Problem 3 – Problem Set 3 – Due Wednesday, April 20, 2016

Problem 5.

Part 5A. Alice would like to privately send a bit \( a \in \{0, 1\} \) to Bob. They share a uniformly random key \( k \in \{0, 1, 2\} \). How can Alice send her bit to Bob in a way that achieves the property we called perfect privacy? Justify your answer.

Part 5B. Alice shuffles a deck of cards and deals it out to herself and Bob so that each gets half of the 52 cards. Alice now wishes to send a secret message \( M \) to Bob. Eavesdropper Eve is watching and sees the transmissions.

Suppose Alice’s message \( M \in \{0, 1\}^{48} \) is a string of 48 bits. Describe how Alice can communicate \( M \) to Bob in a way that achieves perfect privacy.

Part 5C. Now suppose Alice’s message \( M \in \{0, 1\}^{49} \) is 49 bits. Prove that there does not exist a protocol that allows Alice to communicate \( M \) to Bob in a way that achieves perfect privacy.

Problem 6. The RC4 algorithm maps a key \( K \in \text{Byte}^k \) to a keystream \( RC4(K) \), where \( k \in [1..255] \). Investigate empirically the probability \( p_i \) that the second byte of RC4 output is \( i \in \{0, \ldots, 9\} \) (written as a byte). For concreteness, assume a key length of \( k = 16 \) bytes. Now describe a simple adversary to distinguish RC4 output (with a random 16-byte key) from truly random bits. Estimate your adversary’s advantage.

Problem 7. Let \( \mathcal{F} : K \times N \times N \rightarrow \{0, 1\}^n \) be a stream cipher that, on input \((K, N, n)\), outputs an \( n \)-bit string. We defined the advantage of an adversary \( A \) in attacking \( \mathcal{F} \) to be

\[
\text{Adv}^1_{\mathcal{F}}(A) = \Pr[A^{\mathcal{F}(K, \cdot, \cdot)} \rightarrow 1] - \Pr[A^{\mathcal{F}(\cdot, \cdot, \cdot)} \rightarrow 1].
\]

The first oracle chooses a random key \( K \leftarrow \mathcal{K} \) and then, on input \((N, n)\), outputs \( \mathcal{F}(K, N, n) \). The second oracle, on input \((N, n)\), outputs \( n \) random bits. Either way, the adversary is not allowed to ask invalid queries or to repeat the first component (the \( N \)-value) of any query.

Consider a related definition for advantage, where we say

\[
\text{Adv}^2_{\mathcal{F}}(A) = 2 \Pr[b \leftarrow \{0, 1\}; \text{if } b = 1 \text{ then } K \leftarrow \mathcal{K}, f(\cdot, \cdot) \leftarrow \mathcal{F}(K, \cdot, \cdot) \text{ else } f \leftarrow \$ \text{ : } A^{f(\cdot, \cdot)} \rightarrow b] - 1.
\]

As before, the adversary is not allowed to ask invalid queries or to repeat \( N \)-values.

Give a clear English-language description of the adversary’s aim in the second definition. Then prove that the two notions are identical: \( \text{Adv}^1_{\mathcal{F}}(A) = \text{Adv}^2_{\mathcal{F}}(A) \).