Criptografie și Securitate

Sistemul de criptare Cezar

(a) Studiați sistemul Cezar. Criptați un mesaj oarecare și vedeți cum funcționează.

Transformare în sistemul Cezar cu cheia de criptare k = 3:

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
DEFGHIJKLMNOPQRSTUVWXYZABC
```

Folosind alfabetul de mai sus putem cripta un mesaj:

```
MESAJ → PHVDM
```

(b) Decriptați următorul mesaj (este în engleză):

```
LZWJW SJW SDKG DWLLWJK GX ZAK LG UAUWJG SK OWDD SK LG ZAK AFLA
ESLWK GF HJANSLW SXXSAJK SFV AF LZW DSLLWJ AX ZW ZSV SFQLZAFY
UGFXAVWFLASD LG KSQ ZW OJGLW AL AF UAHZWJ LZSL AK TQ KG UZSFYA
FY LZW GJVWJ GX LZW DWLLWJK GX LZW SDHZSTWL LZSL FGL S OGJV UG
MDV TW ESVW GML AX SFQGFW OAKZWK LG VWUAHZWJ LZWKW SFV YWL SL
LZWAJ EWSFAFY ZW EMKL KMTKLALMLW LZW XGMJLZ DWLLWJ GX LZW SDHZ
STWL FSEWDQ V XGJ S SFV KG OALZ LZW GLZWJK LZW DANWK GX LZW US
WKSJK DAXW GX BMDAMK USWKSJ
```

La o scurtă privire asupra textului de mai sus observăm că litera W apare în majoritatea cuvintelor, deci putem deduce că este una dintre cele mai comune litere ale limbii engleze.

Inițial am corelat W cu litera A (cheia k = 22):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
EFGHIJKLMNOPQRSTUVWXYZABCD
```

Vedem încă din primul cuvânt că această decodificare nu este corectă:

```
LZWJW → PDANA
```

Apoi am încercat corelarea W → E (cheia k = 18):

```
ABCDEFGHIJKLMNOPQRSTUVWXYZ
IJKLMNOPQRSTUVWXYZABCDEFGH
```

Folosind această cheie, decodificarea primului cuvânt este un cuvânt existent în limba engleză:

```
LZWJW → THERE
```

Așadar, putem decodifica tot textul:

```
THERE ARE ALSO LETTERS OF HIS TO CICERO AS WELL AS TO HIS INTI
MATES ON PRIVATE AFFAIRS AND IN THE LATTER IF HE HAD ANYTHING
CONFIDENTIAL TO SAY HE WROTE IT IN CIPHER THAT IS BY SO CHANGI
NG THE ORDER OF THE LETTERS OF THE ALPHABET THAT NOT A WORD CO
ULD BE MADE OUT IF ANYONE WISHES TO DECIPHER THESE AND GET AT
THEIR MEANING HE MUST SUBSTITUTE THE FOURTH LETTER OF THE ALPH
ABET NAMELY D FOR A AND SO WITH THE OTHERS THE LIVES OF THE CA
ESARS LIFE OF JULIUS CAESAR
```

(c) Care este mesajul? Dar cheia?

Mesajul este cel prezentat anterior, iar cheia este k = 18.

(d) Câte chei posibile sunt?

Dacă folosim linkul de decriptare dat in laborator (https://www.boxentriq.com/code-breaking/caesar-cipher) și încercăm, pe rând, toate cele 26 de chei existente observăm că doar cheia 18 dă un text în limba engleză. Așadar, este o singură cheie posibilă.