Homework sheet 1, due 19 November 2026 at 13:30

Make sure to justify your answers in detail and to give clear arguments. Document all steps, in particular of algorithms; it is not sufficient to state the correct result without the explanation. If the problem statement asks for usage of a particular algorithm other solutions will not be accepted even if they give the correct result.
Form groups of 3 or 4 students, and submit *one* version of the homework solutions together. Submit your homework by encrypted and signed email to all 4 TAs/instructors. You can find their keys on the course page.

Put your teammates in cc and do not forget to attach your public key and those of your teammates, else the TAs cannot reply to you.

1. This question is about the one-time pad used twice.

   You observe that Bob sends two messages

   `hyeuxafohfhpfefxloblgirb`

   and

   `hyeuqsosoyozeijdqiuadfv` .

   Based on the start you suspect that he is using the one-time pad incorrectly. The first one goes to his friends Wilhelmina and Theodor.

   What does he say in the second message? | 8 points |

2. The affine encryption system is a symmetric system. The key consists of two integers $0 \leq a, b < 26$ with $\gcd(a, 26) = 1$. Messages and ciphertexts are also integers in $[0, 25]$. Message m is encrypted as $c = a \cdot m + b \bmod 26$.

   (a) Explain how decryption works. | 4 points |

   (b) Your key is $(a, b) = (5, 7)$ and you receive the ciphertext 17. Compute the plaintext. | 3 points |

   (c) Compute the size of the keyspace, i.e. how many different keys exist. Note the different restrictions on a and b. | 5 points |