

## MODERN CRYPTOGRAPHY

Bachelor Computer Science, University of Amsterdam, 2017/18

TEACHER: Christian Schaffner, TA: Jan Czajkowski, Chris Majenz

# Problem set x2

We will work on the following exercises together during the work sessions on Tuesday and Friday.

The last questions are marked as homework exercises. Your homework must be handed in within one week **electronically via Canvas before Thursday, 14 September 2017, 20:00h**. This deadline is strict and late submissions are graded with a 0. At the end of the course, the lowest of all the homework grades will be dropped.

You are strongly encouraged to work together on the exercises, including the homework. However, after this discussion phase, you have to write down and submit your own individual solution.

## Problem 1: Probability theory and Bayes' rule

Let  $E_1$  and  $E_2$  be probability events. Then,  $E_1 \wedge E_2$  denotes their conjunction, i.e.  $E_1 \wedge E_2$  is the event that *both*  $E_1$  and  $E_2$  occur. The *conditional probability of  $E_1$  given  $E_2$* , denoted  $\Pr[E_1|E_2]$  is defined as

$$\Pr[E_1|E_2] := \frac{\Pr[E_1 \wedge E_2]}{\Pr[E_2]}$$

as long as  $\Pr[E_2] \neq 0$ .

- (a) Let  $E_1$  and  $E_2$  be probability events with  $\Pr[E_2] \neq 0$ . Using the definitions above, prove what is known as *Bayes' rule*:

$$\Pr[E_1|E_2] = \frac{\Pr[E_1] \cdot \Pr[E_2|E_1]}{\Pr[E_2]}.$$

- (b) Let the probability that a news article contains the word *president* be 20%. The probability that it contains the word *president* if it already contains the word *Trump* is 35%. The probability that it contains the word *Trump* is 10%. Under these assumptions, what is the probability that a news article contains the word *Trump* if it already contains the word *president*?

- (c) Let the probability that a certain cryptographic protocol is *secure* and *efficient* be 10%. The probability that it is *not secure* if it is *efficient* is 80%. What is the probability that

1. the protocol is *secure* if it is *efficient*?
2. the protocol is *efficient*?

## Problem 2: Perfect security

Archaeologists found the following encryption table — unfortunately it is not complete.

|   | > | ∨ | < | ∧ |
|---|---|---|---|---|
| • |   |   | < | ∧ |
| ↔ | < |   | > |   |
| ⊙ | ∧ | > |   |   |
| ⊖ |   |   |   |   |

On another papyrus it is explained that this encryption was used during war. The movements “left”, “right”, “attack” and “withdrawal” were represented by  $\mathcal{M} = \{<, >, \wedge, \vee\}$ . The keyspace was  $\mathcal{K} = \{\bullet, \leftrightarrow, \odot, \ominus\}$ . Ciphertext and plaintext used the same alphabet, i.e.  $\mathcal{C} = \mathcal{M}$ .

The key was picked by tossing a coin twice. For every transmission a new key was used.

- (a) Complete the table to form a perfectly secure encryption scheme.
- (b) When using the one-time pad with the key  $k = 0^\ell$ , we have that  $\text{Enc}_k(m) = k \oplus m = m$  and the message is sent in the clear! It has therefore been suggested to modify the one-time pad by only encrypting with  $k \neq 0^\ell$  (i.e., to have Gen choose  $k$  uniformly from the set of *nonzero* keys of length  $\ell$ ). Is this modified scheme still perfectly secret? Explain.