Pràctica 2

Per a aquesta pràctica, s'han implementat diversos algorismes bàsics de criptografia modular utilitzant Python. Els algorismes es troben organitzats en fitxers separats dins la carpeta Exercici1, i posteriorment s'han reutilitzat a Exercici2 per dur a terme la simulació del sistema RSA.

Els algorismes implementats són:

Algorisme d'Euclides per calcular el màxim comú divisor (MCD) entre dos enters.

```python
def maxim_comu_divisor(a, b):
    while b != 0:
        a, b = b, a % b
    return a
```

Algorisme d'Euclides estès per calcular l'invers modular, necessari en la generació de la clau privada RSA.

```python
def euclides_extes(a, b):
    if b == 0:
        return a, 1, 0
    else:
        d, x1, y1 = euclides_extes(b, a % b)
        x = y1
        y = x1 - (a // b) * y1
        return d, x, y

def invers_modular(d, n):
    d = d % n  # Ens assegurem que d està dins del mòdul
    gcd, x, _ = euclides_extes(d, n)
    if gcd != 1:
        return None  # No hi ha invers si no són coprimers
    return x % n  # L'invers ha de ser dins de Z_n
```

Exponenciació binària modular, que permet calcular potències modulars de manera eficient, utilitzada tant en el xifrat com en el desxifrat del missatge.

```python
def exponenciacio_binaria(m, e, n):
    resultat = 1
    m = m % n  # Ens assegurem que m < n per evitar nombres grans innecessaris

    while e > 0:
        if e % 2 == 1:          # Si el bit actual d'e és 1
            resultat = (resultat * m) % n
        m = (m * m) % n         # Quadrat del base
        e = e // 2              # Anem al següent bit (divisió per 2)

    return resultat
```

Per fer la simulació RSA a Exercici2, l'usuari introdueix dos nombres primers (p i q), a partir dels quals es calcula el mòdul n, la funció d'Euler φ(n), i es defineix l'exponent públic e. A continuació, es calcula l'invers modular d, i es generen les claus pública i privada. Finalment, es xifra i desxifra un missatge utilitzant l'exponenciació modular, i es comprova que el missatge original es recupera correctament.

Per reutilitzar els algorismes entre carpetes, s'ha afegit dinàmicament la ruta de Exercici1 al sys.path de Python dins de l'script de simulació, permetent així importar directament les funcions necessàries.

Per l'exercici tres, s'han utilitzat les comandes proporcionades per tal de generar una clau privada, i una clau pública a partir d'aquesta. En el apartat a es demana passar els nombres que representen p, q, n i e, d'hexadecimal a decimal, i aquest és el resultat que ens dona mitjançant un codi que s'ha fet per passar a decimal.

p =
167011447547345728933230408596655483823025527351171638664960988258488645906865711271035021070017334308766014757246721438345786718086434438185635530609804198795261900187227964510725788331289532942572922835270915814298107171348171945360689113954576959819567853467091230588797236014492498843570449717676154921303

q =
161691457884174529782134958452207504595433588067950397613417403186008591704536084845925940762797690761912811309311306778428076281066862875903668998348845577653827027731758785407337572061406382630380800384953822931331302 0

606890822351712270405555315766290554840441200688859941617924347618478149756371697390875 31

n =

150781595870902335896290309074365040257410679994091712317378039820451273052210550152719286353027768602687054078895288367847656772775704177195366446954997901617615069347489786993140298099285153035014154073675219928413301378442914091314670195211122149406972029652812884476975345193473159746848531914271764107823

e =

157421993084665685934989017816650073358310251103823440299209608140132713005641430765169559051821883967677980310575079270219458149183993789530790992384302677516189459727570994700483312455209722874017726402276966500029773599689671082788519604581076904891801342448938670955221637511013009804579412558703126388277

Per la segona part de l'exercic, s'ha intercanviat les claus públiques amb el company Sergio i s'ha pogut tant desxifrar el missatge que ha passat ell xifrat amb la meva clau pública, com també s'ha pogut xifrar un missatge amb la seva clau pública. Aquest és el missatge xifrat:

I aquest el contingut després de desxifrar-lo amb la meva clau pública: