PRAKTIKA

1. Definitu prozedure bat, Giltzak_definitu, ondokoa egin behar duena: p, q bi zenbaki lehenak emanik n modulua, r gako publikoa eta s gako pribatua kalkulatu. Prozedure hori osokoak.adb fitxategian osatu.

2. Aurreko prozedurarekin eta $p = 17$, $q = 23$ zenbaki lehenekin kalkulatu n, r, s balioak.

3. Erabil itzazu RSA algoritmoa eta aurreko ariketan kalkulatutako balioak eta kodetu 'kaixo.' mezua. Mezuak kodetzeko eta deskodetzeko prozedurak eta funtzioak mezuak.adb fitxategian daude.

4. Erabil ezazu RSA algoritmoa eta bigarren ariketan kalkulatutako balioak eta deskodetuko ondoko mezua: 79, 273, 77, 45, .

5. Erabil ezazu RSA algoritmoa, $n = 85$ eta $r = 3$ (gako publikoa) zenbakiekin eta kodetuko 'kaixo.' mezua.

6. Deskodetu aurreko ariketan lortutako emaitza $n = 85$ eta $s = 11$ (gako pribatua) zenbakiak erabiliz. Mezua ondo deskodetu da? Zergaitik?

7. Giltzak_definitu prozedurarekin eta $p = 97$ eta $q = 101$ zenbaki lehenekin kalkulatu n, r, s balioak.

8. Erabil itzazu RSA algoritmoa eta aurreko ariketan kalkulatutako balioak eta kodetu 'kaixo.' mezua.

9. Saiatu deskodetzen aurreko mezua.

10. Errepikatu 7., 8. eta 9. ariketak baina zenbaki hauekin:

$$p = 491 \text{ eta } q = 499$$

$$p = 991 \text{ eta } q = 997$$