Kryptografi: RSA

Här kommer fyra stycken RSA-uppgifter. I varje uppgift är målet att dekryptera det hemliga meddelandet. Längst ner i dokumentet hittar du lite hjälpfunktioner.

```
Uppgift 0:
p = 367
q = 389
e = 5
c = 34770
```

```
Uppgift 1:
n = 187
e = 3
c = 132
```

```
Uppgift 2:
n = 2745221164897
e = 7
ciphertext = '0115a852f517'
```

OBS: inte samma lösning som tidigare!

```
Uppgift 3:
n1 =
323170060713110073007148766886699519604441026697154840321303454275246551
388678908931972014115229134636887179609218980194941195591504909210950881
523864482843329669006988419225067849033411549401645316243081867032848474
980973054785214742444218621168776362440167645004236798256686885604663405
327877462880867863779999947876487484631391448722998694385330303115987002
401930407462713304133200910117307257272770076203432998602610177086925869
677604204653238737530812611963153574847611639174685608330064850534713384
599908183959160387292420680711007288837652945275592522016285511736845323
378726724507742740918830067460762376577 61
n2 =
323170060713110073007148766886699519604441026697154840321303454275246551
388678908931972014115229134636887179609218980194941195591504909210950881
523864482844864621677033266105766848534746090750395549327319959124633267
686609317757673608507421236012980094768429116017287951031868185106118831
610360506589234644649484763823382291944175141152766147084230576369898352
898758460025057247703238014036677335809347518543846077864872674099672252
649513471522122707153714737774322402680947568529601947669098530386201483
585468084172535591915193453768009394877582831502777070559823383733152438
447671347575734473217340570668 50250481981
e = 65537
ciphertext1 =
'260a9da13252490ba5b71926125d38993c7e58d95014dfbff8c1c24298b3aed44caa2c6
f92be2cfbf707512777c56f562f14e52dff1b546559c0a9577cf918f6f08780f76163b73
```

```
295061c95f8e673990d206bb5fa664ccb2e48a505dba15c2a4a5e33442fc3586f12c2a87
9ae961c78021172f1aeb5ddd6d01f37b0d9b3e9631fe95d284b30d65157aa463b6f738fc
508227124734ff08372c329c711dae0924e3e75d4b68e957f471b09c4ee7afa220a28b1c
98f9e0082352066dee8f5e4056e406046e720e95c7ece061c5c8086de72b444fe53883eb
3dbc6706a3fcf28e9a2228a3dcc8824d11d0720c256355b8ec14bb28319d4456b3b07d82
48d11a617'
ciphertext2 =
'10d0ecbf0765b2f9aa9c0d88ce6692eb8352dc966995346d34fd1121051753d1a148375
1fa48971c6d363c4d65dc724c1ce33afedd17bed28a8b1a50e6bb7531cc011ef3a8031dd
247545b83d2416d376be82adebc344a9af4002744c3ddab101ef46ed22fc869d1dfa4b5c
a67f82237105089272e0b236cfc07740d754ced0af191624b56a71f5490c17db8d1638e2
63d2d56eb0cd352edbaf2990f6440e118e40efbfcaea43cf4e9d116d8753ce10a16f0a58
0def1055fb02ff0e78c04ed5e1f0092d39f42780d4c0a14897efebb95cce4f1a4f4b3c0c
a4472bb11414ee96309429f5f04983f81de8cdd9c5d31fce790e43d9e01577d74b2ca979
2b3d57575'
```

Hjälpkod:

```
#!/usr/bin/env python3
import math

def encrypt(m, e, n):
      assert 0 < m and m < n, "Message m must be smaller than n."
      return pow(m, e, n)

def encrypt_string(text, e, n):
      m = int.from_bytes(text.encode(), "big")
      c = encrypt(m, e, n)
      ciphertext = c.to_bytes(math.ceil(math.log(c, 256)), "big").hex()
      return ciphertext

def decrypt(c, d, n):
      assert 0 < c and c < n, "Message c must be smaller than n."
      return pow(c, d, n)

def decrypt_string(ciphertext, d, n):
      c = int.from_bytes(bytes.fromhex(ciphertext), "big")
      m = decrypt(c, d, n)
      text = m.to_bytes(math.ceil(math.log(m, 256)), "big").decode()
      return text

def generate_d(p, q, e):
      return pow(e, -1, (p-1)*(q-1))
```

Skapad av Mattias Grenfeldt