Introduction to Cryptography
Exercise Week 3

Dr. Patrick Struck
patrick.struck@uni.kn

Leon Weingarten
leon.weingarten@uni.kn

Jonah Herr
jonah.herr@uni.kn

Exercise 1.

(a) Prove that the Vigenère cipher using (fixed) period t is perfectly secret when used to encrypt messages of length t, and when the key is only used once.

(b) Prove (without using Theorem 2.11) that the Vigenère cipher is not perfectly indistinguishable for messages of length 4 when period $t = 3$ is used.

Exercise 2.

Prove that, by redefining the key space, we may assume that `Enc` is deterministic without changing $\Pr[C = c \mid M = m]$.

Hint: Move the randomness out of `Enc`.

Exercise 3.

Let $\mathcal{M} = \{a, b\}, \mathcal{K} = \{K_1, K_2, K_3, K_4, K_5\}$ and $\mathcal{C} = \{1, 2, 3, 4, 5\}$. Further, suppose the encryption function is represented by the following encryption matrix:

	a	b
K_1	1	2
K_2	2	3
K_3	3	1
K_4	4	5
K_5	5	4

For example, using key K_2, b is encrypted to 3. Now choose two positive real numbers α and β such that $\alpha + \beta = 1$, and define $\Pr[K_1] = \Pr[K_2] = \Pr[K_3] = \alpha/3$ and $\Pr[K_4] = \Pr[K_5] = \beta/2$.

Prove that this cryptosystem achieves perfect secrecy.

Exercise* 4.

Let $\epsilon > 0$ be a constant. Say an encryption scheme is ϵ-perfectly secret if for every adversary $\mathcal{A}$ it holds that

$$\Pr[\mathrm{PrivK}^{\mathrm{eav}}_{\mathcal{A},\Pi} = 1] \leq \frac{1}{2} + \epsilon.$$

Consider a variant of the one-time pad where $\mathcal{M} = \{0,1\}^\ell$ and the key is chosen uniformly from an arbitrary set $\mathcal{K} \subseteq \{0,1\}^\ell$ with $|\mathcal{K}| = (1-\epsilon) \cdot 2^\ell$; encryption and decryption are otherwise the same.

Prove that this scheme is $\left(\frac{\epsilon}{2(1-\epsilon)}\right)$-perfectly secret when $\epsilon \leq \frac{1}{2}$.

Hint: Consider a toy example to get an idea of how this could work. What message/ciphertext-pairs are possible?