Solving a Cryptography Problem Using the Master Pyraminx

Zhang, Alexander (School: Lynbrook High School)

Purpose: There is always a pressing need for secure cryptography. Most problems used in cryptography act on finite abelian groups, which are groups with finite elements with all pairs of elements commuting. Finite non-abelian groups are generally harder to use but are faster than finite abelian groups. The Master Pyraminx can represent finite non-abelian groups, making their use in cryptography easier to understand. Procedure: The group structure of the Master Pyraminx was found using group theory. Properties of the Master Pyraminx were found through analysis of the group structure. The program to verify the group structure and solve any configuration was written in python. Configurations to test the program were generated manually. Observations/Data/Results: The Master Pyraminx had 8.2E+24 total configurations, which is when the puzzle is disassembled and randomly reassembled. 2.2E+17 of the configurations were solvable, meaning they were in the same orbit as the starting configuration. Finite non-abelian groups need to use different cryptography protocols for encryption and decryption than finite abelian groups, so the Master Pyraminx was used in a key exchange and a public key cryptosystem. Conclusions: Having 80 bits of security, which takes 1.2E+24 operations to hack, is currently considered safe, so with nearly 8.2E+24 total configurations, the Master Pyraminx is feasible in cryptography. This implies that non-abelian groups can have great potential in cryptography, especially larger groups.

Awards Won:
Mu Alpha Theta, National High School and Two-Year College Mathematics Honor Society: Second Award of $1,000