Private-Key Cryptosystem Using p x p x p Rubik's Cube Group

Viboonsunti, Pasawat (School: Kamnoetvidya Science Academy)

Rungruengsakorn, Sirada (School: Kamnoetvidya Science Academy)

In modern cryptosystems, even if the adversaries can access the communication medium and initially have the same knowledge as the communicators, sent messages are still safe, since they are guarded by the computational complexity, which requires impractical cracking time. Current cryptosystems capitalize on the computational complexity of mathematical structures. For instance, ECC relies on elliptic curves, and RSA relies on prime numbers, but there is a structure we found brimming with potential that had never been fully developed into a cryptosystem, the Rubik’s cube. Some have studied only the 3 x 3 x 3 Rubik’s cube, which lacks in amount of configuration required for long cracking times, while some others have initiated methods that we found less secure. This inspired us to expanded the size of the regular 3 x 3 x 3 to Rubik’s cube with the size of an arbitrary prime number and constructed a new cryptosystem by extracting its complexity, which escalates as the size increases. In this project, we have designed, proved, and tested various elements of our cryptosystem. First, we have defined a mathematical group of the Rubik’s cube then proved the various properties of the Rubik’s cube that leads to its complexity. Next, we designed the algorithm to map each text message to its corresponding configuration of the Rubik’s cube. Then we showed how this idea could be applied to establish secure communication between two parties. Lastly, we test the potential and vulnerability of the cryptosystem created.