Indistinguishable Encryptions in the Presence of an Eavesdropper
Class Exercise—2/22/18

Assume G is a PRG with input length n and output length $n+1$. Do the following encryption schemes Π have indistinguishable encryptions in the presence of an eavesdropper? If yes, formally prove that if G is a PRG then the scheme is secure. If not, present a ppt adversary A and show that $\Pr\left[PrivK^{eav}{}_{A,\Pi}(n) = 1\right] \geq 1/2 + \rho(n)$ for some non-negligible $\rho()$.

1. Π is defined as follows: Gen outputs a random key k of length n. To encrypt a message $m = m_1||m_2$, where m_1, m_2 each have length $n+1$, output $c \coloneqq (c_1||c_2) \coloneqq G(k) \oplus m_1 \,||\, G(k) \oplus m_2$. To decrypt output $m_1||m_2 = G(k) \oplus c_1||G(k) \oplus c_2$.

2. Π is defined as follows: Gen outputs a random key k of length n. To encrypt a message m, where m has length $n+1$, output $c := G(k) \oplus m\,||0^n$. To decrypt, output the first n bits of $c \oplus (G(k)||0^n)$.