Universität Leipzig
Institute of Computer Science
Winter term 2026/2027

Andreas Maletti

Exercises for the lecture

Cryptography

Exercise Sheet 2

for the exercise on October 30th, 2026

Exercise 2.1

Decrypt. (will not be done during exercise)

```
FusluytuffuslfihfxjfilvqljfxutKilfilyfxjtuszlyxtfilcxtafujqbbly
FiljzxtwjhtahyyukjubuqfyhwluqjbuyfqtlUyfufhnlHycjhwhxtjfhJlhubf
yuqszljHtasmueeujxtwltafilcfuaxlfujzlleTucuylhtasmhjzllefujhmkl
ltaFililhyfhrilhtafilfiuqjhtathfqyhzjiurnjFihfBzljixjilxyfuFxjh
rutjqcchfxutAlguqfzmfuslkxjilaFuaxlfujzlleFujzlleelyrihtrlfuAyl
hchmlfilylxjfilyqsBuyxtfihfjzlleubalhfikihfaylhcjchmruclKiltkli
hgljiqbbzlaubbfixjcuyfhzruxzCqjfwxglqjehqjlFilylxjfilyljelrfFih
fchnljRhzhcxfmubjuzutwzxblBuykiukuqzaslhyfilKixejhtaJruytjubfxc
lFilUeeyljjuyjkyutwfileyuqachtjRutfqclzmFilehtwjubaxjexjlaZuglf
ilZhkjalzhmFilxtjuzltrlubUbbxrlhtafiljeqytjFihfehfxltfclyxfubfi
qtkuyfimfhnljKiltilixcjlzbcxwifixjVqxlfqjchnlKxfihshylSuanxtKiu
kuqzaBhyalzjslhyFuwyqtfhtajklhfqtalyhklhymzxblSqffihffilaylhaub
juclfixtwhbflyalhfiFilqtaxjruglylaruqtfymbyuckiujlsuqytTufyhglz
zlyylfqytjeqoozljfilkxzzHtachnljqjyhfilyslhyfiujlxzzjklihglFiht
bzmfuufilyjfihfklntuktufubFiqjrutjrxltrlauljchnlrukhyajubqjhzzH
tafiqjfilthfxgliqlubYljuzqfxutXjjxrnzxlauglykxfifilehzlrhjfubfi
uqwifHtaltflyeyxjljubwylhfexfrihtacucltfKxfifixjylwhyafilxyRqyy
ltfjfqythkymHtazujlfilthclubHrfxutJubfmuqtukFilbhxyUeilzxhTmcei
xtfimUyxjutjSlhzzcmjxtjylclcslyla
```

(Ciphertext available in Moodle; capitalization only for readability; lower- and upper-case letters can be treated the same)

Exercise 2.2

Consider the same message scenario as in Exercise 1.1, but in this case the user utilizes the Vigenère cipher. For key lengths 2, 4 and 8 show how the attacker with access to the resulting ciphertext can determine the user's message, or explain why this is not possible.

Exercise 2.3

Consider the following simplification of the Enigma machine for just 6 letters $A = \{0, \ldots, 5\}$. It consists of an electric switchboard that implements a permutation π_k that swaps exactly two letters (and keeps the remaining letters the same) followed by 3 rotors and a reflector. A suitable switchboard configuration is the permutation $(1\,3)$ in cycle notation, which is the permutation $\pi\colon A \to A$ given by

$$\pi(0) = 0 \quad \pi(1) = 3 \quad \pi(2) = 2 \quad \pi(3) = 1 \quad \pi(4) = 4 \quad \pi(5) = 5 \ .$$

The rotors are given by their base permutations

$$\pi_1 = (0\,1\,5\,2\,3) \qquad \pi_2 = (0\,3\,4\,1\,5\,2) \qquad \pi_3 = (0\,5\,1)\,(2\,3)$$

in cycle notation. However, the rotors can be rotated, which adds or subtracts (modulo 6) to the elements in cycle notation. For example, rotating the first rotor one position downward yields the permutation $(1\,2\,0\,3\,4)$. We use $\pi_{1,k}$, $\pi_{2,k}$, and $\pi_{3,k}$ for the actual permutations implemented by the rotors given the key $k \in K$. Finally, the reflector can be formalized by the permutation $r = (1\,6)\,(2\,5)\,(3\,4)$ in cycle notation and it sends the signal backwards through the 3 rotors again. Thus, the encryption based on key k is

$$\begin{aligned} \mathrm{enc}_k(m) &= \pi_k^{-1}(\pi_{1,k}^{-1}(\pi_{2,k}^{-1}(\pi_{3,k}^{-1}(r(\pi_{3,k}(\pi_{2,k}(\pi_{1,k}(\pi_k(m)))))))))\\ \mathrm{enc}_k &= \pi_k \,;\, \pi_{1,k} \,;\, \pi_{2,k} \,;\, \pi_{3,k} \,;\, r \,;\, \pi_{3,k}^{-1} \,;\, \pi_{2,k}^{-1} \,;\, \pi_{1,k}^{-1} \,;\, \pi_k^{-1} \end{aligned}$$

(a) Determine a suitable key space for this encryption scheme.

(b) The full Enigma machine uses 26 letters and the electric switchboard swaps exactly 6 pairs of letters (and thus has 14 fixpoints). Determine a suitable key space for the full Enigma machine.

(c) Would you consider Enigma secure today?

Exercise 2.4

Let $\ell \in \mathbb{N}$ be the key and message length of a one-time pad encryption scheme $(\mathrm{gen}, \mathrm{enc}, \mathrm{dec})$. Since the key $k = 0^\ell$ leads to $\mathrm{enc}_k = \mathrm{dec}_k = \mathrm{id}_M$, we should maybe avoid this key. In other words, for this special key encryption and decryption do nothing and just return their input. We thus modify the encryption scheme such that

$$P_K(k) = \begin{cases} 0 & \text{if } k = 0^\ell \\ \frac{1}{2^\ell - 1} & \text{otherwise} \end{cases} \qquad \text{(uniform distribution on the nonzero keys)}$$

(For example, 'gen' returns the first ℓ bits from the random bit tape unless these bits are all 0. If they are all 0, then it recursively tries the next ℓ bits.) Is this scheme still perfectly secret? Prove your answer.

Exercise 2.5

Suppose a one-time pad encryption scheme with key length $\ell \in \mathbb{N}$. Obviously, the key space has size 2^ℓ, so we just try all 2^ℓ keys and decrypt a ciphertext with all those keys and accept the decryption if it returns proper English. This procedure obviously takes exponential time, but is clearly computable. However, we proved that one-time pad is perfectly secret. Explain the flaw in the above brute-force approach.

Exercise 2.6

Let $\ell \in \mathbb{N}$. Consider the following program: Draw k from a uniform distribution on $\{0,1\}^\ell$, draw m from any unknown distribution on $\{0,1\}^\ell$, and return $k \oplus m$. The two draws are independent. Prove that the program returns values uniformly distributed in $\{0,1\}^\ell$. (In other words, as long as one summand of an XOR is uniformly distributed, the XOR operation removes any bias; i.e., turns any arbitrary distribution of the other summand into a uniform output distribution.)