HS Projects in ML-Cryptography: TO DO LIST

by William Gasarch

Here is our TO DO list for now

1. Do everything on the TO DO list for Crypto except the linear cong generators (you can do that for fun but it won't be needed later in your project). For now NOT including the stuff with letters and numbers since that introduces complexity we don't need yet.

2. Do the classification Project for Iris Flowers that David Zhen assigned you.

3. Write a program that will learn, given a text that was shifted, what it was shifted by. Note that it will train on LOTS of texts that are shifted.

4. Write a program that will learn, given a text that was coded by the affine cipher, what the a, b are. Note that it will train on LOTS of texts that are mapped by an affine function.

5. Write a program that will learn, given a text that was coded by the 2×2 matrix cipher, what the matrix is. Note that it will train on LOTS of texts that are mapped by a 2×2 matrix.

6. Extend to 3×3 matrix, 4×4, see when it stops working. Since there are MANY 20×20 matrices you may want to use a variant of the trick I had on the sides: first learn what happens to every 20th letter.

7. Write a program that will learn, given a text that was coded by a gen sub cipher, what the perm is. There are MANY perms so that might be an issue.