Problem sheet 1 for Course 02231, 2025

These practice problems have the purpose of helping you understand the material better and learning the skills that are necessary to analyze cryptographic constructions, and sometimes to prepare you for the next class. All answers should be supported by a written justification. To gauge whether a justification is sufficient, ask yourself if your peers would be convinced by it without additional explanations.

Exercise 1.1 This exercise is in preparation for the second lecture. We start by recapping some notation. A random variable X on a finite set $\mathcal{V}$ is an element of $\mathcal{V}$ chosen at random according a probability distribution $D : \mathcal{V} \to \mathbb{R}$, i.e. a function such that $D(x) \geq 0$ for all $x \in \mathcal{V}$ and

$$\sum_{x \in \mathcal{V}} D(x) = 1.$$

We write $X \leftarrow D$ to mean "X is sampled according to D". If D is the uniform distribution, i.e. $D(x) = \frac{1}{|\mathcal{V}|}$ for all x, then we also write $X \leftarrow \mathcal{V}$.

a) Let $X_1, X_2, X_3, X_4 \leftarrow \{1, 2, 3, 4, 5, 6\}$ be four throws of a fair die. Compute the probability that $X_i = 6$ for at least one $i \in \{1, 2, 3, 4\}$. Write down your calculation using (some of) the notation introduced above.

b) Your friend offers you the following bet: Before your friend tosses a coin 10 times (denote "heads" by 0 and "tails" by 1) you can either try to guess the first 6 coin tosses, or you can guess a sequence of 7 coin toss results where you think it will be a sub-sequence of the tosses (Example: if you guessed $0, 0, 1, 0, 1, 1, 1$ and the tosses come up $1, 0, \mathbf{0}, \mathbf{0}, \mathbf{1}, \mathbf{0}, \mathbf{1}, \mathbf{1}, \mathbf{1}, 0$ you win). If you win, you get DKK50, if you lose you have to pay DKK1. Describe a strategy and compute its winning probability. Is your strategy the best strategy? If so, why? Would you take the bet?

Exercise 1.2 Here is another problem about probability, to practice thinking about independence.

1. Here are three joint probability distributions p_i, $i = 1, 2, 3$, on $\{0,1\} \times \{0,1\}$ given as matrices, the upper left entry is $p_i(0,0)$, the upper right entry is $p_i(0,1)$ etc. Let $(X_i, Y_i) \leftarrow p_i$ be random variables with joint distribution p_i. Which of the pairs are independent?

$$p_1 : \begin{pmatrix} \frac{1}{2} & 0 \\ 0 & \frac{1}{2} \end{pmatrix}$$
$$p_2 : \begin{pmatrix} \frac{1}{3} & \frac{1}{3} \\ 0 & \frac{1}{3} \end{pmatrix}$$
$$p_3 : \begin{pmatrix} \frac{1}{4} & \frac{1}{4} \\ \frac{1}{4} & \frac{1}{4} \end{pmatrix}$$

Exercise 1.3 We can generalize the Caesar cipher from the lecture in the following straightforward way: consider the alphabet $\mathcal{X} = \{x_0, \ldots, x_{\ell-1}\}$ over which plaintext and ciphertext

space are defined. The key is a uniformly random number $k \in \{0, \ldots, \ell - 1\}$. The encryption of a string $m = x_{i_0} x_{i_1} \ldots x_{i_{M-1}}$ of letters in $\mathcal{X}$ replaces each character x_i by x_j with $j = i + k \bmod \ell$, i.e.

$$e_k(m) = x_{i_0+k \bmod \ell} x_{i_1+k \bmod \ell} \ldots x_{i_{M-1}+k \bmod \ell}.$$

Decryption is given by $d_k(c) = e_{-k \bmod \ell}(c)$.

Let $\mathcal{Y} = \{y_0, \ldots, y_{127}\}$ be the ASCII character table `https://simple.m.wikipedia.org/wiki/File:ASCII-Table-wide.svg`, so we have for example $y_0 =$ `NULL`, $y_{65} =$ `A` and $y_{49} =$ `1`. For any $a, b \in \{0, \ldots, 127\}$, define $\mathcal{X}_{a,b} = \{x_0, \ldots, x_{b-a}\}$ with $x_i = y_{i+a}$. For any such alphabet $\mathcal{X}_{a,b}$ we can consider the Caesar cipher on it. For some $a, b \in \{0, \ldots, 127\}$, the following is a ciphertext that was generated by encrypting a message string m consisting of English text with characters from $\mathcal{X}_{a,b}$ only, using the Caesar cipher on $\mathcal{X}_{a,b}$:

```
;\r6TXfTe~r[bjrTeXrlbhrWb\aZ2rHf\aZrUeb^XarVelcgb~r[h[2r;TccXafrgbrg[X
rUXfgrbYrhf!!!rAXkgrg\‘XrTebhaW~rgelr48F $%+r\ar:T_b\fr6bhagXer@bWXsss
```

Find the plaintext m, the values a and b, and the key!

Hints:

1. You might need to "escape" some characters when handing the ciphertext string to a program. The ciphertext as given above does not contain any escape sequences.
2. You can solve this problem by "brute force". In that case, the challenge is to find a way to automatically check whether a string of ASCII characters is English text. Another option is to look at the most frequent characters ("frequency analysis").
3. The plaintext is regular English text. In particular, it has spaces.

Exercise 1.4 Practice applying Kerckhoffs' principle. To do that, pick a physical security system (door lock, camera surveillance, boarding passes...) and analyze in howfar common instances of the system fulfil Kerckhoffs' principle.

Exercise 1.5 The last exercise is more for your fun: to read up a bit on the history of cryptography and how it sometimes fails.

Here are the three examples from the introductory lecture:

1. The Battle of Midway: `https://www.nsa.gov/portals/75/documents/about/cryptologic-heritage/historical-figures-publications/publications/wwii/battle-midway.pdf`
2. The history of the German ENIGMA: `https://www.dpma.de/english/our_office/publications/milestones/computerpioneers/enigma/index.html`
3. CCA security is not just a joke: `https://blog.cryptographyengineering.com/2016/03/21/attack-of-week-apple-imessage/`

There are of course many interesting websites and books about cryptography and its history. A somewhat outdated, but still interesting book is *The Codebreakers* by David Kahn.