TMA4155 — Solutions to exercise 5

Kristian Gjøsteen

2005-09-28

Task 1 — RSA encryption

We have two public keys $pk_1 = (n, e_1)$ and $pk_2 = (n, e_2)$, and encrypting a message with both keys yields:

$$\mathcal{E}(pk_2, \mathcal{E}(pk_1, m)) = (m^{e_1} \bmod n)^{e_2} \bmod n.$$

Since $(m^{e_1})^{e_2} \equiv m^{e_1 e_2} \pmod{n}$, this double encryption is the same as encrypting once with the public key $(n, e_1 e_2)$.

Task 2 — Euclid's algorithm

a. $\gcd(157, 153) = 1$ because:

$$\begin{aligned} 157 &= 1 \cdot 153 + 4 \\ 153 &= 38 \cdot 4 + 1 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

b. $\gcd(153, 187) = 17$ because:

$$\begin{aligned} 187 &= 1 \cdot 153 + 34 \\ 153 &= 4 \cdot 34 + 17 \\ 34 &= 2 \cdot 17 + 0 \end{aligned}$$

c. $\gcd(10005, 1101) = 3$ because:

$$\begin{aligned} 10005 &= 9 \cdot 1101 + 96 \\ 1101 &= 11 \cdot 96 + 45 \\ 96 &= 2 \cdot 45 + 6 \\ 45 &= 7 \cdot 6 + 3 \\ 6 &= 2 \cdot 3 + 0 \end{aligned}$$

d. $\gcd(10005, 1103) = 1$ because:

$$\begin{aligned} 10005 &= 9 \cdot 1103 + 78 \\ 1103 &= 14 \cdot 78 + 11 \\ 78 &= 7 \cdot 11 + 1 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

Task 3 — Modular inverses

a. An inverse to 153 modulo 157 is 39 because:

$$\begin{aligned} 157 &= 1 \cdot 153 + 4 & &= 153 - 38(157 - 153) = 39 \cdot 153 - 38 \cdot 157 \\ 153 &= 38 \cdot 4 + 1 & 1 &= 153 - 38 \cdot 4 \\ 4 &= 4 \cdot 1 + 0 \end{aligned}$$

b. From **a.** we find that -38 is an inverse to 157 modulo 153.

c. An inverse to 1103 modulo 10005 is -898 because:

$$\begin{aligned} & & &= 99 \cdot 10005 - 898 \cdot 1103 \\ 10005 &= 9 \cdot 1103 + 78 & &= 99(10005 - 9 \cdot 1103) - 7 \cdot 1103 \\ 1103 &= 14 \cdot 78 + 11 & &= 78 - 7(1103 - 14 \cdot 78) = 99 \cdot 78 - 7 \cdot 1103 \\ 78 &= 7 \cdot 11 + 1 & 1 &= 78 - 7 \cdot 11 \\ 11 &= 11 \cdot 1 + 0 \end{aligned}$$

d. An inverse to 73 modulo 1103 is 136 because:

$$\begin{aligned} 1103 &= 15 \cdot 73 + 8 & &= 73 - 9(1103 - 15 \cdot 73) = 136 \cdot 73 - 9 \cdot 1103 \\ 73 &= 9 \cdot 8 + 1 & 1 &= 73 - 9 \cdot 8 \\ 8 &= 8 \cdot 1 + 0 \end{aligned}$$

Task 4 — Primality testing

First we note that $560 = 2^9 + 2^5 + 2^4$. For 2, we compute

$$
\begin{aligned}
2^2 \bmod 561 &= 4 \\
2^{2^2} \bmod 561 &= 4^2 \bmod 561 = 16 \\
2^{2^3} \bmod 561 &= 16^2 \bmod 561 = 256 \\
2^{2^4} \bmod 561 &= 256^2 \bmod 561 = 460 \\
2^{2^5} \bmod 561 &= 460^2 \bmod 561 = 103 \\
2^{2^6} \bmod 561 &= 103^2 \bmod 561 = 511 \\
2^{2^7} \bmod 561 &= 511^2 \bmod 561 = 256 \\
2^{2^8} \bmod 561 &= 256^2 \bmod 561 = 460 \\
2^{2^9} \bmod 561 &= 460^2 \bmod 561 = 103
\end{aligned}
$$

and

$$2^{560} \equiv 2^{2^9} 2^{2^5} 2^{2^4} \equiv 103 \cdot 103 \cdot 460 \equiv 1 \pmod{561}.$$

For 5, we compute

$$
\begin{aligned}
5^2 \bmod 561 &== 25 \\
5^{2^2} \bmod 561 &= 25^2 \bmod 561 = 64 \\
5^{2^3} \bmod 561 &= 64^2 \bmod 561 = 169 \\
5^{2^4} \bmod 561 &= 169^2 \bmod 561 = 511 \\
5^{2^5} \bmod 561 &= 511^2 \bmod 561 = 256 \\
5^{2^6} \bmod 561 &= 256^2 \bmod 561 = 460 \\
5^{2^7} \bmod 561 &= 460^2 \bmod 561 = 103 \\
5^{2^8} \bmod 561 &= 103^2 \bmod 561 = 511 \\
5^{2^9} \bmod 561 &= 511^2 \bmod 561 = 256
\end{aligned}
$$

and

$$5^{560} \equiv 5^{2^9} 5^{2^5} 5^{2^4} \equiv 256 \cdot 256 \cdot 511 \equiv 1 \pmod{561}.$$

For 7, we compute

$$\begin{aligned}
7^2 \bmod 561 &= 49\\
7^{2^2} \bmod 561 &= 49^2 \bmod 561 = 157\\
7^{2^3} \bmod 561 &= 157^2 \bmod 561 = 526\\
7^{2^4} \bmod 561 &= 526^2 \bmod 561 = 103\\
7^{2^5} \bmod 561 &= 103^2 \bmod 561 = 511\\
7^{2^6} \bmod 561 &= 511^2 \bmod 561 = 256\\
7^{2^7} \bmod 561 &= 256^2 \bmod 561 = 460\\
7^{2^8} \bmod 561 &= 460^2 \bmod 561 = 103\\
7^{2^9} \bmod 561 &= 103^2 \bmod 561 = 511
\end{aligned}$$

and

$$7^{560} \equiv 7^{2^9} 7^{2^5} 7^{2^4} \equiv 511 \cdot 511 \cdot 103 \equiv 1 \pmod{561}.$$

After these three tests, the Fermat test would conclude that 561 may be prime.