Universität Leipzig
Institute of Computer Science
Winter term 2026/2027

Andreas Maletti

Exercises for the lecture

Cryptography

Solutions to 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)

Solution: It is a monoalphabetic cipher and decrypts to the famous “To be or not to be” monologue of Shakepeare’s Hamlet.

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.

Solution: For key lengths 2 and 4, the first and fifth letter are both encrypted by the first letter of the key, so the same argument as before applies to this case. We can, for example, use the letter distance argument to determine the message. For key length 8, this attack is clearly not possible; in fact there is no attack at all because the cipher is perfectly secret in that case.

To show perfect secrecy, let us assume a uniformly distributed key and consider a ciphertext $c = c_1 \cdots c_8$. As expected, let $m =$ "superman" and $m' =$ "cablecar". Let us compute the relevant values (using the simplified formula for uniformly distributed keys) for perfect secrecy

$$\sum_{k \in K} \mathsf{P}[c \leftarrow \mathrm{enc}_k(m)] \stackrel{?}{=} \sum_{k \in K} \mathsf{P}[c \leftarrow \mathrm{enc}_k(m')]$$

As encryption is deterministic for the Vigenère cipher, these sums just count the number of keys that turn the messages m and m', respectively, into the ciphertext c. Obviously, there is exactly one key in both cases that induces the required letter shifts, so we obtain

$$1 = \sum_{k \in K} \mathsf{P}[c \leftarrow \mathrm{enc}_k(m)] = \sum_{k \in K} \mathsf{P}[c \leftarrow \mathrm{enc}_k(m')] = 1$$

showing that the Vigenère cipher with message space $M = \{m, m'\}$ and uniformly distributed keys of lenght 8 is perfectly secret.

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 $r = (0\,5)\,(1\,4)\,(2\,3)$ in cycle notation and it sends the signal backwards through the 3 rotors and switchboard again. Thus, the encryption based on key k is

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

(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?

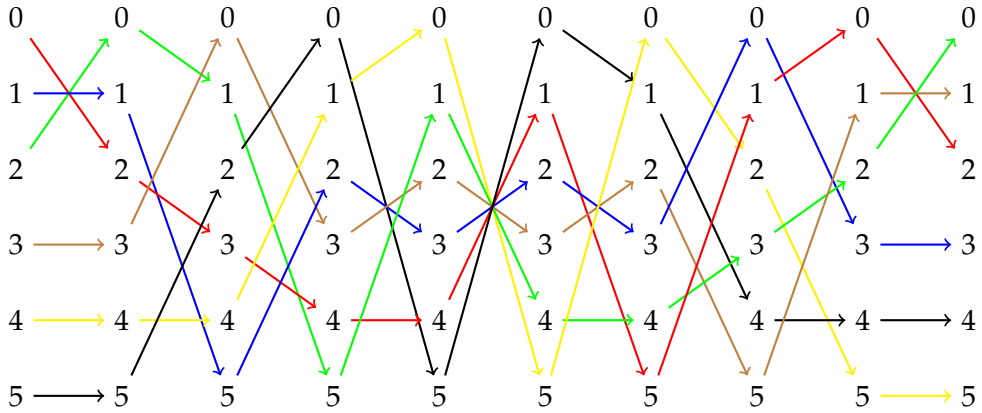
Solution:

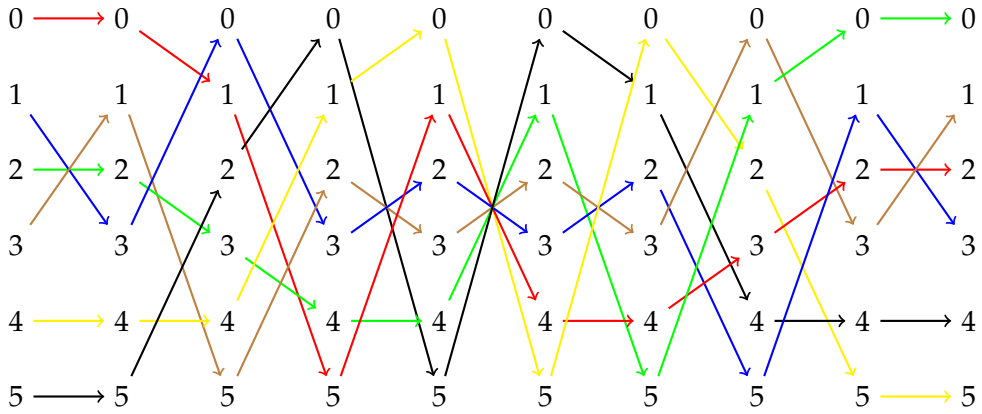
(a) Let $n = |A| = 6$. Obviously the switchboard configuration is part of the key. Since it is restricted to swap a single pair of letters, the key need only store two different letters, for which we have $n(n-1)$ options. Since the order of letters to be swapped is irrelevant, we actually only have $\binom{n}{2} = \frac{1}{2}n(n-1)$ options. Additionally, the positions of the rotors can be stored as offsets $a_1, a_2, a_3 \in A$. Thus, a suitable key space is

$$K = \{(b, b', a_1, a_2, a_3) \in A^5 \mid b < b'\}$$

and its size is $\binom{n}{2} \cdot n^3 = \frac{1}{2}(n-1)n^4 = 3,240$. However, since this version implements a monoalphabetic cipher (which is not true for the actual Enigma) the effective key space size is at most $6! = 720$. Indeed it is obvious to see that no input can map to itself in the output (since the switchboard and rotors essentially implement a fixed permutation h and due to the action of the reflector we always obtain $h^{-1}(5 - h(a)) \neq a$ for all $a \in A$. This holds because $5 - a' \neq a'$ for all $a' \in A$ and thus in particular $5 - h(a) \neq h(a)$. Since we have $h^{-1}(h(a)) = a$, $5 - h(a) \neq h(a)$, and h^{-1} is injective, we must have $h^{-1}(5 - h(a)) \neq h^{-1}(h(a)) = a$). Thus the number of actually achievable permutations is even smaller since the permutation cannot have a single fixpoint. For those interested, these permutations are called derangements and they lead to the effective key space size being at most $!6 = 265$.

Below are two configurations that lead to the same encryptions (i.e., 2 keys that act identically during encryption). Both implement the permutation $(0\,2)\,(1\,3)\,(4\,5)$. In the upper configuration we use the swap of 0 and 2 in the switchboard and the 3 rotors each in base position, so the key would be $(0, 2, 0, 0, 0)$ in our key space. In the lower configuration we swap 1 and 3 and again leave the rotors in their base position, so that key would be $(1, 3, 0, 0, 0)$.





(b) Using the same approach for the original Enigma alphabet, we let $n = 26$ and obtain

$$K = \Big\{ (b_1, b_1', \ldots, b_6, b_6', a_1, a_2, a_3) \in A^{15} \mid b_1 < b_1', \ldots, b_6 < b_6', \\ b_1 < b_2 < \cdots < b_6 \\ \big|\{b_1, b_1', \ldots, b_6, b_6'\}\big| = 12 \Big\}$$

and its size is

$$\frac{\binom{n}{2} \cdot \binom{n-2}{2} \cdot \binom{n-4}{2} \cdot \binom{n-6}{2} \cdot \binom{n-8}{2} \cdot \binom{n-10}{2}}{6!} \cdot n^3 = 100,391,791,500 \cdot 26^3 \\ = 1,764,486,127,404,000 \ .$$

Once again the effective key space size is limited by the number of possible permutations (or possible derangements), which is

$$26! = 403,291,461,126,605,635,584,000,000$$
$$!26 = 148,362,637,348,470,135,821,287,825$$

and thus no further limitation.

In the actual Enigma the 3 mentioned rotors could not only be rotated inside their rotor slot, but they could also be used in a different rotor slot. In other words, the rotor represented by π_1 could be slotted into the second or third rotor slot. This slightly extends the key space as the order of the rotors needs to become part of the key, but this would still yield a monoalphabetic cipher. However, in the original Enigma each input triggered a rotation of the rotor in the third rotor slot and once enough inputs were supplied to complete a full rotation of the last rotor, the second rotor would advance one position. Finally, the rotor in the first slot would advance one position once the middle rotor completed a full rotation. Naturally, these changes of the rotor orientations yield that the Enigma cipher is not monoalphabetic.

(c) The key space size, although impressive as a number, is way too small. Under the assumptions of Exercise 1.2 (Ryzen 9950x3D), brute-forcing this encryption scheme will only take time 2 h. If we instead use the Fujitsu Fugaku mentioned in the lecture we can brute-force it in $4 \cdot 10^{-3}$ s $= 4$ ms.

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.

Solution: Obviously this modified scheme is no longer perfectly secret. Consider the ciphertext $c = 1^\ell$ and the messages $m = 0^\ell$ and $m' = 1^\ell$. For perfect secrecy we need to have

$$\sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m)\big] \stackrel{?}{=} \sum_{k \in K} \mathsf{P}_K(k) \cdot \mathsf{P}\big[c \leftarrow \mathrm{enc}_k(m')\big] \ .$$

Clearly the left-hand side evaluates to $\frac{1}{2^\ell - 1}$ (using the only possible key 1^ℓ), whereas the right-hand side evaluates to 0 (using impossible key 0^ℓ). This inequality proves that the scheme is no longer perfectly secret.