Oppgave 1 – Tallteori

1a)

$$\frac{72}{2} = 36\mathbb{R}0$$
$$\frac{36}{2} = 18\mathbb{R}0$$
$$\frac{18}{2} = 9\mathbb{R}0$$
$$\frac{9}{2} = 4\mathbb{R}1$$
$$\frac{4}{2} = 2\mathbb{R}0$$
$$\frac{2}{2} = 1\mathbb{R}0$$
$$\frac{1}{2} = 0\mathbb{R}1$$
$$\Downarrow$$
$$72_{10} = 1001000_2$$

$$\frac{136}{2} = 136\mathbb{R}0$$
$$\frac{68}{2} = 68\mathbb{R}0$$
$$\frac{34}{2} = 34\mathbb{R}0$$
$$\frac{17}{2} = 8\mathbb{R}1$$
$$\frac{8}{2} = 4\mathbb{R}0$$
$$\frac{4}{2} = 2\mathbb{R}0$$
$$\frac{2}{2} = 1\mathbb{R}0$$
$$\frac{1}{2} = 0\mathbb{R}1$$
$$\Downarrow$$
$$136_{10} = 10001000_2$$

1b)

Skal regne ut $a = 11^{72}$ og $b = 11^{136}$ modulo 10001

$$\begin{aligned} a &= 11^{72} = 11^{1001000_2} \\ &= 11^{64+8} \\ b &= 11^{136} = 11^{10001000_2} \\ &= 11^{128+8} \end{aligned}$$

Finner toerpotenser av 11:

$$\begin{aligned} 11^2 &= 121 \pmod{10001} \\ 11^4 &= 11^{2\cdot 2} \equiv 14641 \equiv 4640 \pmod{10001} \\ 11^8 &= (11^4)^2 = 21529600 \equiv 7448 \pmod{10001} \\ 11^{16} &= (11^8)^2 = 55472704 \equiv 7158 \pmod{10001} \\ 11^{32} &= (11^{16})^2 = 51236964 \equiv 1841 \pmod{10001} \\ 11^{64} &= (11^{32})^2 = 3389281 \equiv 8943 \pmod{10001} \\ 11^{128} &= (11^{64})^2 = 79977249 \equiv 9253 \pmod{10001} \end{aligned}$$

Regner ut:

$$\begin{aligned} a &= 11^{64+8} = 8943 \cdot 7448 = 66607464 \equiv 804 \pmod{10001} \\ b &= 11^{128+8} = 9253 \cdot 7448 = 68916344 \equiv 9454 \pmod{10001} \end{aligned}$$

Tallene er såpass små (relativt sett) at Gnome Calculator fint klarer å verifisere svarene mine

1c)

Bruker Euklids algoritme:

$$\begin{aligned} \gcd(a, 10001) &= \gcd(10001, 804) \quad \text{(fra 1b)} \\ \gcd(10001, 804) &= \gcd(804, 10001 \bmod 804) = \gcd(804, 353) \\ \gcd(804, 353) &= \gcd(353, 804 \bmod 353) = \gcd(353, 98) \\ \gcd(353, 98) &= \gcd(98, 59) = \gcd(59, 39) = \gcd(39, 20) \\ \gcd(39, 20) &= \gcd(20, 19) = \gcd(19, 1) = \gcd(1, 0) = 1 \end{aligned}$$

$$
\begin{aligned}
\gcd(b, 10001) &= \gcd(10001, 9454) \quad \text{(fra 1b)} \\
\gcd(10001, 9454) &= \gcd(9454, 10001 \bmod 9454) = \gcd(9454, 547) \\
\gcd(9454, 547) &= \gcd(547, 155) = \gcd(155, 82) = \gcd(82, 73) \\
\gcd(82, 73) &= \gcd(73, 9) = \gcd(9, 1) = \gcd(1, 0) = 1
\end{aligned}
$$

Tester med haskell:

```haskell
gcd 10001 804
1
gcd 10001 9454
1
```

1d)

Skal regne ut $ab \pmod{10001}$ – bruker resultatene fra 1b:

$$ab \equiv 804 \cdot 9454 = 7601016 \equiv 256 \pmod{10001}$$

Gnome: 256

Oppgave 2 – RSA-system

2a) – Systemet

Velger to primtall innenfor 8 bits:

$$p = 251 = 1111\ 1011_2, \quad q = 241 = 1111\ 0001_2$$

(brukte Wikipedias liste over de første 1000 primtallene)

Disse gir $n = pq = 251 \cdot 241 = 60\,491$ Finner så $\phi(n) = (p-1)(q-1) = 250 \cdot 240 = 60\,000$

Faktoriseringen av $60\,000$ er lett å finne:

$$60\,000 = 6 \cdot 10^4 = 2 \cdot 3 \cdot (2 \cdot 5)^4 = 2^5 \cdot 3 \cdot 5^4$$

Velger $e = 7$ (det minste tallet som er innbyrdes primisk med $\phi(n)$)

Har da offentlig nøkkel $(n, e) = (60\,491, 7)$

2b) – Den private nøkkelen

Finner d som multiplikativ invers av e modulo $\phi(n)$, med funksjonen `extended_euclid` i `rsa.py` (lett omskriving av algoritme 5.3):

$$7 \cdot 17\,143 \equiv 1 \pmod{60\,000}$$

Har da den private nøkkelen $(p, q, d) = (251, 241, 17\,143)$

2c) – Bruk

Skal kryptere 42. La oss starte som en som vil kommunisere med nøkkelens innehaver:

$$e_K(42) = x^e \bmod n = 42^7 \bmod 60\,491, \quad 7 = 0111_2 \Rightarrow l = 3$$

Følger algoritme 5.5 slavisk (lar n stå som variabel):

$$\begin{aligned}
z &= 1 \\
\text{Starter med } i &= 2; \\
z &= 1^2 \bmod n = 1 \\
\text{Vet at } c_2 &= 1, \text{ så} \\
z &= z \cdot x \bmod n = 1 \cdot 42 \bmod n = 42 \\
\text{Setter så } i &= 1; \\
z &= 42^2 \bmod n = 1764 \\
\text{Vet at } c_1 &= 1, \text{ så} \\
z &= 1764 \cdot 42 \bmod n = 13597 \\
\text{Til sist lar vi } i &= 0; \\
z &= 13597^2 \bmod n = 184878409 \bmod n = 17913 \\
\text{Vet at } c_0 &= 1, \text{ så} \\
z &= 17913 \cdot 42 \bmod n = 26454
\end{aligned}$$

Igjen er Gnome Calculator enig med meg.

Vi har kryptert 42 til $26\,454$. Tid for å gå tilbake:

$$d_K(26\,454) = x^d \bmod n = 26\,454^{17\,143} \bmod 60\,491,$$
$$17\,143 = 0100\;0010\;1111\;0111_2 \Rightarrow l = 15$$

For variasjonens skyld (og siden d er betydelig større enn e) gjør jeg dekrypteringen programmatisk, etter mønster av algoritme 5.5 i læreboka:

```python
def square_and_multiply(x, e, n):
    z = 1
    for i in reversed(range(0, e.bit_length())):
        z = z*z % n
        if (e >> i) & 1 == 1:
            z = z*x % n
    return z
```

Kjører `square_and_multiply(26454,17143,60491)` og får tilbake `42`.

Oppgave 3 – Pollard p-1

3a) – Gitt B og n

Algoritmen:

```python
def pollard_p_minus_one(n, B):
    a = 2
    for i in range(2, B+1):
        a = square_and_multiply(a, i, n)
    d = gcd(n, a-1)
    if 1 < d < n:
        return d
    raise ArithmeticError(f'Pollard p-1 failure: d={d}')
```

der `gcd` er en implementasjon av Euklids algoritme. Se `rsa.py`.

Med $n = 1829$ og $B = 5$ får jeg 31. Har da $p = 31$ og $q = \frac{1829}{31} = 59$.

3b) – Finn B-er uten å teste

Skal finne B-er som fungerer for $n_1 = 18779$ og $n_2 = 42583$.
Faktoriserer med `factor`-kommandoen:

$$n_1 = 18779 = 89 \cdot 211, \quad n_2 = 42583 = 97 \cdot 439$$

Faktoriserer så $p-1$ og $q-1$ for hver n:

$$n_1: \ p-1 = 88 = 2^3 \cdot 11 = 8 \cdot 11, \quad q-1 = 210 = 2 \cdot 3 \cdot 5 \cdot 7$$
$$n_2: \ p-1 = 96 = 2^5 \cdot 3 = 3 \cdot 32, \quad q-1 = 438 = 2 \cdot 3 \cdot 73$$

Velger $B_1 = 7$ og $B_2 = 32$ siden de er de minste av de største primtallspotensene til faktorene av henholdsvis n_1 og n_2.

Gjorde en test med koden jeg skrev til forrige oppgave, disse B-ene stemmer.

3c) – Prøv forskjellige B-er

Ser at for $n = 6319 = 71 \cdot 89$ så er $p-1 = 70$ og $q-1 = 88$ partall som *ikke* kan være delelige på 3. Vet da at vi kan starte f.o.m. 5.

Skrev litt kode for å kjøre koden jeg skrev for forskjellige B-er i et intervall. Kjørte `try_some_bees(6319,5,11)` og fikk til svar at $B = 7$ fungerer.

Oppgave 4 – Pollard rho

Skrev litt enkel Python-kode for å utføre Pollard ρ-metoden.

Følgen vår er gitt av $f(x) = x^2 + 1$ og startverdien $x_1 = 1$.

Antall iterasjoner er $i - 1$ i uthoppet, siden startverdien gjelder for $i = 1$.

4a)

For $n = 851$ finner vi 37 etter 9 iterasjoner.

Tabell med mer manuell løsning:

i	x_i	d
1	1	-
2	2	$\gcd(2-1, 851) = 1$
3	5	-
4	26	$\gcd(26-2, 851) = 1$
5	677	-

i	x_i	d
6	492	$\gcd(492-5, 851) = 1$
7	381	-
8	492	$\gcd(492-26, 851) = 1$
9	381	-
10	492	$\gcd(492-677 \bmod 851, 851) = 37$

4b)

For $n = 1517$ finner vi *også* 37 etter 9 iterasjoner.

4c)

For $n = 31861$ finner vi 151, igjen etter 9 iterasjoner.

Oppgave 5 – Bevis

5a)

Skal bevise at for RSA gjelder

$$e_K(x_1)e_K(x_2) \equiv e_K(x_1x_2) \pmod n,$$

altså at krypteringen er multiplikativ.

Vet at krypteringsfunksjonen i RSA er $e_K(x) = x^e \bmod n$.

$$\begin{aligned} e_K(x_1)e_K(x_2) \bmod n &= (x_1^e \bmod n) \cdot (x_2^e \bmod n) \bmod n \\ &= (x_1x_2 \bmod n)^e \bmod n \\ &= (x_1x_2)^e \bmod n \\ &= e_K(x_1x_2) \bmod n,\ Q.E.D. \end{aligned}$$

5b)

Har en chiffertekst y, skal kunne finne en $y' \neq y$ slik at vi med $x' = d_K(y')$ kan finne $x = d_K(y)$. Vi vet også den ofentlige nøkkelen (n, e).

Vet at $y = e_K(x) = x^e \bmod n$. Om vi lar

$$y' = 2^e y = e_K(2x) = 2^e x^e \bmod n,$$

får vi

$$x' = d_K(y') = d_K((2x)^e \bmod n) = (2x)^{e \cdot d} \bmod n = 2x \bmod n,$$

og kan finne klarteksten $x = x'/2 \bmod n$.

Vi kan altså finne x ved å dele x' på 2 hvis x' er et partall, eller gange x' med den multiplikative inverse av 2 modulo n.

Oppgave 6 – RSA-angrep

6a)

p og q er to store primtall. Da er de også *oddetall*.

La $q = 2a + 1$ og $p = 2b + 1$, der $a, b \in \mathbb{N}$.

$$\begin{aligned} q - p = (2a+1) - (2b+1) &= 2(a-b) + (1-1) \\ &= 2(a-b) = 2d, \quad Q.E.D. \end{aligned}$$

6b)

Et kvadrattall kan skrives som x^2 der $x \in \mathbb{N}$.

$$\begin{aligned} n + d^2 &= qp + \left(\frac{1}{2}(q-p)\right)^2 = qp + \left(\frac{1}{2}\right)^2 (q-p)^2 = qp + \frac{1}{4}(q^2 - 2qp + p^2) \\ &= qp - \frac{1}{2}qp + \frac{1}{4}q^2 + \frac{1}{4}p^2 = \frac{1}{4}q^2 + \frac{1}{2} \cdot \frac{2}{2}qp + \frac{1}{4}p^2 \\ &= \frac{1}{4}\left(q^2 + 2qp + p^2\right) = \frac{1}{2^2}(q+p)^2 = \left(\frac{1}{2}(q+p)\right)^2 = x^2, \quad Q.E.D. \end{aligned}$$

6c)

Vet at $n = pq$ og

$$n + d^2 = k^2,$$

der k er et heltall.

Om vi snur litt om på uttrykket og bruker tredje kvadratsetning, får vi

$$n = k^2 - d^2 = (k + d)(k - d) = pq,$$

og dermed vil $p = k + d$ og $q = k - d$ være faktorene til n.

6d)

Skal faktorisere $n = 2189284635403183$.

Finner en d ved å prøve meg fram ($\sqrt{n + d^2}$ må være et heltall):

$$\begin{aligned} d = 0 &: \sqrt{n + d^2} \approx 46789791,99\ldots \\ d = 1 &: \sqrt{n + d^2} \approx 46789791,99\ldots \\ d = 2 &: \sqrt{n + d^2} \approx 46789791,99\ldots \\ &\vdots \\ d = 9 &: \sqrt{n + d^2} = 46789792 = k \end{aligned}$$

Da får vi faktorene

$$p = k + d = 46789792 + 9 = 46789801$$

og

$$q = k - d = 46789792 - 9 = 46789783$$

PS: Det er også mulig å jukse seg fram til hvilken d som passer.

Ved å faktorisere $n = 46789783 \cdot 46789801$ og ta differansen $|p - q| = 18 = d^2$, ser vi at $d = 9$ fungerer…