Prof. Martin Hofmann
Dr. Ulrich Schöpp

Ludwig-Maximilians-Universität München
Institut für Informatik
Summer 2017

Cryptography

Exercise Sheet 3

Exercise 2-3 was not finished in Tutorial 2 and will be discussed in Tutorial 3.

Exercise 3-1 Suppose that f is negligible. Show that the following functions are negligible for any polynomial p.

a) $g(n) := p(n) \cdot f(n)$

b) $h(n) := f(p(n))$, assuming that $n \leq p(n)$ holds for all n.

Solution (Sketch): The function f is negligible if for any positive polynomial q there exists a number N such that $f(n) < 1/q(n)$ for all $n > N$.

Question makes sense only if p goes from nat to nat.

a) Let r be any positive polynomial. Define $q(n) := r(n)p(n)$. Since f is negligible, there exists N, such that $f(n) < 1/q(n)$ for all $n > N$. Then, $g(n) = p(n) \cdot f(n) < p(n)/(r(n)p(n)) = 1/r(n)$.

b) (Note that if p is constant, then $h(n)$ is not negligible.)

   Let r be any positive polynomial. Since f is negligible, there exists N, such that $f(n) < 1/r(n)$ for all $n > N$. For any positive polynomial r, there exists a number M, such that r is monotonically increasing. (The derivative of polynomials is a polynomial and has only a constant number of roots. From a certain point on, its sign cannot change.) Thus, $n \leq p(n)$ implies $r(n) \leq r(p(n))$ for all large enough n. This implies $1/r(p(n)) \leq 1/r(n)$, so we get the required $h(n) = f(p(n))) < 1/r(p(n)) \leq 1/r(n)$.

Exercise 3-2 The notion of indistinguishability in the presence of an eavesdropper was defined using an experiment in which the adversary must choose two messages of the same size in the first step. Show that if the adversary were not restricted to messages of the same size, then no encryption scheme would be indistinguishable in the presence of an eavesdropper.

Hint: Consider how large the cryptotext of any particular message could be.

Solution (Sketch): Consider the length of a single character message m for any parameter n. Since all algorithms are required to be probabilistic polynomial time, the length of any key and thus any cryptotext must be polynomial in n. Hence, there exists a polynomial q, such that the cryptotext of any single-character message has length $\leq q(n)$.

Define $\mathcal{A}$ so that it first outputs $m_0 := 0$ and a random message of length $m_1 := q(n) + 3$.

When given the ciphertext c, $\mathcal{A}$ outputs $b' := 1$ if c is longer than $q(n)$ and $b' := 0$ otherwise.

What is the probability that $\mathcal{A}$ gives the wrong answer? If the code c is long, then $\mathcal{A}$ can be sure that the message must have been m_1. But long messages could also map to short codes, so $\mathcal{A}$ could mistakenly output $b' = 1$ if the code c is short. What is the probability of this? There are $2^{q(n)+1} - 1$ messages of size $\leq q(n)$. Since there are $2^{q(n)+3}$ possible source messages, only $2^{q(n)+1}/2^{q(n)+3} = 1/4$ of these messages can have a short code. Hence, $\mathcal{A}$ will give the wrong answer in at most $1/4$ of all cases. This is clearly better than negligible.

Exercise 3-3 Let G be a pseudorandom generator. Which of the following definitions defines a pseudorandom generators as well?

a) $G_1(s) = G(s_0 \dots s_{\lfloor n/2 \rfloor})$, where n is the length of n and s_i is the i-th character in s. Thus, for example, $G_1(01101) = G(011)$.

Solution (Sketch): This defines a pseudorandom generator.

We have to show that $|P(D(r) = 1) - P(D(G_1(s)) = 1)|$ is negligible. We can split s into two random variables s_1 and s_2, of half the length such that $s = s_1 s_2$. Then the above becomes $|P(D(r) = 1) - P(D(G_1(s_1 s_2)) = 1)|$ which is the same as $|P(D(r) = 1) - P(D(G(s_1)) = 1)|$.

By assumption we know that $|P(D(r) = 1) - P(D(G(s_1)) = 1)|$ is less than $1/q(n/2)$ for any polynomial q (note that s_1 has length $n/2$). So, if p is any polynomial, then we can define $q(m) := p(2m)$, and we have $1/q(n/2) = 1/(p(2n/2)) = 1/p(n)$. This means that $|P(D(r) = 1) - P(D(G(s_1)) = 1)|$ is negligible, which is what we had to show.

b) $G_2(s) = G(s)G(s)$, where juxtaposition denotes concatenation of words.

Solution (Sketch): This is not always pseudorandom.

Let us construct a distinguisher D that can distinguish G_2 from a true random source with non-negligible probability. Define $D(v)$ to be 0 if v has the form ww for some w, and 1 otherwise. This is clearly computable in polynomial time.

Consider $|P(D(r) = 1) - P(D(G_2(s)) = 1)|$. There are 2^n possible values for the random variable s and $2^{2l(n)}$ possible values for r (and the sample space is made up from these possibilities). By definition, $P(D(r) = 1) = (2^{2l(n)} - 2^{l(n)})/2^{2l(n)} =$

$1 - 1/2^{l(n)}$ ($2^{2l(n)}$ is the number of possibilities for r, $2^{l(n)}$ is the number of possibilities for words of the form ww). Further, $P(D(G_2(s)) = 1) = 0$. So, overall $|P(D(r) = 1) - P(D(G_2(s)) = 1)| = 1 - 1/2^{l(n)}$, which is clearly not negligible.

c) $G_3(s) = G(s_0 \dots s_{\lfloor n/2 \rfloor}) G(s_{\lfloor n/2 \rfloor + 1} \dots s_{n-1})$

Solution (Sketch): By assumption on G, we know that for any probabilistic polynomial time distinguisher D we have $|P(D(r) = 1) - P(D(G(s)) = 1)| \leq f_1(n)$ for some negligible function f_1.

For any fixed s' we can then show that for any polynomial time distinguisher E we have $|P(E(rG(s')) = 1) - P(E(G(s)G(s')) = 1)| \leq f_{s'}(n)$ for some negligible $f_{s'}$. Consider arbitrary E. Then we can construct D as follows: On input w, compute $G(s')$ and invoke $E(wG(s'))$. This has the right format for a distinguisher for G. By construction, we have $|P(E(rG(s')) = 1) - P(E(G(s)G(s')) = 1)| = |P(D(r) = 1) - P(D(G(s)) = 1)|$. This quantity must be negligible by assumption on G.

Now we note $P(E(rG(t)) = 1) = \sum_{s'} P(E(rG(t)) = 1 \mid t = s') \cdot P(t = s')$ and $P(E(G(s)G(t)) = 1) = \sum_{s'} P(E(G(s)G(t)) = 1 \mid t = s') \cdot P(t = s')$, where t is a random variable with uniform distribution. Hence,

$$
\begin{aligned}
&|P(E(rG(t)) = 1) - P(E(G(s)G(t)) = 1)| \\
&= \left| \sum_{s'} P(E(rG(t)) = 1 \mid t = s') \cdot P(t = s') - \sum_{s'} P(E(G(s)G(t)) = 1 \mid t = s') \cdot P(t = s') \right| \\
&= \left| \sum_{s'} P(t = s') \cdot (P(E(rG(s')) = 1) - P(E(G(s)G(s')) = 1)) \right| \\
&\leq \sum_{s'} P(t = s') \cdot f_2(n) \\
&\leq f_2(n) \ ,
\end{aligned}
$$

where $f_2(n) := \max_{s'} f_{s'}(n)$, which is still negligible.

By analogous reasoning, we get $|P(E(ru) = 1) - P(E(rG(t)) = 1)| \leq f_3(n)$.

Putting this together, we get:

$$
\begin{aligned}
&|P(E(ru) = 1) - P(E(G(s)G(t)) = 1)| \\
&= |P(E(ru) = 1) - P(E(rG(t)) = 1) - (P(E(G(s)G(t)) = 1) - P(E(rG(t)) = 1))| \\
&\leq |P(E(ru) = 1) - P(E(rG(t)) = 1)| + |P(E(G(s)G(t)) = 1) - P(E(rG(t)) = 1)| \\
&\leq f_2(n) + f_3(n)
\end{aligned}
$$

This is negligible, as required.

d) $G_4(s) = G(ss)$

Solution (Sketch): This is not always pseudorandom. Take, for example, G_3 for G. Then G_4 becomes just G_2, and we have argued above that this is not pseudorandom.