# Exercise Sheet 3

*Cryptography and Security 2022*

## Exercise 1 Latin Squares

Let $n$ be a positive integer. A *Latin square* of order $n$ is an $n \times n$ matrix $L = (\ell_{i,j})_{1 \leq i,j \leq n}$ with entries $\ell_{i,j} \in \{1, \ldots, n\}$, such that each element of the set $\{1, \ldots, n\}$ appears exactly once in each row and each column of $L$. A Latin square defines a cipher over the message space $\mathcal{X} = \{1, \ldots, n\}$ and the key space $\mathcal{K} = \{1, \ldots, n\}$, for which the encryption of a plaintext $x \in \mathcal{X}$ under a key $k \in \mathcal{K}$ is defined by $y = C_k(x) = \ell_{k,x}$.

1. Find a Latin square $L$ of order 4. Using this matrix, encrypt the plaintext $x = 3$ with the key $k = 2$.

2. Prove that a Latin square defines a cipher which achieves perfect secrecy if the key is uniformly distributed, independent from the plaintext, and used only once.

## Exercise 2 Vernam with Two Dice

Our crypto apprentice decided to encrypt messages $x \in \mathbf{Z}_{12}$ (instead of bits) using the generalized Vernam cipher in the group $\mathbf{Z}_{12}$. As he did not fully understand the course, he decided to pick a key $k$ (for each $x$) by rolling two dice (with 6 faces numbered from 1 to 6) and setting $k = k_1 + k_2$ to the sum of the two faces up $k_1$ and $k_2$. The encryption of $x$ with key $k$ is then $y = (x + k) \bmod 12$.

1. Why is this encryption scheme insecure?

2. We still use $k = k_1 + k_2$. Given a factor $n$ of 12, we now take $x \in \mathbf{Z}_n$ and $y = (x + k) \bmod n$. Show that for some values $n$, this provides perfect secrecy but for others, this does not. (Consider *all* factors $n$ of 12.)

3. Finally, the crypto apprentice decides to encrypt a bit $x \in \{0, 1\}$ into $y = (x + k) \bmod 4$, still with $k = k_1 + k_2$ from rolling the two 6-face dice. We assume that $x$ is uniformly distributed in $\{0, 1\}$. For each $c$, compute the probabilities $\Pr[x = 0 | y = c]$ and $\Pr[x = 1 | y = c]$.

4. By taking $\tilde{x} \in \{0, 1\}$ as a function of $c$ such that $\Pr[x = \tilde{x} | y = c]$ is maximal, compute the probability $P_e = \Pr[x \neq \tilde{x}]$ (still when $x$ is uniform in $\{0, 1\}$).

## Exercise 3 Subgroup

Let $G$ be a multiplicative group and $S$ a non-empty subset of $G$ such that for all $a, b \in S$ we have $ab^{-1} \in S$. Show that $S$ is a group.

## Exercise 4 Pairwise Different Sampling

We throw an unbiased dice 12 times and get the samples $x_1, \ldots, x_{12} \in \{1, \ldots, 6\}$. We define pairs $y_i = (x_{2i-1}, x_{2i})$ for $i \in [1, 6]$ i.e., $y_1 = (x_1, x_2)$, ..., $y_6 = (x_{11}, x_{12})$. What is the probability that

- $\forall i, j \in \{1, \ldots, 6\}, i \neq j$ we have, $y_i \neq y_j$
- $\exists i, j \in \{1, \ldots, 6\}, i \neq j$ s.t., $y_i \neq y_j$