1. Krüpteeri tekst „TALLINNA ÜLIKOOLI INFORMAATIKA INSTITUUT“ kasutades Caesari šifrit. Nihe *n* peab olema Sinu sünnikuupäevale vastav arv. Kirjelda tehtavate sammude põhimõtet ning esita krüpteerimist samm-sammult.

Abiks on järgmine tabel:

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| 1. a 2. b 3. c 4. d 5. e | 1. f 2. g 3. h 4. i 5. j | 1. k 2. l 3. n 4. m 5. o | 1. p 2. q 3. r 4. s 5. t | 1. u 2. v 3. w 4. x 5. y 6. z |

ning valem:



Dekrüpteeri neli esimest tähte, kasutades dekrüpteerimiseks mõeldut valemit 

1. Krüpteeri tekst „TALLINNA ÜLIKOOLI INFORMAATIKA INSTITUUT“ kasutades Vigenere’i šifrit ning võtmesõnana enda perekonnanimi. Kirjelda tehtavate sammude põhimõtet ning esita krüpteerimist samm-sammult.

Kasutades valemit C_i \equiv (P_i + K_i) \mod\ 26 kinnita enda tehtud sammude korrektsust (tähtede nummerdamine on 0-st 25-ni)

Abiks on eelnevas ülesandes toodud tabel.

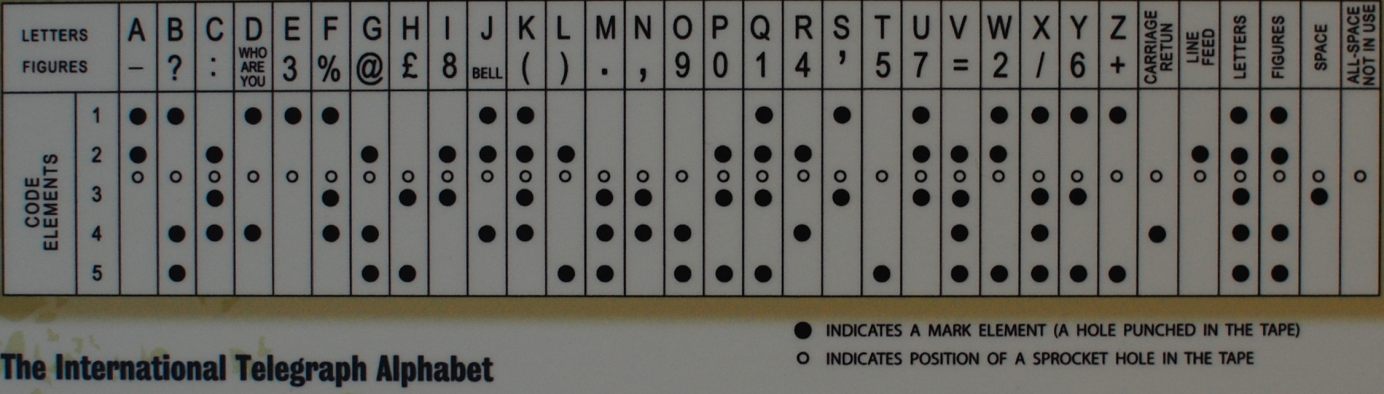
Kasutades dekrüpteerimiseks mõeldut valemit 

esita nelja esimese tähe dekrüpteerimist.

1. Võrdle lühidalt omavahel Enigma ja Lorenzi masinaid:

|  |  |  |
| --- | --- | --- |
|  | Enigma | Lorenzi |
| Rootorite arv |  |  |
| Substitutsioonide arv |  |  |
| Asenduste põhimõte |  |  |

1. Kirjuta sõna Tallinn ja sama pikkusega võti, mis on moodustatud Sinu nimest ja vajadusel perekonnanimest kasutades Baudot koodi, mis on toodut algjärgneval pildil:



1. Lorentzi masina šifris kasutatakse valemit: avatekst XOR võti = šifreeritud tekst. Kasuta eelnevas punktis saadud koode avateksti ja võtme jaoks ning arvuta šifreeritud tekst.

Teisenda saadut šifreeritud teksti kood tähtedeks.