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 es un número de L dígits.

4. Trocegem P en tants blocs P_i (de L-1 digits cada un) com facin falta (aixi $P_i < n$ 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. Decodifica 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 dexifrada, 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 al final d'aquest fitxer, per un destinatari que usa la següent clau pública:

$$(n = RSA_9 = 297045209, e = 31273).$$

Sabem que RSA-9 es MOLT poc segur i volem advertir-lo. Per això, li dexifrareu el missatge i li enviareu el missatge dexifrat.

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. Entregueu: codi font, factors de n, clau privada k, missatge encriptat C i missatge desencriptat P

Missatge xifrat:

C =

19094749006694409915726786426036136111702277811812035711174400128787637613744206
42508667542398307811237490211426838040469252850264245482776756430565725540434116 5
61553020040401526700269229222227519041935405280404245031736640950789455110347703 1
20427075422268360000608076520486620651273777201600938362322499772697167252468159 7
61187188960596666720664810740082821531580089692733828892354253301770912601331833 3
61418461172613211940690941202343214230004559220786025242324712571178877081003561 8
30609374730232219652402688461953656072250877 73

(ULL: al carregar aquest missatge treieu els retorns de línia per tenir una única string numèrica)