CRYPTOGRAPHY CHALLENGE: CAESAR'S CIPHER

WHAT IS CAESAR'S CIPHER?

The Caesar cipher shifts all the letters of the alphabet in the text by a constant amount. For example, if the shift value is 2, the letter 'a' becomes 'c', letter 'b' becomes 'd', and so on.

The letters at the end of the alphabet wrap around it, so with the same shift value of 2 the letter 'y' becomes 'a' and 'z' becomes 'b'.

EXAMPLES

EXAMPLE 1

"Hello World Hack" using Caesar's cipher with a shift value of 2 becomes "Jgnnq Yqtnf Jcem".

EXAMPLE 2

"An apple a day keeps the doctor away" with a shift value of 5 becomes "Fs fuuqj f ifd pjjux ymj ithytw fbfd".

PREPARATIONS

Before starting this challenge, it's be good to have some paper and something to write with near you. You can also use a text editor on your computer instead, if you prefer so.

WARM-UP CHALLENGE

Knowing that the first word of the following text is "Welcome", try to decrypt it:

> Dlsjvtl av aol jyfwavnyhwof johsslunl vm aol Olssv Dvysk Ohjr! Pm fvb thuhnlk av kljvkl aopz tlzzhnl pa tlhuz aoha fvb hyl vu aol ypnoa ayhjr! Fvb jhu uvd tvcl vu av aol ulea whya vm aol johsslunl.

PROBLEM 1

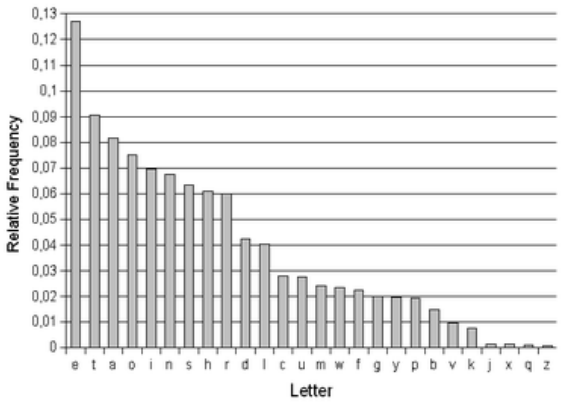
Julia is sending a secret message by SMS to her friend Scarlett. Knowing that the shift value is less than 10, try to decrypt the message:

> Qr Bljauncc! R jv qxumrwp j enah bnlanc kracqmjh yjach. R jv fjrcrwp oxa hxd jc vh qxdbn cqrb Oarmjh jc bnenw x'luxlt rw cqn nenwrwp.

PROBLEM 2

Kristina has found an old encrypted letter in her great grandmother's storage box. She doesn't know what the shift value is, so it could be any number from 1 to 25 (a shift value of 26 results in the same original letters). Kristina could try all shift values one by one, that she realises that might take too much time so she thinks of some tricks to make her task easier.

- She found a list of the most frequent words in English (in order of highest frequency from left to right):
  the, of, and, a , to, in , is, you, that, it, he, was, for, on, are , as, with, his, they, I, at, be, this
- She also found this graph online showing the most frequent letters in English words.



(Source: https://www3.nd.edu/~busiforc/handouts/cryptography/380px-English-slf2.png)

Using these tips, try to decrypt the letter:

> Fhmaxk,
>
> B tf lmbee axkx tm max N.L. Gtote Ahlibmte uxbgz ptmvaxw hoxk ur lhfx xqixkml bg max tkm hy ukbgzbgz hgx utvd mh ghkfte. B tf yxxebgz ybgx tgw wtgwr tgw pbla B ptl pbma rhn tgw max uhrl uxbgz lh vehlx, unm bm phg'm ux ehgz ghp, B ahix. B gxxwxw t lahkm kxlm yhk fr gxkoxl pxkx dbgw hy cbmmxkr. B atox uxxg ehhdbgz mh max ukbzam lbwx hy ebyx tgw xoxkrmabgz bl zhbgz mh mnkg hnm tee kbzam. Paxkx maxkx bl t pbee maxkx bl t ptr.
>
> Bl Wtw lmbee dbvdbgz mahlx vanuur exzl tkhngw tgw lfhdbgz abl ybox vxgm vbztkl? Ahp bl Ltgwyhkw'l ztkwxg vhfbgz tehgz B pbla B vhnew mtlmx lhfx hy maxf obvmhkr ztkwxg oxzxmtuexl hy abl. Exm'l axtk ykhf rhn tee.
>
> Ehox - Yktgd.

PROBLEM 3

The following text has been encrypted using Caesar's cypher, but there is also another way in which the text is modified. Can you decrypt the message?

> vqrlwdoxwdujqrf
>
> whhkv phoerus hkw ql vhjqhoodkf bksdujrwsbuf hkw ood ghvvds hy'xrb ,vlkw wsbufhg rw zrk wxr huxjli rw ghjdqdp hy'xrb il
>
> hjdvvhp ghvuhyhu d vl vlkw

SUBMIT YOUR ANSWERS

Submit your answers here: https://forms.gle/RxjY6JMpy14UAyra6.

YOU'VE FINISHED THE CHALLENGES!

Congratulations on finishing all the challenges. If you want to read more on cryptography, here are a few useful links:

A THREE PART SERIES: THE LEGACY OF WOMEN IN AMERICAN CRYPTOLOGY

https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2103832/the-legacy-of-women-in-american-cryptology-part-1/

https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2109747/the-legacy-of-women-in-american-cryptology-part-2/

https://www.nsa.gov/News-Features/News-Stories/Article-View/Article/2119320/the-legacy-of-women-in-american-cryptology-part-3/

MORE ABOUT CIPHERS AND THEIR USE IN REAL LIFE

https://www.cerias.purdue.edu/education/k-12/teaching_resources/lessons_presentations/cryptology.html