
HACK
UTK

Competition

- Runs until October 9
- Two problems
  - Substitution Cipher
  - Vigenere Cipher
- First person to submit a solution (to either) wins

Competition

- You can only win the easy problem once and you must be have not started CS 360 (So Freshman or Sophomore)*
- Awards awarded at the next meeting*

Substitution Cipher

- Instead of just using letters we have all valid ascii bytes (128! key size)
- For this problem I have provided the frequency in freq.txt
- The ciphertext is in encrypted.txt

Vigenere Ciphers

- Again we’re using binary instead of the alphabet
- Using xor instead of rotation
- First thing is to get the length

Breaking Vigenere

- Try to find the key length
  - Using analysis to find a distribution of characters that matches the text
  - Match the sum of the squares of the frequencies of given letters to see if it “looks” like english
  - If it looks like English then you’ve found the key length

Breaking Vigenere

- Then use a shift cipher to break each letter
- Or in this case test 0-128 to see if the text decrypts to english characters
- Find the flags

Problems

web.eecs.utk.edu/~cdean16/substitution.tar.gz

web.eecs.utk.edu/~cdean16/binary-vigenere.tar.gz

Answers

- Email your answers to hackutk@gmail.com
- Attend the next meeting to find out if you won

Problems

web.eecs.utk.edu/~cdean16/substitution.tar.gz

web.eecs.utk.edu/~cdean16/binary-vigenere.tar.gz