoración de los estudiantes, sobre todo en aquellos ítems que habían obtenido las puntuaciones más bajas en cursos anteriores, como la aproximación a las aplicaciones prácticas de los contenidos teóricos estudiados.

Así mismo, los alumnos han valorado positivamente el uso de esta herramienta en los programas de formación en ciberseguridad, lo que supone un aspecto a considerar en las metodologías futuras de otras materias y otros cursos.

Agradecimientos.

Este trabajo se ha realizado con el apoyo del Instituto Nacional de Ciberseguridad de España (INCIBE), y por el proyecto MTM-2013-45588-C3-1-P del Ministerio de Economía y Competitividad.

References

[1] Jain P. , Gyanchandani M., and Khare N.: ”Big data privacy: a technological perspective and review”, in *Journal of Big Data*, vol. 3, pp. 1-25, 2016.

[2] Carrillo Ruiz, J.A., *et al.*: ”Big Data en los entornos de Defensa y Seguridad”, Instituto Español de Estudios Estratégicos, 2013. Recuperado de http://www.ieee.es/Galerias/fichero/docs_investig/DIEEEINV03-2013_Big_Data_Entornos_DefensaSeguridad_CarrilloRuiz.pdf

[3] Gentry, C.,Fully: ” Homomorphic Encryption Using Ideal Lattices”, en *Proceedings of the Forty-first Annual ACM Symposium on Theory of Computing* ,STOC ’09, pp. 169 - 178, 2009.

[4] Hu V., Schnitzer A., Sandlin K.: "Attribute Based Access Control Definition and Considerations", en *Special Publicationdel National Institute of Standards and Technology*, 800-162, 2013. Recuperado de http://csrc.nist.gov/projects/abac/july2013_workshop/july2013_abac_workshop_abac-sp.pdf

[5] Chase, M. and Kamara, S.: "Structured Encryption and Controlled Disclosure", en *Advances in Cryptology*, pp 577-594, 2010.

[6] Curtmola, R. , Garay, J. , Kamara, S. and Ostrovsky, R: "Symmetric Searchable Encryption: Improved Definitions and Efficient Constructions", en *ACM Conference on Computer & Communication Security*, CCS'06, pp.79-88. 2006.

[7] Boneh, D., Kushilevitz, E. , Ostrovsky, O, Skeith, W.: "Public Key Encryption That Allows PIR Queries" en *Advances in Cryptology – CRYPTO 2007*, pp 50-67, 2007.

[8] van Dijk, M., Gentry, G., Halevi S., and Vaikuntanathan V. : "Fully Homomorphic Encryption Over the Integers", en *Eurocrypt 2010*, pp. 24-43, 2010.

[9] Ateniese, G., Kamara, S.and Katz j. : "Proofs of Storage from Homomorphic Identification Schemes", en *Advances in Cryptology – Asiacrypt, 2010*, pp.319 - 333, 2010.

[10] Shor, P. :"Polynomial-Time Algorithms for Prime Factorization and Discrete Logarithms on a Quantum Computer", en *Journal of Computation*, vol. 26, pp. 1484–1509, 1997.

[11] Bernstein, D. J., Buchmann, J., Dahmen, E. : *Post-Quantum Cryptography*, Ed. Springer. 2008

[12] Estándares de excelencia de la National Security Agency. Recuperado de https://www.nsa.gov/resources/educators/centers-academic-excellence/cyber-operations/requirements.shtml

[13] Información sobre el Master de Investigación en Ciberseguridad de la Universidad de León. Recuperado de http://www.unileon.es/estudiantes/estudiantes-master/oferta-titulaciones/mu-ciberseguridad.

[14] Perry R.P. and Smart J.C., "Effective teaching in higher education: research and practice", editado por Academic Press, New York, 1997.

[15] Verdugo Matés M.V, Cal Bouzada,M.I. :" Valoración de la enseñanza: SEEQ", en *Revista de Formación e Innovación Educativa Universitaria*, Vol. 3, N. 4, pp. 182-193, 2010.

[16] Información sobre el Master Profesional en Tecnologías de la Seguridad de la Universidad de León. Recuperado de http://masterseguridad.unileon.es.

[17] M.V. Carriegos, Noemí DeCastro-García and J.F. García-Sierra :" Main Challenges in Teaching/Learning of Mathematics for Cyber-security", en *Proceedings of First Conference of International Network for Didactic Research in University Mathematics (INDRUM 2016)*, pp.423-424. ISSN: 2496-1027, 2016.

[18] De Corral, I., Almajano, M., Domingo, J. : "La encuesta SEEQ como instrumento de mejora continuada: aplicaciones en diferentes contextos universitarios", en *Congrés Internacional de Docència Universitària i Innovació*. pp. 1-14, 2008.

[19] Zubizarreta, J. *et al*, *The learning portfolio: Reflective practice for improving student learning*, Bolton: Anker, 2004.

[20] Domínguez-García S., García-Planas M.I, Palau Martín R., Taberna Torre J.: "Uso del e-portafolio en la formación: el e-portafolio integral", en CIDUI Congrés Internacional de Docéncia Universitária i Innovació, 2015.

[21] Fink, L. D. *Creating significant learning experiences*. San Francisco: Jossey-Bass, 2003.

[22] Ashcroft DM, Hall J. : "Using portfolios to learn about prescribing: Qualitative insights into students experiences" en *Pharmacy Education*, Vol. 6, n. 1, pp. 1 - 5, 2006.

[23] Elango S, Jutti RC, Lee LK.: "Portfolio as a learning tool: Students' perspective", en *Annals of Academy of Medicine, Singapore*, Vol. 34, n.8, pp. 511 - 514, 2005.

[24] Barquero B., Bosch M. and Gascón J.: " Incidencia del aplicacionismo en la integración de la modelización matemática en la enseñanza universitaria de las ciencias experimentales", en *Enseñanza de las Ciencias*, Vol. 32, n. 1, pp. 83-100, 2014.

[25] Herramienta de criptografía. Recuperado de http://www.cs.du.edu/~petr/cryptographers_toolkit/cryptographers_toolkit.html

[26] Software Maxima. Recuperado de http://maxima.sourceforge.net/es/

[27] Herramienta disponible en https://pari.math.u-bordeaux.fr

[28] Domínguez-García S. , García-Planas M.I, Palau R., y Taberna J.: " Evaluating an e- portfolio for a linear algebra course using rubrics", en *Proceedings of INTED2015 Conference*, pp. 1366- 1372, 2015.

[29] Conde M.A., Rodríguez-Sedano *et al*,: "Evaluation of teamwork competence acquisition by using CTMTC methodology and Learning Analytics Techniques", en Proceedings of the Fourth International Conference on Technological Ecosystems for Enhancing Multiculturality, TEEM '16 , pp. 787-794 , 2016.

VIII. Material suplementario

A. Project I: Mathematical Foundations and Classical Cryptography.

We have intercepted the following message

tlwowmyjqtsubcmjsztosotwkkyotputrwzw
pruptuawwzowmjwttlwmjsztcfgujqtlkoowmyjqtsrwzwproupfsu
pawwzqpgowmjwttlwaws

Our spy agent has obtained a fragment of plaintext, and its corresponding ciphertext.

$\mathcal{P}$: *Indeed, as I learned, there were on the planet where the little prince lived, as on all planets, good plants and bad plants. In consequence, there were good seeds from good plants, and bad seeds from bad plants. But seeds are invisible. They sleep deep in the heart of the earth's darkness, until some one among them is seized with the desire to awaken. Then this little seed will stretch itself and begin, timidly at first, to push a charming little sprig inoffensively upward toward the sun. If it is only a sprout of radish or the sprig of a rose-bush, one would let it grow wherever it might wish. But when it is a bad plant, one must destroy it as soon as possible, the very first instant that one recognizes it.*

$\mathcal{C}$: *qprwwrcoqfwcjpwrtlwjwiwjwuptlwzfcpwtilwjwtlwfqttfwzjqpmwfqdwrcoupcffzfcpwtoguurzfcptocprhc rzfcptoqpmupoweywpmwtlwjwiwjwguurowwrobjukgurzfcptocprhcrowwrobjukhcrzfcptohytowwrocjwqpd qoqhfwtlwsofwwzrwwzqptlwlwcjtubtlwwcjtlorcjapwooyptqfoukwupwckupgtlwkqoowqxwriqtltlwrwoqjw tucicawptlwptlqofqttfwowwriqffotjwtmlqtowfbcprhwgqptqkqrfsctbqjottuzyolcmlcjkqpgfqttfwozjq gqpubbwpoqdwfsyzicjrtuicjrtlwoypqbqtqoupfscozjuytubjcrqolujtlwozjqgubcjuowhyolupwiuyfrfwtq tgjuiilwjwdwjqtkqgltiqolhytilwpqtqochcrzfcptupwkyotrwotjusqtcoouupcozuooqhfwtlwdwjsbqjotqp otcpttlctupwjwmugpqxwoqt*

Moreover, we know that the message has been encrypted in an alphabet of 26 letters, and with an affine transformation of individual characters (without taking into account blank spaces, periods or commas).

1) Using the stats's function in http://www.cs.du.edu/~petr/cryptographers_toolkit/cryptographers_toolkit.html, perform a frequence analysis and write the equations that let us obtain the encryption key.
2) Solve the equations above.
3) Compute a' and b', the decryption key.
4) Write the decrypt map.
5) Use the monalphabetic decryption function in http://www.cs.du.edu/~petr/cryptographers_toolkit/cryptographers_toolkit.html to decrypt the intercepted message.

B. Project II: Public Key Cryptography.

Instructions: In this data base you have to write your public keys and exchange messages with your classmates. You must send two ciphertexts (using the two cryptosystems seen in class, i. e, RSA and ElGamal) to the classmate that follows you on the list (the last user has to send the ciphertexts to the first user). You can find that list in the doc file with RSA public key.

C. Project III: Authentication and Cryptanalysis.

Instructions: Participants have to send short messages (aprox. 30 characters), digitally signed, through a public channel (a moodle forum).

All messages will use the following alphabet (if necessary, modify the first line of criptopari.gp):

Alf="ABCDEFGHIJKLMNOPQRSTUVWXYZ., "

Load library file criptopari.gp into PARI's memory with the command čriptopari.gp

1) Each participant will generate his/her own RSA keys, (nA,eA,dA) for sending, and (nB,eB,dB) for receiving.
2) You can use the pari commands provided in class to generate your private and public keys.
3) Each participant will post a message in the forum indicating his name and the values of nA,eA,nB,eB,k (dA,dB must be saved). Each message sent to this user must be EXACTLY k characters long.
4) In order to send a message from A to be, sender A uses his values (nA,dA) and the values (nB,eB) of the recepient B.
   The signed message is generated this way:
   firmarRSA(message,nA,dA,nB,eB)
   where message="....." is a text string whose length is EXACTLY EQUAL to the value of k published by the recipient B (fill in with spaces, dots or commas if necessary).
   In the forum, publish something like this: message from ... to ..., including the text output when executing the previous command.
5) In order to decrypt and verify the received message, B does:
   verificarfirmaRSA(cryptogram,nA,eA,nB,dB)
   where cryptogram is the received string "...."
6) In a first round of messages, only the authorized recipients will try to read the messages.
7) As will be seen, the keys are too short, the modules can be factorized, and the private keys obtained. Therefore, we now begin a second stage: reading unauthorized messages, replacing someone else's identity, modify a message, etc.

D. FINAL PROJECT: Decrypting secure connection information

Instructions:

1) Choose a secure website.
2) Click on the lock icon to access the information about how the secure connection is established. You should obtain a window with information similar to shown in *Fig. 6*:

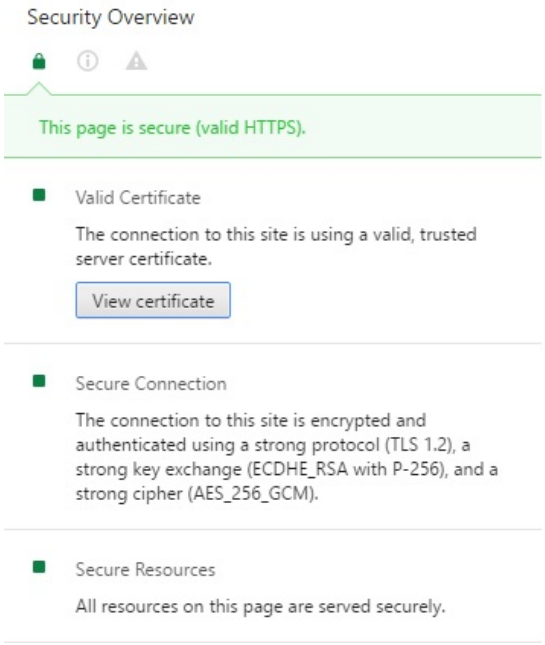

Fig. 6. Final project: Decrypting secure connection information

3) You need to explain all the details about the following items:
   a) Valid Certificate:
      - Reason why certificates are needed.
      - Certification authority that issued the certificate.
      - Expiration date of the certificate.
      - Digital signature algorithm used.
      - Hash function used.
   b) Secure connection:
      - Explain which protocol is used.
      - Give an overview on how TLS works.
      - Explain how the connection is secured and which different algorithms are used to guarantee this secure connection. You need to explain which kind of algorithms they are and give an overview about them.
      - Explain why you think those algorithms and modes of operations have been chosen.
4) Submit a document with the solutions via Moodle: if you have a handwritten version, you can scan the document or simply take a picture of the solutions and include it in the document.