Problem 1

Assuming 1000 4GHz machines can crack 2^{48} keys per second, How many years would it take to try all possibilities of 64 bit encryption? How many years would it take to try all possibilities of 128 bit encryption?

$$2^{64-48} = 2^{16} \text{ sec} \approx 18.204 \text{ hours}$$

$$2^{128-48} = 2^{80} \text{ sec} \approx 3.831 \times 10^{16} \text{ years}$$

Problem 2

Encrypt the message "we are all together" Using a double transposition cipher (of the type described in the course slides) with 4 rows and 4 columns, using the row permutation $(1, 2, 3, 4) \mapsto (2, 4, 1, 3)$ and the column permutation $(1, 2, 3, 4) \mapsto (3, 1, 2, 4)$.

$$\begin{Bmatrix} w & e & a & r \\ e & a & l & l \\ t & o & g & e \\ t & h & e & r \end{Bmatrix} \mapsto \begin{Bmatrix} e & a & l & l \\ t & h & e & r \\ w & e & a & r \\ t & o & g & e \end{Bmatrix} \mapsto \begin{Bmatrix} l & e & a & l \\ e & t & h & r \\ a & w & e & r \\ g & t & o & e \end{Bmatrix}$$

Problem 3

Using the ciphertext.txt file in the "SubstitutionProgramDistS20.zip" file associated with the assignment is an encrypted article about security that was created using a least simple substitution encryption. You must crack the key for the cipher from the encoded characters from the message. To do this use the same java tool we used in class (found on Blackboard in the zip file attached to this assignment). Make sure to read the "SubstitutionReadMe.txt" which explains how to use the program. Enter below the contents of the cipher.txt mapping (if a character(s) are never used just leave the mapping in upper case) and then the decoded text for the first sentence.

```
xbeadvfrqywiuzglmosjkctphn
ABCDEFGHIJKLMNOPQRSTUVWXYZ
```

employer demand for cybersecurity professionals across the united state continues is soaring, according to new data sourced by burning glass technologies.