Problem Set 2

We will work on the following exercises together during the work session on Friday, 8 Sep 2017.

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 *effficient* is 80%. What is the probability that

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

Problem 2: Shift cipher is not perfectly secure

Let us consider the shift cipher with the following message distribution: $\Pr[M = \texttt{ik}] = 0.1, \Pr[M = \texttt{op}] = 0.3, \Pr[M = \texttt{de}] = 0.6$.

(a) Calculate the probability $\Pr[M = \texttt{ik} \mid C = \texttt{ab}]$ that the message `ik` was encrypted when ciphertext `ab` is observed.

(b) Calculate the probability $\Pr[M = \texttt{op} \mid C = \texttt{ab}]$ that the message `op` was encrypted when ciphertext `ab` is observed.

(c) Conclude that the shift cipher is not perfectly secure.

Problem 3: Perfect security

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

	$>$	$\vee$	$<$	$\wedge$
$\bullet$			$<$	$\wedge$
$\leftrightarrows$	$<$		$>$	
$\circlearrowleft$	$\wedge$	$>$		
$\circlearrowright$				

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 $\mathcal{K} = \{\bullet, \leftrightarrows, \circlearrowleft, \circlearrowright\}$. 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.

Complete the table to form a perfectly secure encryption scheme.

Problem 4: Message in the clear

When using the one-time pad with the key $k = 0^\ell$, we have that $\mathsf{Enc}_k(m) = k \oplus m = m$ 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 ℓ). Is this modified scheme still perfectly secret? Explain.