Cryptography: Homework 3

(Deadline: October 18, 2018)

1. (15 points) Let n be a positive integer. A *Latin square* of order n is an $n \times n$ matrix $L = (\ell_{i,j})_{1 \le i,j \le n}$ with entries $\ell_{i,j} \in \{1, 2, \ldots, n\}$, such that each element of the set $\{1, 2, \ldots, n\}$ appears exactly once in each row and each column of L. A Latin square defines a private-key encryption Π over the message space $\mathcal{M} = \{1, 2, \ldots, n\}$ and the key space $\mathcal{K} = \{1, 2, \ldots, n\}$: **Gen** simply chooses a key $k \leftarrow \mathcal{K}$ uniformly at random, and the encryption of a plaintext $m \in \mathcal{M}$ under k is defined by $c = \mathbf{Enc}(k, m) = \ell_{k,m}$. Show that the private-key encryption Π defined by a Latin square is perfectly secret.

2. (30 points) Let Π denote the Vigenère cipher where the message space consists of all 3-character strings (over the English alphabet), and the key is generated by first choosing the period t uniformly from $\{1, 2, 3\}$ and then letting the key be a uniform string of length t.

   (a) Define $\mathcal{A}$ as follows: $\mathcal{A}$ outputs $m_0 =$ aab and $m_1 =$ abb. When given a ciphertext c, it outputs 0 if the first character of c is the same as the second character of c, and outputs 1 otherwise. Compute $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$.

   (b) Construct and analyze an adversary $\mathcal{A}'$ for which $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A}',\Pi} = 1]$ is greater than your answer from part (a).