Problem sheet 1 for Course 01410, 2023

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 Suppose for each of the following pairs of encryption and decryption algorithms, encryption expects 2 bit strings of length n as an input, a key $k \in \{0,1\}^n$ and a message $m \in \{0,1\}^n$. Which of them define a correct symmetric-key cryptosystem, i.e., for which of them is it true that $d_k(e_k(m)) = m$ for all $k, m \in \{0,1\}^n$?

a) Define
$$e_k(m) = m \oplus k \quad \text{and} \quad d_k(c) = c \oplus k,$$
where $\oplus$ denotes bit-wise XOR.

b) Let $\text{num}(s)$ be the integer obtained by regarding the string s as a binary integer, and for some integer $N \leq 2^n - 1$, let $\text{string}_n(N)$ be the bitstring of length n such that $\text{num}(\text{string}_n(N)) = N$. Define

Define
$$e_k(m) = \text{num}(m) \cdot \text{num}(k)$$
and
$$d_k(c) = \text{string}_n\left(\frac{c}{\text{num}(k)}\right).$$

c) Define
$$e_k(m) = \text{num}(k) + \text{num}(m) \bmod 2^n$$
and
$$d_k(c) = \text{string}_n(c - \text{num}(k) \bmod 2^n).$$
Here, $a \bmod b$ is the remainder when dividing an integer a by an integer b.

d) Define $e_k(m) = m_{[1,N-2]}$ and $d_k(c) = c \| 0$, where $s_{[a,b]}$ denotes the substring of s from bit number a to bit number b, both included, and $s_1 \| s_2$ denotes the concatenation of s_1 and s_2.

Exercise 1.2 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 $x \in V$ and
$$\sum_{x \in V} D(x) = 1.$$
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 dice. 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 1.3 The Caesar cipher with alphabet $\mathcal{X} = \{x_0, \ldots, x_{\ell-1}\}$ is the following encryption scheme. The key is a uniformly random number $k \in \{0, \ldots, \ell - 1\}$. The encryption of a string $s = x_{i_0} x_{i_1} \ldots x_{i_{M-1}}$ of letters in $\mathcal{X}$ replaces each character x_i by x_j with $j = i + k \bmod \ell$, i.e.

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

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

Let $\mathcal{Y} = \{y_0, \ldots, y_{127}\}$ be the ASCII character table, so we have for example $y_0 = \texttt{NULL}$, $y_{65} = \texttt{a}$ and $y_{49} = \texttt{1}$. 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.