

Exercise Sheet 1

Cryptography and Security 2022

These exercises are based on a previous instance of the prerequisites-test “Homework 1”. The original test contained only questions marked with ►; the non-marked questions were added to help you. The “Extra hints” were also *not* included in the original test.

Exercise 1 Element order

This is an example of an exercise from group theory. We let G be a finite multiplicative group.

1. Given an element $a \in G$, what is the definition of its inverse a^{-1} ?
2. What is the definition of *order* of an element $a \in G$?
- 3 Show that in *any* finite multiplicative group G , for all $a \in G$, a and its inverse, a^{-1} , have the same order.

Exercise 2 Algebra

This is an example exercise from algebra; it shows how knowing *how to apply* the correct theorem can simplify our lives.

1. What does the Little Fermat Theorem say?
- 2 Compute $\sum_{i=1}^{100} i^6 \bmod 7$. HINT: Look for a useful theorem for computing $i^6 \bmod 7$.

Exercise 3 Extended Euclidean Algorithm

Practice makes perfect particularly applies to this algorithm.

Given the following equation:

$$1081x + 299y = 23$$

Find the set of (x, y) solutions.

Exercise 4 Random variables

This is an exercise for basic probability theory. We have n independent random variables $X_1, \dots, X_n$ defined as

$$X_i := \begin{cases} 1 & \text{with probability } p \\ i & \text{with probability } 1 - p \end{cases}$$

- 1 Compute $E[\sum_{i=1}^n i \cdot X_i]$.
- 2 Assume $p = \frac{1}{2}$. Compute $\text{Var}[i \cdot X_i]$.

Exercise 5 Expected complexity

We investigate the complexity of a *simple* randomized algorithm in this exercise. Let X be a die and let $x \leftarrow X$ denote rolling the die and obtaining number $x \in \{1, 2, 3, 4, 5, 6\}$. We execute the following algorithm:

```
1:  $N = 0$ 
2: repeat
3:    $x \leftarrow X$ 
4:   if  $x \leq 2$  then
5:      $N = N + 2$ 
6:   else if  $x \leq 4$  then
7:      $N = N + 1$ 
8:   end if
9: until  $x \geq 5$ 
```

1. What is the expected number of iterations of the repeat-until loop?
2. Given that the algorithm terminates in the r -th iteration, what is the expected value of N ?

Note: Every new die-roll is independent! **Extra hint:** If there is a known probability distribution that matches the variable we study, it can provide useful answers.