MA080G Cryptography Summary Block 3

Viktor Rosvall

May 13, 2019

Discrete Logarithm problem

Knapsack problem [1]

Let's say we have a *knapsack* with a volume of b units, and a list of items $a_1, a_2, ..., a_k$. We want to know if we can fill the knapsack with *some* of the items.

We want to find a tuple e of length k, where $e \in \{0, 1\}$, and

$$\sum_{i=0}^{k} e_i a_i = b.$$

The knapsack problem is NP since we can easily check if a solution is correct. Finding this solution is hard. We have in the worst-case 2^k possible e tuples to check.

Merkle-Hellman knapsack cipher

ElGamal cryptosystem

Sophie-Germain primes

References

[1] P. J. Cameron, *Notes on cryptography*.
`http://www.maths.qmul.ac.uk/ pjc/notes/crypt.pdf` Page 78-80