**Cryptanalysis of a class of ciphers based on**

**genetic algorithm**

WenQiang Bao(wb854) Min Kim(mjk884)

Oct 25, 2020

***Introduction***

As a group, we started by brainstorming different ideas and decryption techniques. In the early stage of the project, our ideas focused on letter frequency, probability distribution, and Kasiski attack. In the end, we decided to use a genetic algorithm to break ciphertext for both test cases. The code is written in Python. By giving different options to run both tests successfully.

We both contributed build ideas. WenQiang focused on implementing and testing the algorithm and Min contributed to the report and testing the algorithm.

***Informal explanation***

Our decryption algorithm is based on a Genetic Algorithm. This is great when we find a suitability function that reflects the fitness of a key. Therefore, we believe that efficient GA should consist of a good Suitability Function including crossover and mutation. First, we initialize the population. Then we find the fitness of the population. When it is in gram score we computed frequency distribution for all the bigrams in the text by building a score table, we added to fitness. After the first round of fitness calculation, depends on pcf value we give weight on fitness. Then we select parents based on fitness which is based on probability. Next, we do two-point crossover and mutation. We randomly chose two positions and swap. Note that we first randomly choose from 1 to 27 then choose from the offset. Based on transposition we calculate fitness and select the max fitness. Finally, we choose for the best.

Our decryption process can be simply written as follow:

GeneticAlgorithm()

initialize population

find fitness of population

while (termination criteria is reached) do

parent selection

crossover with probability // transposition

mutation with probability // transposition

fitness calculation

selection

find best

return best

***Rigorous description***

In this part we will look into our code more closely. The main function of our algorithm as follow.