FACULTAD DE CIENCIAS FÍSICAS

GRADO EN INGENIERÍA ELECTRÓNICA DE COMUNICACIONES

Curso 2019-20

Ficha de Trabajo Fin de Grado

DEPARTAMENTO:	Arquitectura de Computadores y Automática	
TÍTULO:	Implementación reconfigurable de algoritmos criptográficos	
TITLE:	Reconfigurable implementation of cryptographic algorithms	
SUPERVISOR/ES:	José Luis Imaña Pascual	
NÚMERO DE PLAZAS:	2	
ASIGNACIÓN DE TFG:	Selección directa ☒	Selección por expediente ☐

OBJETIVOS:

Al finalizar el trabajo, el alumno será capaz de:

- Comprender las bases criptográficas y el funcionamiento de distintos algoritmos de cifrado.
- Comprender las operaciones involucradas en dichos algoritmos.
- Realizar la descripción en un lenguaje de descripción de hardware utilizando herramientas de diseño electrónico automatizado.
- Realizar la simulación e implementación reconfigurable de dicha descripción.
- Analizar e interpretar los resultados obtenidos.

METODOLOGÍA:

- El alumno adquirirá los conocimientos básicos necesarios sobre criptografía y realizará un estudio previo de distintos algoritmos de cifrado.
- El alumno realizará una descripción sintetizable en el lenguaje de descripción de hardware VHDL de uno de los algoritmos criptográficos.
- El alumno utilizará una herramienta de diseño electrónico automatizado para la implementación y simulación de dicha descripción sobre dispositivos reconfigurables.
- El alumno realizará el análisis de los resultados experimentales obtenidos y extraerá conclusiones de los mismos.

ACTIVIDADES FORMATIVAS:

Tutorías de un profesor experto en el tema.

BIBLIOGRAFÍA:

1.- A.J. Menezes, P.C. van Oorschot, S.A. Vanstone. “Handbook of Applied Cryptography”, CRC Press, 1997.

2.- J. Pastor Franco, M.A. Sarasa López, J.L. Salazar Riaño. “Criptografía Digital. Fundamentos y Aplicaciones”, Prensas Universitarias de Zaragoza, 2001.

3.- S. Brown, Z. Vranesic. “Fundamentos de lógica digital con diseño VHDL”, McGraw-Hill, 2000.

4.- P.J. Ashenden. “The designer’s guide to VHDL”, Morgan Kaufmann, 2008.