CSA E0 235: Cryptography 16/08/2019

Tutorial 2

Instructor: Arpita Patra *Question Set*

1. Consider a variant of the one time pad with message space $\{0,1\}^L$ where the key space $\mathcal{K}$ is restricted to all L-bit strings with an even number of 1s. Is this scheme perfectly indistinguishable?

2. The message space is $\mathcal{M} = \{m \in \{0,1\}^l |$ the last bit of m is $0\}$. **Gen** chooses a uniform key from $\{0,1\}^{l-1}$. $\mathbf{Enc}_k(m)$ returns ciphertext $m \oplus (k||0)$, and $\mathbf{Dec}_k(c)$ returns $c \oplus (k||0)$. Is the scheme perfectly secure?

3. Let $E = (\mathbf{E}, \mathbf{D})$ be a semantically secure cipher defined over $(\mathcal{K}, \mathcal{M}, \mathcal{C})$, where $\mathcal{M} = \mathcal{C} = \{0,1\}^L$. Are the following encryption schemes perfectly indistinguishable? Prove or refute :

   - $E_1(k,m) := E(k,m)||\ parity(m)$
   - $E_2(k,m) := E(k, reverse(m))$

4. Modify the one-time pad so that keys are used twice. That is, let the key-space $\mathcal{K}$ be such that first a key k' is uniformly chosen from $\{0,1\}^{l/2}$ and then the key is denoted by k = $k'||k'$ where $||$ denotes concatenation. In addition, define $M = C = \{0,1\}^l$. Prove or disprove that this scheme is perfectly secure.