

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:

0- a	5- f	10- k	15- p	20- u
1- b	6- g	11- l	16- q	21- v
2- c	7- h	12- n	17- r	22- w
3- d	8- i	13- m	18- s	23- x
4- e	9- j	14- o	19- t	24- y
				25- z

ning valem:

$$E_n(x) = (x + n) \pmod{26}.$$

Dekrüpteeri neli esimest tähte, kasutades dekrüpteerimiseks mõeldut valemit

$$D_n(x) = (x - n) \pmod{26}.$$

2. 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  $C_i \equiv (P_i + K_i) \pmod{26}$  kinnita enda tehtud sammude korrektsust (tähtede nummerdamine on 0-st 25-ni) Abiks on eelnevas ülesandes toodud tabel.

Kasutades dekrüpteerimiseks mõeldut valemit  $P_i \equiv (C_i - K_i) \pmod{26}$  esita nelja esimese tähe dekrüpteerimist.

3. Uurige CocoVila ekspertsüsteemi kübersündmuste liigitamiseks ning joonistage plokk skeemi vastavate kübersündmuste liigitamise visualiseerimiseks.
4. Uurige Vabariigi Valitsuse 12. augusti 2004. a määrust nr 273, mis asub aadressil <http://riigiteataja.ee/ert/act.jsp?id=791875> ning moodustage turvaklass
- ÕIS-is kasutavale andmekogule
  - ASIO tunniplaani andmekogule
  - Swedbank'i või mõne teise panga online-panga andmekogule.
  - E-hääletamises kasutavale andmekogule

Põhjenda oma valikuid.

Uri abiprogrammi, mis asub aadressil <http://www.ria.ee/isketooriist> (või loe juhendi, mis asub aadressil [http://www.ria.ee/public/ISKE/iske\\_kataloogid\\_5\\_00.pdf](http://www.ria.ee/public/ISKE/iske_kataloogid_5_00.pdf)) ning vali vajalikud turvamehhanismid.