# Homework Assignment 9

Due before 7:00 pm, Thursday, December 10, 2020

**Instructions** Work the problems below, prepare your answers in electronic form, and submit your solutions to Canvas as usual. As always, you must properly cite all resources that you use to solve the problems.

## 1 Zero knowledge (6 points)

Alice used the simplified one-round FFS protocol (lecture 19a) to convince Bob that her publicly posted number $v$ is a quadratic residue modulo $n$, where $n$ is the product of distinct odd primes. ($n$ is also public.) In the course of their conversation, they generated a transcript of 20 triples $(x_i, b_i, y_i)$, $i = 1, \ldots, 20$.

Bob is excited to learn that Alice was telling the truth when she told him that not only is $v$ a quadratic residue, but she also knows a square root of it. He tells his friend Charlie that Alice really was truthful and that Charlie should trust Alice. To convince Charlie, Bob forwards him a copy of the transcript.

Charlie isn't convinced of anything and still doesn't trust Alice. Why not? Explain!
[Hint: Show how Bob could have constructed the transcript without knowing Alice's secret (and without even talking to Alice).]

## 2 Cryptographically strong PRSG (4 points)

Happy's roommate, Naive Nelson, is building a pseudorandom sequence generator. He has found a PRSG $G$ that takes a 128-bit seed $s$ and outputs a bit string $x$ of length 1000. Naive wants to generate bit strings of length $\ell = 100,000$, so he creates a new generator $G'$ that works in stages. His idea is to use $G$ repeatedly, obtaining 1000 bits each time. To avoid getting repetitions of the same 1000-bit string, he uses the last 128 bits of each block as a seed for the next block.

Here is his algorithm for computing $G'(s)$:

$s$ is the initial seed;
$i \leftarrow 0$;
$y \leftarrow \lambda$;
**while** $i < 100$ **do**
  $x \leftarrow G(s)$;
  $s \leftarrow \text{last}(128, x)$;
  $i \leftarrow i + 1$
  $y \leftarrow y \,||\, x$
**end while**
**return** $y$;

In this notation, $\lambda$ denotes the empty string, $||$ denotes concatenation, and $\text{last}(k, x)$ returns the last $k$ bits of $x$.

Explain in words why $G'(s)$ is not cryptographically strong.
[Hint: Describe how knowing some of the pseudorandom output bits allows the rest to be easily predicted.]