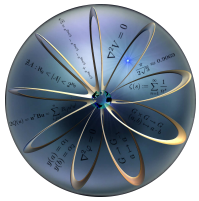

planetmath.org

Math for the people, by the people.

Merkle-Hellman scheme

Canonical name	MerkleHellmanScheme
Date of creation	2013-03-22 15:12:40
Last modified on	2013-03-22 15:12:40
Owner	aoh45 (5079)
Last modified by	aoh45 (5079)
Numerical id	5
Author	aoh45 (5079)
Entry type	Definition
Classification	msc 94A60
Synonym	Merkle-Hellman cryptosystem

The *Merkle-Hellman* cryptosystem was one of the earliest examples of public key cryptography, and depends on the NP-complete problem "SUBSET SUM" for its security.

Suppose Bob wants to send Alice a message.

Alice generates private key $a_1, a_2, \ldots a_n$ which is a superincreasing sequence. She then picks $d \gg \sum_{i=1}^{n} a_i$ and h comprime with d. Using the euclidean algorithm, she finds h^{-1} such that $hh^{-1} \equiv 1 \pmod{d}$.

Alice now generates her public key $b_1, b_2, \ldots b_n$ where $b_i = ha_i \pmod{d}$ and sends this to Bob.

Bob breaks up his message into binary strings of length n. To send the string $m_1 m_2 \ldots m_n$ to Alice, he forms $C = \sum_{i=1}^{n} m_i b_i$ and sends C to Alice.

On receiving C, Alice forms $V = h^{-1}C \pmod{d}$. Now, since $b_i = ha_i \pmod{d}$, we have that $V = \sum_{i=1}^{n} m_i a_i$. Since a_i is a superincreasing sequence, it is easy to recover the m_i if you know V and a_i, and it takes $O(n)$ arithmetic operations.

In 1982, a fast algorithm was found for recovering the message knowing only the public key and the cryptogram C. It takes advantage of the fact that the public key b_i is not generated in a random way, but comes from a superincreasing sequence.