TEORÍA DE CÓDIGOS Y CRIPTOGRAFÍA

Curso 2010–11

TRABAJOS VOLUNTARIOS

CRIPTOGRAFÍA

1. La máquina ENIGMA. 50898167 y 51091419
2. Funciones de resumen (hash). 53455565
3. DES (Data Encryption Standard): Descripción y posibles ataques. 52478032 y 4619118
4. AES (Advanced Encryption Standard): Descripción y posibles ataques. 50764728 y 53500515
5. Protocolos de conocimiento cero. 2720548, 78945073, 70076525
6. Aplicaciones a las comunicaciones. 50860035 y 50113631
7. Aplicaciones bancarias. 70076780, 50388040 y 46836650
8. Protocolos de firma digital. 2266963
9. Criptosistemas basados en el problema de la mochila: Descripción y posibles ataques. 5288264 y 50760647

FACTORIZACIÓN Y PRIMALIDAD

10. Curvas elípticas y Factorización. 50902327 y 51117108
11. Curvas elípticas y Primalidad. 9028448
12. Test de primalidad de Miller-Rabin. 53455767 y 47302148
13. Símbolos de Jacobi y primalidad: Test de Solovay-Strassen. 53500115
14. Números de Mersenne y Test de Lucas-Lehmer. 51102452
15. Test de primalidad AKS ("Primes is in P"). 45665662
16. El método de factorización rho de Pollard. 70074630, 47306417 y 50770410
17. El método de factorización $p-1$ de Pollard. 53657141 y 70079515
18. El método de factorización mediante fracciones continuas. 51077416 y 71227426
19. La criba cuadrática. 5289306
20. Ataques contra RSA. 47454532 y 2711892

CÓDIGOS DETECTORES/CORRECTORES

21. Códigos de Huffman. 70082199
22. Códigos de Golay. 51478244 y 44553728
23. Teorema de Shanon. 48996893
24. Códigos compresores. 53502375