

SOLUTION OF EXERCISESHEET 3

Exercise 3-1

Trying some values:

$$\begin{array}{llllll}
 k = 2 & a = 27 & b = 72 & c = |b - a| = 72 - 27 = 45 & d = 45 & e = 54 \\
 k = 3 & a = 398 & b = 983 & c = |983 - 398| = 585 & d = 585 & e = 558 \\
 k = 3 & a = 398 & b = 938 & c = |983 - 398| = 441 & d = 441 & e = 144 \\
 k = 3 & a = 321 & b = 213 & c = |321 - 213| = 108 & d = 18 & e = 81
 \end{array}$$

In the table above one can see that the sum of the digits of d , respectively e is always a multiple of 9.

The reason for this lies in the construction of the 'pseudorandom generator'. b has the same digits like a only in an other order. To get c we subtract the greater number of those from the smaller, so c is always positive. Then we remove all 0-digits to get d and scramble the letters again for e . The sum of digits didn't change after the computation of c , so we look at c to argue that this sum is always a multiple of 9.

If $a > b$ we compute for the sum of the digits of $c = a - b$: $(a_1 - b_1) + (a_2 - b_2) + \dots + (a_n - b_n) = a_1 + a_2 + \dots + a_n - (b_1 + b_2 + \dots + b_n)$. But this only hold if $a_n > b_n$.

If $a_i < b_i$ then it is $(a_1 - b_1) + (a_2 - b_2) + \dots + (a_{i-1} - b_{i-1} - 1) + (a_i - b_i + 10) + \dots + (a_n - b_n) = a_1 + a_2 + \dots + a_n - (b_1 + b_2 + \dots + b_n) + 9$

The sum of the digit of a has to be the same like the sum of the digits from b , because b has the same digits like a only in an other order, so $a_1 + a_2 + \dots + a_n - (b_1 + b_2 + \dots + b_n) = 0$.

If $a_i < b_i$ holds for y positions the sum of the digits is $9 \cdot y$. a and b have the same digits, so $a_i < b_i$ holds at least for one position, so $y \geq 1$.

This argumentation is the same for $b > a$, so the sum of the digits from c , respectively d or e , is always a multiple from 9.

If now all but the last digit of e are given one can always determine the last digit, because the sum of all digits has to be a multiple of 9. So the described generator does not pass the next-character test.

If the sum of the digits is already 9, the last bit has to be 9 as well, because all 0-digits had erased. If this is not the case, we could not determine if the last digit has to be 0 or 9.

Exercise 3-2

(a) Is $G_a(s) = G(s)||0$ a secure PRG?

No since the last bit is always 1. This bit is not uniformly at random because the probability of that bit being 1 is 100% instead of 50%.

$\Rightarrow G_a$ is not a PRG

(b) Is $G_b(s||b) = G(s)||b$ where $|b| = 1$ a secure PRG?

Yes because adding a single random but fixed bit has the probability 50% being 1 and 50% being 0 meaning b is uniformly random. $b = \{0, 1\}$ is a pseudorandom generator and the concatenation of two pseudorandom number generators is a pseudorandom number generator itself. Also since b is part of the argument G_b is deterministic.

$\Rightarrow G_b$ is a secure PRG

(c) Is $G_c(s) = G(s)||0$ a secure PRG?



SOLUTION OF EXERCISESHEET 3

(d) Is $G_d(s) = G(s || 0^{|s|})$ a secure PRG?

(e) Is $G_e(s) = G(s) \oplus 1^{|s|}$ a secure PRG?

Yes because $G(s) \oplus 1^{|s|} = G(s)$ and $G(s)$ is per definition a secure PRG.

\Rightarrow Therefore $G_e(s)$ is also a secure PRG.

(f) Is $G_f(s) = \text{trunc}(G(\text{trunc}(s)))$ a secure PRG?

where $\text{trunc}(x)$ for a nonempty string x denotes all but the last bit of x .

(For this part, assume that $l(n) \leq n + 2$, and ignore the fact that G_f is undefined on input strings of length 1.)