GROUP THEORY PROJECTS

These are non-evaluative projects. If you find a topic interesting you can collaborate and work on them. Topics are not balanced in difficulty and some projects have a better road map than others.

Contents

1 Rotation

Hamilton's quaternions provide a mathematical model to express three dimensional rotations without the problem of gimbal lock.
This project is similar to 3Blue1Browns's video about quaternions and draws from his explorable webpage about them.

1.1 Reading Material

3Blue1Brown's video.
Quaternions and Rotation, `graphics.stanford.edu`
Visualizing Quaternions, Andrew J. Hanson.

1.2 Project requirements

Provide some mathematical background on Hamilton's quaternions.
Describe instances of gimbal lock when using euler angles.
Build an interactive model that accepts $(\theta_1, \phi_1), (\theta_2, \phi_2)$ as inputs and outputs the quaternion that rotates a fixed camera from (θ_1, ϕ_1) to (θ_2, ϕ_2) along with an animation that illustrates the rotation.

2 Encryption

This project will examine the vulnerabilities in a poorly implemented Diffie Helman encryption process.

2.1 Reading Material

RSA Cryptosystem, `crypto.stanford.edu`
Discrete Logarithms, `kuleuven.be/cosic`
Basic Algorithms, `math.auckland.ac.nz/crypto-book`

2.2 Project requirements

Provide some background, both historical and mathematical, on the Diffie-Helman scheme.
Build two objects Alice and Bob. Alice can encrypt messages and Bob can decrypt them, you can assume the message is just an integer $m < 7777774777777$.
Use the multiplicative group of integers modulo 7777774777777 to build an encryption channel between the two objects.
Build an object Eve that can intercept these messages and then try to decrypt them.
Run Bob and Eve's decryption algorithms in two parallel threads and see if Eve can decrypt the message within a time window t.
Note down your results with atleast two different attacks.

2.3 Stretch Goal

Try encrypting a 140 character message.

3 Fractals

This project will plot the cayley graph's of free groups in TEX.

3.1 Reading Material

Drawing with TikZ, `tex.stackexchange`
Free groups
Embedding, `math.stackexchange`

3.2 Project Requirements

Describe some of the properties of free groups.
Using the TikZ package, show that the free group generated by three elements can be embedded in a free group generated by two.

3.3 Stretch Goal

Can you plot an embedding of a free group generated by five elements?

4 Factorio

This project is based off of this post. The project will try to use factorio's belts to compute braid group operations.

4.1 Reading Material

Game Mechanics, `forums.factorio`
Braids, `math.osu.edu`

4.2 Project requirements

Provide some background on braid groups.
Use a long belt loop of copper plates and iron plates to represent the two strands of the braid.
The player can provide two signals to twist the braid in two opposing directions and the designed mechanism should reflect this change on the belts.

4.3 Stretch goal

Build a circuit in factorio that computes an integer equivalent to the current configuration.