ZMATH 2010d.00617

Leonesi, Stefano

The knapsack and its secrets. (Knapsack: lo zaino e i suoi segreti.)

Boll. Docenti Mat., No. 57, 21-30 (2008).

Summary: What do knapsacks, mathematics and secret codes share? In this paper we discuss the knapsack problem (or subset-sum problem) and its applications to public-key cryptosystems. Their past and future are considered and evaluated, basically in terms of security and efficiency.

Classification: P20 F60
Keywords: knapsack cryptosystems; Merkle-Hellman cryptosystem; elementary number theory