Pràctica 6: RSA

1. Esbrina el significat de la funció `FromDigits` del *Mathematica* per mitjà dels exemples següents:

```
?FromDigits
FromDigits[{1, 2, 3}, 10]
FromDigits[{1, 2, 3}, 100]
FromDigits[{1, 2, 3}, 95]
```

2. Esbrina el significat de la funció `IntegerDigits`.

Converteix la llista $\{9, 8, 7, 6, 5, 4, 3, 2, 1\}$ en un nombre escrit en base 95 i recupera els seus dígits:

```
nom95=FromDigits[{9,8,7,6,5,4,3,2,1},95]
IntegerDigits[nom95, 95]
```

3. En un directori RSA trobem l'adreça `(PQ = 11293220177790248609, e = 5)`.

(Aquesta clau no és gens segura, com comprovaràs a l'exercici següent.) Considera el missatge

```
mT = "Llistat de bancs en crisi"
```

Envia aquest missatge xifrat amb RSA a l'adreça anterior.

```
PQ = 11293220177790248609
e = 5
mA = ToCharacterCode[mT]
m95 = mA-32
m10 = FromDigits[m95,95]
mPQ = IntegerDigits[m10, PQ]
mPQX = Function[x, PowerMod[x, e, PQ]]/@ mPQ
mX95 = IntegerDigits[mPQX, 95]
mXT = FromCharacterCode[mX95+32] (*criptograma*)
```

4. Trenca la clau de l'exercici anterior i desxifra el missatge xifrat anterior.

```
{PP,QQ} = Transpose[FactorInteger[PQ]][[1]]
MM = LCM[PP - 1,QQ - 1]
d = PowerMod[e, -1, MM]
mXT
mXA = ToCharacterCode[mXT]
mX95 = mXA -32
mXPQ = Table[FromDigits[mX95[[k]], 95], {k, 1, Length[mX95]}]
mXPQY = Function[x, PowerMod[x, d, PQ]]/@ mXPQ
mXY10 = FromDigits[mXPQY, PQ]
mXYA = IntegerDigits[mXY10, 95] + 32
mXYT = FromCharacterCode[mXYA]
```

Obervació: Si en lloc d'utilitzar el mínim comú múltiple de `PP-1` i `QQ-1` s'utilitza el valor de la φ d'Euler, `Phi=(PP-1)(QQ-1)`, s'obté un (altre) valor de d que també es pot usar per a desxifrar el missatge.

5. Construeix-te una clau `(PQ, e, d)` per al sistema RSA:

(a) Tria dos nombres primers P, Q (una mica grans).

(b) Considera el mòdul PQ donat pel seu producte, calcula el mínim comú múltiple, M, de $P-1$ i $Q-1$ i tria un nombre natural $d > 1$ tal que $\mathrm{mcd}(d, M) = 1$.

(c) Calcula un nombre e solució de la congruència

$$d\,e \equiv 1 \pmod{M}.$$

(d) Fes pública la teva clau (PQ, e).

(e) Guarda't, i no mostris a ningú, la part privada de la teva clau (P, Q, d).