Adleman, Leonard M.

On breaking the iterated Merkle-Hellman public-key cryptosystem. (English) Zbl 0543.94011

Advances in cryptology, Proc. Workshop Santa Barbara/Calif. 1982, 303-308 (1983).

[For the entire collection see Zbl 0511.00040.]

The Merkle-Hellman public-key cryptosystem [*R. C. Merkle* and *M. E. Hellman*, IEEE Trans. Inf. Theory IT-24, 525-530 (1978)] is based on the knapsack problem, both a basic method and an iterated method were presented in the mentioned paper. The iterated method was introduced "for improving the security and utility of the basic method." *A. Shamir* [Proc. 23rd Ann. Symp. Found. Comput. Sci. 1982] demonstrated that the basic knapsack cryptosystem was insecure. In addition, Shamir states that the most important remaining open is the cryptographic security of the iterated systems. In this paper, we build upon Shamir's results to establish the insecurity of the iterated systems as well.

MSC:

94A60 Cryptography

Cited in **1** Document

Keywords:

cryptology; Merkle-Hellman public-key cryptosystem; knapsack problem; security; iterated systems