SOLUTIONS TO SELECTED EXERCISES TMA4155, 2011

These solutions are meant as a reference for students to check their answers. The solutions lack the reasoning behind the answers. An exam submission should of course also contain the reasoning behind the answers.

Exercise 1

Task 1:

a) ”CKJOJOZ”, b) ”anytime”
c) ”SVRUQVJ”, d) ”affinity”

Task 2:

a) ”meet me at five”
b) decrypts with $x = 9y + 3 \mod 26$

Task 3:

$$\text{a) } gcd(72, 84) = 12,$$
$$\text{b) } gcd(364, 742) = 14, \quad 742 - 2 \cdot 364 = 14$$
$$\text{c) } 123456789 \mod 11 = 9 - 8 + 7 - 6 + 5 - 4 + 3 - 2 + 1 \mod 11.$$

Exercise 2

Task 1:

$$\begin{pmatrix} 1 & 2 & 2 \\ 3 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}^{-1} \mod 10 = \begin{pmatrix} 3 & 0 & 4 \\ 7 & 1 & 5 \\ 7 & 9 & 8 \end{pmatrix}$$

$$A = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \\ 2 & 1 & 1 \end{pmatrix}$$

no inverse $\mod 10$, since $\gcd(\det A, 10) \neq 1$.

Task 2:

$$\begin{gathered}
1.\ x \equiv 3 \mod 9 \\
2.\ x \equiv 4 \mod 8 \\
3.\ x \equiv 5 \mod 9 \\
4.\ \text{no solution} \\
5.\ x \equiv 23 \mod 40
\end{gathered}$$

Task 4:

$$x \equiv 53 \mod 210$$

Task 5:

$$z \equiv 2930 \mod 10403$$

Exercise 3

Task 1:

Encrypting the word banana with initialization vector $(11, 2)$ we get $LBBAIPZW$.
Decryption gives the word "fish".

Task 3:

$$\begin{gathered}
A \equiv 35 \mod 101 \\
B \equiv 47 \mod 101 \\
\text{shared secret } K \equiv 36 \mod 101
\end{gathered}$$

Task 4:

$$\begin{gathered}
\text{a) } d \equiv 1031 \mod 1260 \\
\text{b) } c \equiv 1191 \mod 1333 \\
\text{c) } m \equiv 684 \mod 1333
\end{gathered}$$

Task 5:

Encrypting twice with e_1 and e_2 is the same as encrypting once with e_1e_2, so it provides no extra security.

Task 6:

Eve will recieve from Nelson $(2^e c)^d \equiv 2^{ed} c^d \equiv 2m \mod n$.

Exercise 4

Task 1:

$$(\pm 18)^2 \equiv 2 \mod 23$$
$$5 \text{ has no square roots} \mod 23.$$
$$21 \text{ has no square roots} \mod 23.$$

Task 2:

$$\text{a) } x \equiv \pm 78 \pm 22 \mod 143.$$
$$\text{b) } x \equiv \pm 104 \mod 143.$$
$$\text{c) no solution.}$$

Task 3:

$$(2389)(2381) = 5688209$$
$$(73)(137) = 10001.$$

Task 4:

$$2733 \cdot 16007 \not\equiv 2^3 \cdot 3 \cdot 7 \cdot 11$$
$$(2733 \cdot 16007) \equiv (2^3 \cdot 3 \cdot 7 \cdot 11)^2$$
$$\Rightarrow \gcd(2733 \cdot 16007 - 2^3 \cdot 3 \cdot 7 \cdot 11, n)$$

Task 5:

$$a = 2, B = 5, \gcd(12 - 1, 253) = 11 \to 243 = 11 \cdot 13.$$

Exercise 5

Solutions to all the exam problems can be found on the webpage. Solutions to the exams in 2006 are posted in one file.