EXERCICI COMPUTACIÓ QUÀNTICA

Considereu el següent algorisme d'encriptació RSA.
ENCRIPTACIÓ:

1. Codifiquem l'alfabet en termes del codi ASCII decimal, usant sempre tres xifres. Ex: a = 097, m = 109, ...

2. Expressem el text pla per xifrar en una única string numèrica, P.

3. Llegim la clau pública del destinatari: (n = RSA-L , e), on n = RSA-L és un número de L dígits.

4. Trossegem P en tants blocs P_i (de L-1 dígits cada un) com facin falta (així $P_i < n$ està garantit). Al darrer bloc li afegim zeros a la dreta si cal per que també tingui L-1 dígits.

5. Encriptem cada bloc fent: $C_i = P_i^e \bmod n$. Ens assegurem que cada C_i tingui L dígits (afegim zeros a l'esquerra si cal).

6. Concatenem tots els C_i en una única string C. Enviem el missatge al propietari de la clau pública.

DESENCRIPTACIÓ
El receptor destinatari del missatge el desencripta fent:

1. Trenca la string encriptada C en blocs de L dígits, C_i (tants blocs com calgui).

2. Descodifica cada C_i amb la clau privada k: $P_i = C_i^k \bmod$ n. Cada P_i l'expressa en $L-1$ dígits (afegint zeros a l'esquerra si cal).

3. Concatena tots els P_i per fer una string numèrica desxifrada, P. (ULL: si els tres primers números de P son superiors a 254, el codi ASCII extès màxim, modifica P afegint un zero a l'esquerra)

4. Agrupa la string numèrica P en grups de tres dígits. Han de ser codis ASCII.

5. Tradueix els codis ASCII en els caracters alfabètics corresponents i recomposa el missatge de text original, P.

Exercici:

Heu tingut accés a un missatge, C, xifrat amb RSA i adjuntat amb aquest fitxer, per un destinatari que usa la següent clau pública:

$$(n = \text{RSA-11} = 13011817607, e = 3127313).$$

Sabem que RSA-11 es MOLT poc segur i volem advertir-lo. Per això, li desxifrareu el missatge i li enviareu el missatge desxifrat. Per més seguretat, hi afegireu la vostra signatura encriptada amb PGP (Pretty Good Privacy)

Feu un programa que:

1. Factoritzi n (metode clàssic senzill).
2. Obtingui la clau privada, k.
3. Desencripti C, seguint l'algorisme descrit anteriorment.
4. Escrigui el missatge original desencriptat, P.
5. Afegiu al final del fitxer la vostra signatura encriptada via PGP, amb el següent format:

   - - - - - - - - - -PGP- - - - - - - - - -

   n_v

   e_v

   signatura PGP

   on (n_v,e_v) és la vostra clau pública RSA, que us heu de generar vosaltres mateixos. La poseu aquí en lloc d'un repositori públic.
6. Entregueu: codi font, factors de n, clau privada k i missatge desencriptat P, incloent la vostra signatura encriptada PGP.

Missatge xifrat: El trobareu al fitxer adjunt, missatge-encriptat. A la primera línia hi ha n i a la segona, e. A continuació el missatge xifrat.