Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 2

Exercise 1-4 was not finished in the first Tutorial and will be discussed in Tutorial 2.

Exercise 2-1

- Prove or disprove $P(A) \leq P(A \mid B) + P(\overline{B})$ for arbitrary A and B.
- In a lecture that has been given in 2015 and 2016, the exam results were as follows:

	2015	2016
very good	7%	10%
good	19%	21%
satisfactory	14%	22%
pass	23%	18%
fail	37%	27%

  Suppose you meet two students who took the lecture in the past two years, but not in the same year. The first student tells you that she achieved 'good' result. The second student only managed a 'satisfactory' result. What is the probability that the first student took the course in 2015?

Exercise 2-2 In the lectures, perfect secrecy was defined by means of an indistinguishabilily experiment. An encryption scheme Π is perfectly secret if and only if $P(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}) = 1/2$ for any adversary $\mathcal{A}$.

It was then stated in a Proposition that this definition is equivalent to requiring $P(M = m|C = c) = P(M = m)$ for all m and c that satisfy $P(C = c|M = m) \neq 0$.

In the lectures, only one direction of the proof of this equivalence was spelled out: that the definition with the indistinguishability experiment implies the other definition. Prove the implication in the other direction to complete the proof that the two definitions are equivalent.

Exercise 2-3 Assume given an arbitrary encryption scheme Π with $|\mathcal{K}| < |\mathcal{M}|$. Construct an adversary $\mathcal{A}$ for the indistinguishability experiment that satisfies $P(\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}) > 1/2$.