Solution Sheet 3

Cryptography and Security 2025

Solution 1 Latin Squares

1. An example of Latin square of order 4 is

$$L = \begin{pmatrix} 1 & 4 & 3 & 2 \\ 4 & 2 & 1 & 3 \\ 2 & 3 & 4 & 1 \\ 3 & 1 & 2 & 4 \end{pmatrix}$$

and $C_2(3) = \ell_{2,3} = 1$.

2. Let X be the random variable corresponding to the plaintext, Y be the random variable corresponding to the ciphertext, and K be the random variable corresponding to the key. We have

$$\begin{aligned} \Pr[X = x, Y = y] &= \sum_{k=1}^{n} \Pr[X = x, Y = y \mid K = k] \Pr[K = k] \\ &= \frac{1}{n} \sum_{k=1}^{n} \Pr[X = x, Y = y \mid K = k], \end{aligned}$$

since the key is uniformly distributed. Moreover

$$\Pr[X = x, Y = y \mid K = k] = \mathbf{1}_{\ell_{k,x}=y} \Pr[X = x \mid K = k],$$

as for a given message x and key k there is only one corresponding ciphertext y. Finally, as X and K are independent,

$$\begin{aligned} \Pr[X = x, Y = y] &= \frac{1}{n} \sum_{k=1}^{n} \mathbf{1}_{\ell_{k,x}=y} \Pr[X = x] \\ &= \frac{\Pr[X = x]}{n} \sum_{k=1}^{n} \mathbf{1}_{\ell_{k,x}=y} \\ &= \frac{\Pr[X = x]}{n}, \end{aligned}$$

because, as L is a Latin square, for any x and y there is one, and only one value k such that $\ell_{k,x} = y$. On the other hand

$$\begin{aligned} \Pr[Y = y] &= \sum_{x=1}^{n} \Pr[Y = y, X = x] \\ &= \frac{1}{n} \sum_{x=1}^{n} \Pr[X = x] \\ &= \frac{1}{n}. \end{aligned}$$

We conclude that $\Pr[X = x|Y = y] = \Pr[X = x]$ which concludes the proof.

Solution 2 Vernam with Two Dice

1. In the generalized Vernam cipher, k must be uniformly distributed in $\mathbf{Z}_{12}$. Here, k is a number from 2 to 12. It is not a big deal as it is equivalent to use $k \bmod 12$, but the distribution of $k \bmod 12$ we obtain is far from being uniform in $\mathbf{Z}_{12}$. For instance, $\Pr[k \bmod 12 = 2] = \frac{1}{36}$ and $\Pr[k \bmod 12 = 7] = \frac{1}{6}$.

2. We just have to say for which n is $k \bmod n$ uniformly distributed. Since $k = k_1 + k_2$, the sum of the values k_1 and k_2 of the two dice, and since k_1 and k_2 are independent and uniformly distributed modulo 6, the scheme is secure when n is a factor of 6: $n \in \{1, 2, 3, 6\}$. For $n = 12$, we have seen it is not secure. What remains is $n = 4$.

   $k_1 \bmod 4$ and $k_2 \bmod 4$ have distribution $\Pr[k_i \bmod 4 = i] = \frac{1}{6}$ for $i \in \{0, 3\}$ and $\Pr[k_i \bmod 4 = i] = \frac{1}{3}$ for $i \in \{1, 2\}$. So, $\Pr[k \bmod 4 = 0] = \frac{1}{4}$, $\Pr[k \bmod 4 = 1] = \frac{2}{9}$, $\Pr[k \bmod 4 = 2] = \frac{1}{4}$, and $\Pr[k \bmod 4 = 3] = \frac{5}{18}$. So, it is not uniform and the scheme is not secure for $n = 4$.

3. Using the Bayes formula, we have

$$\Pr[x = b | y = c] = \frac{\Pr[y = c | x = b] \Pr[x = b]}{\sum_{b'} \Pr[y = c | x = b'] \Pr[x = b']}$$

   Clearly, $\Pr[y = c | x = b'] = \Pr[k \equiv c - b' \pmod 4]$ due to the independence between x and k. Since x is uniformly distributed, we obtain

$$\Pr[x = b | y = c] = \frac{\Pr[k \equiv c - b]}{\sum_{b'} \Pr[k \equiv c - b']} = \frac{\Pr[k \equiv c - b]}{\Pr[k \in \{c, c-1\}]}$$

   where values of k are taken modulo 4. Using the distribution that we computed in the previous question, we can fill the following table:

c	$\Pr[x = 0 \mid y = c]$	$\Pr[x = 1 \mid y = c]$
0	9/19	10/19
1	8/17	9/17
2	9/17	8/17
3	10/19	9/19

4. We have $\tilde{x} = 1$ for $c = 0$, $\tilde{x} = 1$ for $c = 1$, $\tilde{x} = 0$ for $c = 2$, and $\tilde{x} = 0$ for $c = 3$. For $x = 0$, $x \neq \tilde{x}$ when $c \in \{0, 1\}$ so $k \bmod 4 \in \{0, 1\}$. For $x = 1$, $x \neq \tilde{x}$ when $c \in \{2, 3\}$ so $k \bmod 4 \in \{1, 2\}$. So, $P_e = \frac{1}{2}\left(\frac{1}{4} + \frac{2}{9}\right) + \frac{1}{2}\left(\frac{2}{9} + \frac{1}{4}\right) = \frac{17}{36} = \frac{1}{2} - \frac{1}{36}$.

Solution 3 Subgroup

In order to prove that S is a group we have to show it fulfils all the properties of a group:

1. neutral element: for an $a \in S$ we have that $aa^{-1} = e \in S$, thus S contains the neutral element e.

2. invertibility: we have that $e \in S$. Then, for any $a \in S$, we have $ea^{-1} \in S$, thus $a^{-1} \in S$.

3. closure: for any $a, b \in S$, we have that $b^{-1} \in S$, thus $a(b^{-1})^{-1} = ab \in S$.

4. associativity: it is inherited from G.

We have proven that S is a group.

Solution 4 Pairwise Different Sampling

Assume each pair as a number with two digits which can have 36 possibilities. The overall probability would be

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

$$\frac{(36)(35)(34)(33)(32)(31)}{6^{12}} = 0.644$$

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

$$1 - \frac{(6)^2}{6^{12}} = 1 - 6^{-10}$$