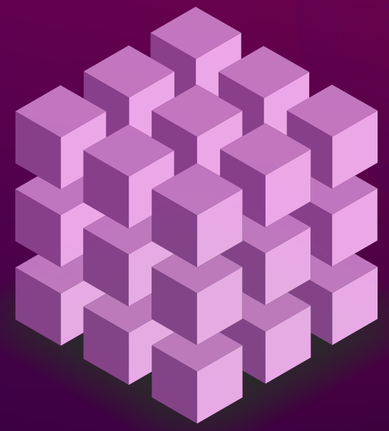
CSE350/550: Network Security

Assignment 01

Project 02



Transposition Cipher

Language Used

- Assembly
- C

Why?
We used Assembly because for our task of implementing a brute force method, we'll need to recursively test all potential keys. Given that this process is expected to consume the majority of the algorithm's time, employing Assembly, a low-level language, promises significantly faster execution.

As clear from the following results, our brute force algorithm is able to crack any length of cipher text in matter of miliseconds and in some cases miliseconds.

```
~/De/cm/senet/transposition_cipher on main ?1 time ./transposition_cipher bruteforce "oihczldehzwcddzlaegzelbidoehezhrdfj"
Ciphertext: oihczldehzwcddzlaegzelbidoehezhrdfj
Key: 7 5 2 4 1 3 6
Plaintext: helloworld
Hash: aicedbeehdhfihgcdejd
./transposition_cipher bruteforce "oihczldehzwcddzlaegzelbidoehezhrdfj"  0.00s user 0.00s system 79% cpu 0.004 total
```

```
~/De/cm/senet/transposition_cipher on main ?1 time ./transposition_cipher bruteforce "moiddtebccaajazaritnsdtebfgbhzifmiaaunbbgcadi"
Ciphertext: moiddtebccaajazaritnsdtebfgbhzifmiaaunbbgcadi
Key: 3 2 1
Plaintext: iamfromiiitdandastudent
Hash: bbecbbcgfacgaabjdhai
./transposition_cipher bruteforce   0.00s user 0.00s system 83% cpu 0.005 total
```

```
~/De/cm/senet/transposition_cipher on main ?1 time ./transposition_cipher bruteforce "tenbbaiiegcnnebktgeaahaccaioafteebifmgcztvrie"
Ciphertext: tenbbaiiegcnnebktgeaahaccaioafteebifmgcztvrie
Key: 6 9 1 2 3 4 5 7 8
Plaintext: attackatfiveinthemorning
Hash: aegaibeeecbcfebgbaci
./transposition_cipher bruteforce   0.02s user 0.00s system 98% cpu 0.025 total
```

Setup our project

- Use *nix environment to avoid and dependency related issues.
- install fasm - required to run assembly code and generate binary
  - https://flatassembler.net/download.php
- install gcc - required to run c code and generate the binary.
- After installing all necessary packages. Go into the transposition_cipher directory and issue a make command to generate all binary files

```
 ~/De/cm/senet/transposition_cipher  on  main  make
fasm decrypt.asm decrypt.o
flat assembler  version 1.73.32  (16384 kilobytes memory)
3 passes, 2008 bytes.
fasm encrypt.asm encrypt.o
flat assembler  version 1.73.32  (16384 kilobytes memory)
3 passes, 1584 bytes.
fasm hash.asm hash.o
flat assembler  version 1.73.32  (16384 kilobytes memory)
3 passes, 752 bytes.
gcc -no-pie transposition_cipher.c decrypt.o encrypt.o hash.o -o transposition_cipher

 ~/De/cm/senet/transposition_cipher  on  main ?1
```

Other Related Information can be found in README.md or transposition_cipher/Readme.md

Thank you!

Lakshay and Ankit