

CURVAS ELÍPTICAS EN LA CRIPTOGRAFÍA

Sofía Almeida Bruno
Antonio Coín Castro
José María Martín Luque

Historia de las Matemáticas
Grado en Matemáticas
UNIVERSIDAD DE GRANADA

15 de noviembre de 2019

ÍNDICE

1	INTRODUCCIÓN	3
2	CURVAS ELÍPTICAS	3
2.1	<i>Curvas elípticas sobre los números reales</i>	3
2.2	<i>Curvas elípticas sobre cuerpos finitos</i>	3
3	EVOLUCIÓN DE LAS CURVAS ELÍPTICAS EN LA CRIPTOGRAFÍA	3
3.1	<i>Criptografía anterior a los años 80</i>	3
3.2	<i>Primera aparición de las curvas elípticas en criptografía</i> .	3
3.3	<i>“Paradigm shift”</i>	3
3.4	<i>Estado actual y algoritmos utilizados</i>	3
4	USOS FUTUROS	3

1. INTRODUCCIÓN
2. CURVAS ELÍPTICAS
 - 2.1. *Curvas elípticas sobre los números reales*
 - 2.2. *Curvas elípticas sobre cuerpos finitos*
3. EVOLUCIÓN DE LAS CURVAS ELÍPTICAS EN LA CRIPTOGRAFÍA
 - 3.1. *Criptografía anterior a los años 80*
 - 3.2. *Primera aparición de las curvas elípticas en criptografía*
 - 3.3. *“Paradigm shift”*
 - 3.4. *Estado actual y algoritmos utilizados*
4. USOS FUTUROS

REFERENCIAS

- [1] S. T. Abedon, P. Hyman y C. Thomas. "Experimental examination of bacteriophage latent-period evolution as a response to bacterial availability". En: *Applied and Environmental Microbiology* 69 (2003), págs. 7499-7506.