

Key length: 2

Key: KS

Decrypted Text: CAESARSWIFEMUSTBEABOVESUSPICION

Key length: 3

Key: KEY

Decrypted Text:

FORTUNEWHICHHASAGREATDEALOFPOWERINOTHERMATTERSBUTESPECIALLYINWARCANBRING  
ABOUTGREATCHANGESINASITUATIONTHROUGHVERYSLIGHTFORCES

Key length: 4

Key: IWKD

Decrypted Text: EXPERIENCEISTHETEACHEROFALLTHINGS

Key length: 5

Key: KELCE

Decrypted Text: IMAGINATIONISMOREIMPORTANTTHANKNOWLEDGE

Key length: 6

Key: HACKER

Decrypted Text:

EDUCATIONISWHATREMAINS AFTER ONE HAS FORGOTTEN WHAT ONE HAS LEARNED IN SCHOOL

**[Optional]** Key length: 7

**[Optional]** Key: NICHOLS

**[Optional]** Decrypted Text: INTELLECTUALS SOLVE PROBLEMS GENIUSES PREVENT THEM

### **Discussion:**

In general, computational complexity of brute force attacks:  $O(m \cdot c^n)$ , where  $n$  is the key length,  $m$  is the complexity of testing one key,  $c$  is the number of difference choices for each key character. That is, in naïve brute force, the average time required to break an encryption **increases exponentially with the key length**. In our experiment,  $c=26$ .

To test one key, the most time-consuming operation is to locate if the decrypted word is in the dictionary. If binary search is used, the time complexity of testing one key could be considered  $O(\log d)$ , where  $d$  is the length of the dictionary. The time complexity could be reduced to constant time, if a hash table is used.