ALI BOUKRICH
STUDENT, MATHEMATICAL AND PHYSICAL SCIENCES

USING THE LLL ALGORITHM IN ATTACKING KNAPSACK CRYPTOSYSTEMS

Knapsack problems are relevant in the fields of complexity theory, applied mathematics and cryptography. In this project, we analyze the security of the knapsack cryptosystem using super increasing sequences which is proposed by Merkle and Hellman. We will show that using the LLL algorithm one can break this public key system in polynomial time.

Research Advisor: Dr. Ha Tran