Cryptography: HW2

Due electronically (via TEACH) on **Wednesday** 27 Jan

1. Which of the following are negligible functions? Justify your answers.

$$\sqrt{\frac{\lambda}{2^\lambda}} \quad \frac{1}{2^{\log(\lambda^2)}} \quad \frac{1}{\lambda^{\log(\lambda)}} \quad \frac{1}{\lambda^2} \quad \frac{1}{2^{(\log\lambda)^2}} \quad \frac{1}{(\log\lambda)^2} \quad \frac{1}{\sqrt{\lambda}} \quad \frac{1}{2^{\sqrt{\lambda}}}$$

2. Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a length-doubling PRG, and consider the algorithm $H : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ given below:

```
H(s):
  x := G(s)
  y := G(0^λ)
  return x ⊕ y
```

   Using the fact that G is a secure PRG, prove that H is also a secure PRG.

3. Let $G : \{0,1\}^\lambda \to \{0,1\}^{2\lambda}$ be a secure length-doubling PRG and consider the algorithm $H : \{0,1\}^\lambda \to \{0,1\}^{3\lambda}$ given below:

```
H(s):
  x := G(s)
  return s||x
```

   Show that H is **not** a secure PRG (even if G is). Describe a successful distinguisher for $\mathcal{L}^H_{\text{prg-real}}$ and $\mathcal{L}^H_{\text{prg-rand}}$. Explicitly compute its advantage.

   Hint: Remember, you are not attacking G. In fact, G may be the best PRG in the world. You are attacking the faulty way in which H uses G.

4. Suppose F is a secure PRF. Define the following function F' as:

$$F'(k, x||x') = F(k,x)||F(k, x \oplus x').$$

   Here, x and x' are each in bits long, where in is the input length of F. Show that F' is **not** a secure PRF (even if F is). Describe a distinguisher and compute its advantage.

   Hint: Remember, you are not attacking F. In fact, F may be the best PRF in the world. You are attacking the faulty way in which F' uses F.