CS4236 Individual Assignment 2

September 7, 2022

1 The rules...

As before.

Assignment deadline is 5pm, 30th Sept 2022. Uploaded to the Canvas assignment submission folder in pdf format. The file name should be like e00XXXXXX.A1.pdf (Your student id and ".A1.pdf").

2 Questions - 5 assignment questions, due 30th Sept.

1. Let $G(s) \stackrel{\text{def}}{=} s \oplus \text{rand}()$, where rand() is a function which returns a truly random bitstring the same size as s, and as usual, $\oplus$ is XOR. Prove or disprove that $G(s)$ is a PRG (a pseudorandom generator). (2 marks)

2. Let $G : \{0,1\}^n \to \{0,1\}^{2n}$ be a PRG. Prove or disprove that the function $G'(s) \stackrel{\text{def}}{=} G(s')$ is also a PRG, where s' is the least significant $n-1$ bits of s. (3 marks)

3. A length preserving function is where the key, the index and the result are all the same size. For example the function $F : \{0,1\}^n \times \{0,1\}^n \to \{0,1\}^n$. If $n = 4$, how many different such functions are there? (2 marks)

4. In the third lecture session, we saw Construction 3.17 which was EAV-Secure (Theorem 3.18, described in class, is the proof). Prove the opposite - i.e. if G is not a PRG, then 3.17 cannot be EAV-secure. (4 marks)

5. Construct a PRG G from a (length preserving) PRF F, and show it is a PRG. (4 marks)