Introduction to Cryptography
Exercise Week 1

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

Exercise 1.
The following ciphertext is the result of encrypting a message with the shift cipher:

```
GURXRLHFRQSBEGURFUVSGPVCURERAPELCGVBAPNARNFV
YLORTHRFFRQOLYBBXVATSBEGURZBFGSERDHRAGYRGGRE
```

Determine the key and decrypt the message.

Exercise 2.
Show that the shift, mono-alphabetic substitution, and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. For the Vigenère cipher, you may assume that the key length t is known.

(Hint: For each cipher, it suffices to obtain a single plaintext-ciphertext pair.)

How long does the plaintext need to be to recover the key in each case?

Exercise 3.
Assume an attacker knows that a user's password is either `abcd` or `bedg`.

(a) Say the user encrypts his password using the shift cipher, and the attacker sees the resulting ciphertext. Show how the attacker can determine the user's password.

(b) Does your method also work if the Vigenère cipher is used, with key length 2, 3, or 4?

Exercise* 4.
We define the following generalization of the shift cipher:

- The key generation algorithm `Gen` selects a random key pair $k = (a, b)$

from the key space

$$\mathcal{K} = \{(a, b) \mid a, b \in \mathbb{Z}_{26}, \gcd(a, 26) = 1\},$$

where $\gcd(\cdot, \cdot)$ denotes the greatest common divisor.

- The encryption function $\texttt{Enc}_{(a,b)}$ transforms a plaintext message $m = m_1 ... m_n \in \mathcal{M} = \mathbb{Z}_{26}^n$ into the ciphertext $c = c_1 ... c_n$ using the formula

  $$c_i = am_i + b \mod 26.$$

  That is, each letter m_i is multiplied by a and then shifted by b, modulo 26.

- The decryption function $\texttt{Dec}_{(a,b)}$ recovers the plaintext from a given ciphertext $c = c_1 ... c_n \in \mathcal{C} = \mathbb{Z}_{26}^n$ using

  $$m_i = a^{-1}(c_i - b) \mod 26,$$

  where a^{-1} is the modular inverse of a modulo 26.

This cryptosystem is called the *affine cipher*. Notably, choosing $a = 1$ reduces it to the standard shift cipher.

(a) Why must a satisfy the condition $\gcd(a, 26) = 1$ in the definition of the key space?

(b) Show that the affine cipher is correct, i.e., prove that applying decryption to an encrypted message recovers the original message,

$$\texttt{Dec}_{(a,b)}(\texttt{Enc}_{(a,b)}(m)) = m, \quad \forall m \in \mathcal{M}, (a, b) \in \mathcal{K}.$$

(c) Encrypt the message `cryptography` using the key $(a, b) = (3, 5)$.

(d) What is the size of the key space? Is a brute-force attack feasible?