MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

# Merkle-Hellman Knapsack Challenge – Part 2

Author: Peter Uelkes

October 2022

# The Merkle-Hellman Knapsack (1/6)

Part 1 of this series described how to realize a symmetric encryption using a Merkle-Hellman knapsack (MHK), which has a special property. In doing so, the knapsack itself had to remain secret.

We now consider the MHK in the form originally proposed by Merkle and Hellman, in which it is suitable for asymmetric encryption (public-key encryption). [3]

The conversion of a message $\mathrm{P}$ into a decimal number $\mathrm{M}$ and further into a binary number $\mathrm{B}$ is done exactly as described in Part 1.

# The Merkle-Hellman Knapsack (2/6)

We again consider the example P="MTC3" with $M = 77846751$ and $B = 10010100011110101101111 1$ as well as the knapsack chosen by Alice

$$
\begin{aligned}
K_1 = [&593, 13, 6252407, 1327, 958200, 2568118886, 51234, 24023, 6, 3470,\\
&54136509, 160, 930178262, 3, 27, 102299137, 82, 15267027, 395469607,\\
&117674, 2064250, 5494084005, 18363310574, 337256, 2, 38825629419, 7920]
\end{aligned}
$$

Now, however, Alice keeps $K_1$ secret and chooses a number $m$ and a number $n$ co-prime to $m$, which is greater than the sum of all elements in $K_1$. Thus, with $\lambda$ as the number of elements in $K_1$, the following holds:

$$n > \sum_{i=1}^{\lambda} k_{1,i} \qquad \text{and} \qquad \mathrm{gcd}(m, n) = 1$$

# The Merkle-Hellman Knapsack (3/6)

Alice chooses $m = 2473$ and $n = 96847338883$.
Using $m$ and $n$, Alice now creates from $K_1 = (k_{1,1}, k_{1,2}, \ldots, k_{1,\lambda})$ a second knapsack $K_2 = (k_{2,1}, k_{2,2}, \ldots, k_{2,\lambda})$ according to the following rule:

$$k_{2,i} = m \cdot k_{1,i} \pmod{n} \qquad \text{for } i = 1, \ldots, \lambda$$

In our example, this results in:

$$\begin{aligned} K_2 = [&1466489, 32149, 15462202511, 3281671, 2369628600, 55880977683,\\ &126701682, 59408879, 14838, 8581310, 37032247874, 395680,\\ &72842047617, 7419, 66771, 59291088035, 202786, 37755357771,\\ &9522949281, 291007802, 5104890250, 28242300745, 87912452258,\\ &834034088, 4946, 40068720134, 19586160] \end{aligned}$$

# The Merkle-Hellman Knapsack (4/6)

The knapsack $K_2$ is now Alice's public key. If Bob wants to send the message "MTC3" to Alice, he encrypts it via the intermediate steps $M$ and $B$ by adding up the corresponding elements from $K_2$. In the example this results in $C' = 359290848768$. To decode this using only the knapsack $K_2$, one would have to solve the subset-sum problem for $K_2$ and $C'$. Since $K_2$ does not have the special property that makes this easy, this task is hard.

Alice, on the other hand, does not solve this problem at all, but computes $m^{-1} \pmod n$, so in our example:

$$2473^{-1} \pmod{96847338883} = 17113743264$$

# The Merkle-Hellman Knapsack (5/6)

From this Alice now obtains $C' \cdot m^{-1} \pmod{n}$, so in the example:

$359290848768 \cdot 17113743264 \pmod{96847338883} = 60846205466$

Now Alice solves the subset-sum problem for $K_1$ and $C = 60846205466$, which is easy because of the special property of $K_1$. It can be shown that the two problems (solving the subset-sum problem for $K_1$ and $C$ or for $K_2$ and $C'$) are equivalent, i.e., give the same binary number $B$. [3]

So Alice's private key consists of

$$\left(K_1, m, n, (m^{-1} \mod n)\right)$$

and her public key is $K_2$.

# The Merkle-Hellman Knapsack (6/6)

In 1983, Shamir was able to show that the simple Merkle-Hellman knapsack was insecure. Subsequently, the attack method "*lattice reduction attack*" (basis reduction in lattices) was developed, which uses means from linear algebra. These are also used in other MTC3 challenges. It can be shown that under certain conditions this attack leads to success with a high probability. [3, 5]

An approximate algorithm for basis reduction in lattices is known as the *LLL algorithm*, named after its inventors Lenstra, Lenstra and Lovàsz. It is implemented, for example, in SAGE. [6]

# Challenge

The Merkle-Hellman knapsack method described above was used to encrypt an English plaintext. The public key, i.e., the knapsack $K_2$, as well as the ciphertext $C'$ are in the additional file *knapsack_part2_add.txt*. The length of $B$ and thus also of $K$ is $\lambda = 266$.

Decrypt the ciphertext. The solution to this challenge is the plaintext in the exact notation resulting from the ASCII encoding (including any spaces and punctuation).

# Resources (1/2)

1. Wikipedia article: en.wikipedia.org/wiki/Merkle-Hellman_knapsack_cryptosystem
2. David Kahn: “The Code-Breakers”, Revised version from 1996
3. M. Stamp, R. Low: “Applied Cryptanalysis – Breaking Ciphers in the Real World”, 2007

# Resources (2/2)

4. Wikipedia article on the subset-sum problem: en.wikipedia.org/wiki/Subset_sum_problem
5. Jinsu Kim: "Analysis of Knapsack Cryptanalysis via Lattice – A Survey", IJCSNS International Journal of Computer Science and Network Security, Vol. 20 No.9, September 2020
6. SageMath (free open-source mathematics software system licensed under the GPL): www.sagemath.org

# Additional files

→ `knapsack_part2_add.txt`: The ciphertext $C'$ and the knapsack $K_2$ of the challenge