Adivinando passwords. Una propuesta para su búsqueda eficiente

Alejandro Mor Michael

Índice

1. Íntroducción
   - Criptografía
   - Funciones resumen
2. Búsqueda de colisiones
   - Algoritmo de Yuval
3. El ataque del arco iris
4. Experimentación
5. Discusión de resultados
6. Conclusiones
7. Referencias

[?]

[1, 2]

[3, 4, 5] [6]

[7]

Referencias I


Martin Hellman.
A cryptanalytic time-memory trade-off.
IEEE transactions on Information Theory, 26(4):401–406, 1980.


Dorothy Elizabeth Robling Denning.
Cryptography and data security.
page 100, Addison-Wesley Longman Publishing Co., Inc., 1982.


Mario Cortina Borja and John Haigh.
The birthday problem.
Significance, 4(3):124–127, 2007.


Ralph Merkle and Martin Hellman.
Hiding information and signatures in trapdoor knapsacks.
IEEE transactions on Information Theory, 24(5):525–530, 1978.

Referencias II

Stephen Pohlig and Martin Hellman.
An improved algorithm for computing logarithms over gf (p) and its cryptographic significance (corresp.).
IEEE Transactions on information Theory, 24(1):106–110, 1978.

Whitfield Diffie and Martin E Hellman.
Special feature exhaustive cryptanalysis of the nbs data encryption standard.
Computer, 10(6):74–84, 1977.

David H Wolpert, William G Macready, et al.
No free lunch theorems for optimization.
IEEE transactions on evolutionary computation, 1(1):67–82, 1997.