Classical Cryptography

by William Gasarch

Here is a list of projects and ideas for projects. They can also be combined.

1. Code up Shift, Affine, and Vigenere ciphers. Code up IS-ENGLISH program. Use those to crack them. Find what the right parameters are for the Affine cipher.

2. Code up a modified Vig and see if its harder to crack.

3. Code up General Sub cipher and a cracker for it.

4. Code up the matrix cipher for 2×2 matrices and a cracker. This should be easy. But then true 3×3, 4×4, and see if it gets harder (it probably will). You will need to know letter freq for blocks-of-2,3,$ldots$. I honestly don't know if, for large n (say $n = 10$) the 10×10 matrix cipher is uncrackable if using cipher-text only.

5. Code up random 2-letter gen sub, 3-letter gen sub, etc and crackers for them.

6. If you know Machine Learning, there may be ML ways to do any of the above. I think there has been some work on this, but you would need to do the ML part, though my assistant Josh can help.

7. Code up the method given to break a psudorandom generator. See if it works on the psuedorandom geneator in Python, Java, whatever or favorite language is.

8. If YOU come up with a project involving classical crypto we can discuss it and I can help you with it.