Leipzig University
Institute of Computer Science
Winter Term 2020/21

Prof. Dr. Andreas Maletti
Fabian Tronicke

Cryptography

Exercise Sheet 2

will be discussed on November 10, 2020

Exercise 2.1

Decrypt the following ciphertext generated by a monoalphabetic substitution cipher:

```
JGRMQOYGHMVBJWRWQFPWHGFFDQGFPFZRKBEEBJIZQQOCIBZKLFAFGQVFZFWWE
OGWOPFGFHWOLPHLRLOLFDMFGQWBLWBWQOLKFWBYLBLYLFSFLJGRMQBOLWJVFP
FWQVHQWFFPQOQVFPQOCFPOGFWFJIGFQVHLHLROQVFGWJVFPFOLFHGQVQVFILE
OGQILHQFQGIQVVOSFAFGBWQVHQWIJVWJVFPFWHGFIWIHZZRQGBABHZQOCGFHX
```

We will not discuss this in detail in the exercise, but only compare the solution.

Exercise 2.2

When using the one-time pad with the key $k = 0^\ell$, then the ciphertext equals the message and encryption does nothing. To avoid this we could modify the one-time pad by only encrypting with $k \neq 0^\ell$ (i.e., to have gen choose k uniformly from the set of nonzero keys of length ℓ).
Is this modified scheme still perfectly secret?

Exercise 2.3

Proof: If k is drawn from a uniform distribution on $\{0,1\}^n$ and m is drawn from any distribution on $\{0,1\}^n$, the resulting $c = k \oplus m$ is also uniformly distributed. You can assume that m and k are drawn independently from each other.

Exercise 2.4

Are uniformly distributed ciphertexts needed for perfect secrecy?
Or more formally:
Proof or refute: If an encryption scheme $\mathcal{E}$ is perfectly secret, then in every scenario $(\mathcal{E}, \mathrm{P}_M)$ we have $\mathrm{P}(c) = \mathrm{P}(c')$ for all ciphertexts $c, c' \in C$.