Matematika Diskretua
Laboratorio saioa: RSA-zifratzea

Laboratorio saio honetan RSA-zifratzea landuko dugu R softwarea erabiliz. Hasteko, mezua **kodetu** behar da (ASCII kodeketara, adibidez, https://eu.wikipedia.org/wiki/ASCII), eta ondoren **zifratu**.

RSA zifratze-algoritmoa aplikatuz mezu bat zifratzea zera da: gako publikoa osatzen duten n eta r balioak erabiliz M_i kode bakoitza R_i bihurtzea, $\boxed{R_i = M_i^r \bmod n}$ berreketa modularra kalkulatuz. Deszifratzea, aldiz, gako pribatua den s balioa ezagutzen bada bakarrik burutu daiteke. Horrela, n eta s ezagunak izanik, R_i kode zifratu bakoitza M_i bihurtuko da $\boxed{M_i = R_i^s \bmod n}$ berreketa modularra kalkulatuz.

Mezuen kodeketarako eta RSA-zifratzea egiteko R funtzio hauek erabil ditzakegu:

- Berreketa modularra kalkulatzeko: `modpower(Ri,s,n)`. Adibidez, 65^{43} mod 85 berreketa modularra `modpower(65,43,85)` aginduaren bidez kalkulatuko dugu (aritmetika modularra gaiko ariketen orriko 8. ariketako bat da).
- Hizkien ASCII kodeak kalkulatzeko (hizkiz hizki edo hitz osoa kolpetik):

  `strtoi(charToRaw("k"),16L)`, `strtoi(charToRaw("kaixo"),16L)`
- ASCII kodeetatik hizkietara pasatzeko (kodez kode edo kode zerrenda bat kolpetik):

  `rawToChar(as.raw(107))`, eta hitz oso bat kolpetik pasatzeko,

  `hitza<-c(107,97,105,120,111)`, `rawToChar(as.raw(hitza))`

Gogoan izan oso handiak diren zenbakiak idazkera zientifikoan erakusten dituela R softwareak. Hala egin ez dezan eta a zenbaki bat bere osotasunean erakuts dezan, honako funtzioa erabil dezakezu: `format(a, scientific=FALSE)`.

1. **Ariketa**. Kodetzea / deskodetzea.

   - Idatz ezazu kodetu(txt) izeneko funtzio bat, parametro moduan "txt"karaktere string-a jaso eta dagozkion ASCII kodeak itzuliko dituena.

     ```
     kodetu <- function(txt)
       {
       }
     ```

     Probak:

     - `testu1=`"kaixo"izanik, `kodetu(testu1)` deiaren irteera:
       107 97 105 120 111
     - `testu2=`"KAIXO"izanik, `kodetu(testu2)` deiaren irteera:
       75 65 73 88 79
     - `testu3=`"Zer moduz?"izanik, `kodetu(testu3)` deiaren irteera:
       90 101 114 32 109 111 100 117 122 63

- Idatz ezazu deskodetu(kodetxt) izeneko funtzio bat, parametro moduan ASCII kodeak jaso eta dagokion karaktere string-a itzuliko duena.

```
deskodetu <- function(kodetxt)
  {
  }
```

Probak:

Aurreko funtzioarekin lortu dituzun ASCII kodeak parametro moduan jaso eta funtzioak "kaixo", "KAIXO"eta "Zer moduz?"mezuak itzuli behar ditu.

2. **Ariketa**. Zifratzea / deszifratzea.

- Idatz ezazu zifratu(kodebektorea,r,n) izeneko funtzio bat, ASCII kodeez osatutako bektore bati dagokion bektore zifratua itzuliko duena.

```
zifratu <- function(kodebektorea,r,n)
  {
  }
```

Zifratzea desberdina da erabiltzen diren RSA gakoen arabera. Proba bat egiteko, RSA_gakoak(97,101) zenbaki lehenetatik abiatuz lortutako n=9797, r=7 gako publikoa erabiliko dugu. "kaixo", "KAIXO"eta "Zer moduz?"mezuei dagozkien ASCII kodeen bektoreak parametro moduan jaso eta funtzioak honako mezu zifratuak itzuli behar ditu:

  - "kaixo", `zifratu(kodebektore1,7,9797)` deiaren irteera:
    2792 5432 4668 4973 7969
  - "KAIXO", `zifratu(kodebektore2,7,9797)` deiaren irteera:
    7976 4764 2565 8540 4974
  - "Zer moduz?", `zifratu(kodebektore3,7,9797)` deiaren irteera:
    375 2222 7721 3675 493 7969 6261 8564 4122 4604

- Idatz ezazu deszifratu(bektorezifratu,s,n) izeneko funtzio bat, bektore zifratu bat jaso eta dagozkion ASCII kodeak itzuliko dituena

```
deszifratu <- function(bektorezifratu,s,n)
  {
  }
```

Proba egiteko, n=9797, r=7 gako publikoari dagokion s=2743 gako pribatua erabiliko dugu. Aurreko funtzioarekin lortu dituzun bektore zifratuak parametro moduan jaso eta funtzioak "kaixo", "KAIXO"eta "Zer moduz?"mezuei dagozkien ASCII kodeak itzuli behar ditu.

Mezu berberak beste gako batzuek erabiliz zifra ditzakezu, adibidez:

- RSA_gakoak(17,23): $n = 391$, $r = 3$, $s = 235$.
- RSA_gakoak(307,397): $n = 121879$, $r = 5$, $s = 96941$.

Egin ezazu proba RSA_gakoak(5,17) zenbaki lehenetatik abiatuz lortutako gakoetarako (n= 85 r= 3, s= 43): Kodetu "kaixo"mezua, zifratu, deszifratu eta deskodetu. Ondo joan da prozesua? Hasierako "kaixo"mezua errekuperatu duzu? Zergatik?

3. **Jolasa**. Mezu zifratuak elkarri trukatuko dizkiogu. Mezuen trukea arbelean egingo dugu, publikoki. Arbelaren bitartez hartzaile eta bidaltzaile izan zaitezke.

   - Hartzaile izateko, idatz itzazu arbelean zure izena eta gako publikoa. Norbaitek zuri mezu zifratu bat bidaltzeko zain geratzen zara. Arbelaren bitartez ezin ditugu oso zenbaki handiak idatzi. Hortaz, gako txikiak erabiliko ditugu eta mezu motzak bidaliko dizkiogu elkarri.
   - Bidaltzaile izateko, beste norbaitek arbelean idatzitako gako publikoak erabiliz, mezu motz bat pentsatu, zifratu eta arbelean idatz ezazu, bere gakoen aldamenean.

   Gakoak eta mezu zifratua denok ikusiko ditugu arbelean. Gako txikiak erabiltzeak **enkriptatze-sistemaren porrota** frogatzeko aukera emango digu denoi. Deszifra itzazu zuri bidaliak izan ez diren mezuak. Horra porrota!!

Gako handiekin eta mezu luzeekin jolas egin nahi baduzu, korreo elektronikoa erabil dezakezu, zure gelakideren bati zure gako publiko handia pasa, hark bidalitako mezu zifratua deszifratzeko. Animatzen zara?