IA012 - tarefa 03

Rodrigo Seiji P. Hirao - 186837

September 2021

1 RSA

```
sage: b = 37+50
sage: max_prime = int(2^(b/2))
sage: p = 1
sage: q = 1
sage: while not is_prime(p):
....:     p = ZZ.random_element(max_prime)
....:
sage: while not is_prime(q):
....:     q = ZZ.random_element(max_prime)
....:
sage: n = p*q
sage: phi_n = (p-1)*(q-1)
sage: e = 2^16+1
sage: gcd(e, phi_n)
1
sage: d = 0.1
sage: k = 0
sage: d = xgcd(e, phi_n)[1]
sage:
sage: n
592914261458741734168608889
sage: e
65537
sage: d
288699314851224364495472 45
sage:
sage: P = 186837
sage: C = mod(P^e, n)
sage: C
562236998635894435646462 27
sage: P = mod(C^d, n)
sage: P
186837
```

2 DH

```
sage: p = 22387059351816344385938388094627461609 7
sage: r = 5
sage: Kpra = 186837
sage: Kprb = 738618
sage: Kpua = mod(r^Kpra, p)
sage: Kpub = mod(r^Kprb, p)
sage: Ka = mod(Kpub^Kpra, p)
sage: Kb = mod(Kpua^Kprb, p)
sage: Ka == Kb
True
sage: Ka
157992952822946587633403121304175477069
sage: Kb
157992952822946587633403121304175477069
```