Introduction to Cryptography
Exercise Week 2

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

Exercise 1.
Consider the following scenario:

Alice wants to encrypt a message of length n using the One-Time Pad, but knows that it will be sent in the clear if the key k happens to be 0^n. To prevent that, she chooses a new random key until $k \neq 0^n$, and only then encrypts her message.

Prove that the resulting scheme is no longer perfectly secret, using

(a) Definition 2.3.

(b) Lemma 2.5. (Reminder: A scheme is perfectly secret if and only if, for every $m, m' \in \mathcal{M}$ and every $c \in \mathcal{C}$, Equation (2.1)

$$\mathsf{Pr}[\mathsf{Enc}_K(m) = c] = \mathsf{Pr}[\mathsf{Enc}_K(m') = c]$$

holds.)

Exercise 2.
In each of the following schemes, $\mathsf{Enc}_k(m) = [m + k \mod 3]$. State in each case whether the scheme is perfectly secret, and justify your answers.

(a) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1\}$.

(b) The message space is $\mathcal{M} = \{0, 1, 2\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

(c) The message space is $\mathcal{M} = \{0, 1\}$, and Gen chooses a uniform key from the key space $\mathcal{K} = \{0, 1, 2\}$.

Exercise 3.

What is the ciphertext that results when the plaintext `0x012345` (written in hex) is encrypted using the one-time pad with key `0xFFEEDD`?

Exercise* 4.

Recall the affine cipher from question 4 of the first exercise sheet. Assume that every key $(a, b) \in \mathcal{K}$ is chosen with equal probability $1/|\mathcal{K}|$.

(a) Show that for messages of length $n \geq 2$, this cipher is not perfectly secret.

(b) Prove that for messages of length $n = 1$, this cipher *is* perfectly secret.

Exercise* 5.

In this problem we consider definitions of perfect secrecy for the encryption of *two* messages, using the same key. Here we consider distributions on pairs of messages from the message space $\mathcal{M}$; we let M_1, M_2 be random variables denoting the first and second message, respectively. (These random variables are not assumed to be independent.) We generate a (single) key k, sample a pair of messages (m_1, m_2) according to the given distribution, and then compute ciphertexts $c_1 \leftarrow \texttt{Enc}_k(m_1)$ and $c_2 \leftarrow \texttt{Enc}_k(m_2)$; this induces a distribution on pairs of ciphertexts and we let C_1, C_2 be the corresponding random variables.

(a) Say encryption scheme (`Gen, Enc, Dec`) is *perfectly secret for two messages* if for all distributions on $\mathcal{M} \times \mathcal{M}$, all $m_1, m_2 \in \mathcal{M}$, and all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$$

Prove that *no* encryption scheme can satisfy this definition.

(b) Say encryption scheme (`Gen, Enc, Dec`) is *perfectly secret for two distinct messages* if for all distributions on $\mathcal{M} \times \mathcal{M}$ where the first and second messages are guaranteed to be different (i.e., distributions on pairs of *distinct* messages), for all $m_1, m_2 \in \mathcal{M}$ and for all ciphertexts $c_1, c_2 \in \mathcal{C}$ with $\Pr[C_1 = c_1 \wedge C_2 = c_2] > 0$:

$$\Pr[M_1 = m_1 \wedge M_2 = m_2 \mid C_1 = c_1 \wedge C_2 = c_2] = \Pr[M_1 = m_1 \wedge M_2 = m_2]$$

Give an encryption scheme that fulfills this property. Can you also prove it?

Hint: Think of permutations. For the proof, you may use Bayes theorem and the law of total probability.