Modern Cryptography
Bachelor Computer Science, University of Amsterdam, 2017/18
teacher: Christian Schaffner, TA: Jan Czajkowski, Christian Majenz

Problem Set 3

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

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.

The problems marked with ★ are more mathematical bonus problems. These bonus problems are optional and will not be part of the material you have to master for the final exam.

Problem 1: Insecurity of Multi-Time Pad

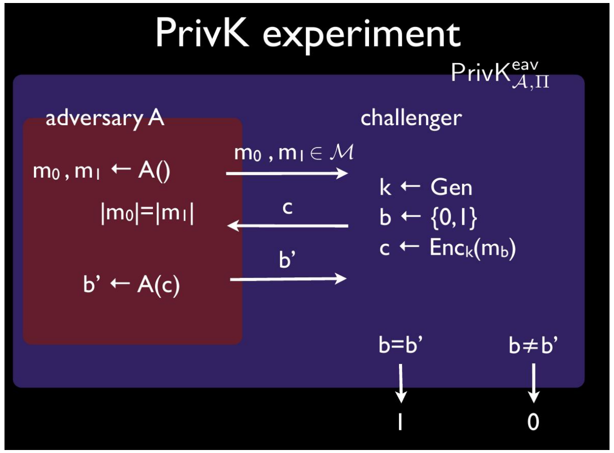
Two ASCII messages containing English letters and spaces only are encrypted using the one-time pad and the same key. The 10th byte of the first ciphertext is observed to be `0xB7` and the 10th byte of the second ciphertext is observed to be `0xE7`. Let m_1 (resp., m_2) denote the 10th ASCII character in the first (resp., second) message. What is the most you can conclude about m_1 and m_2?

Problem 2: The $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ experiment (see Figure 1)

For each of the following scenarios, give the maximal value of $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1]$ and explain how it can be achieved.

(a) Let Π be the shift cipher, and let us consider an adversary $\mathcal{A}$ that submits $m_0 = \texttt{a}$ and $m_1 = \texttt{a}$.

(b) Let Π be the shift cipher, and let us consider an adversary $\mathcal{A}$ that submits $m_0 = \texttt{a}$ and $m_1 = \texttt{b}$.



PrivK experiment

$\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$

adversary A

challenger

$m_0, m_1 \leftarrow A()$

$|m_0|=|m_1|$

$m_0, m_1 \in \mathcal{M}$

$k \leftarrow \mathsf{Gen}$

$b \leftarrow \{0,1\}$

$c \leftarrow \mathsf{Enc}_k(m_b)$

c

b'

$b' \leftarrow A(c)$

$b=b' \rightarrow 1$

$b\neq b' \rightarrow 0$

Figure 1: The $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ experiment

(c) Let Π be the shift cipher, and let us consider an adversary $\mathcal{A}$ that submits $m_0 = \texttt{aa}$ and $m_1 = \texttt{bb}$.

(d) Let Π be the shift cipher, and let us consider an adversary $\mathcal{A}$ that submits $m_0 = \texttt{aa}$ and $m_1 = \texttt{ab}$.

(e) Let Π be the one-time-pad encryption, and let us consider an adversary $\mathcal{A}$ that submits $m_0 = \texttt{aaa}$ and $m_1 = \texttt{abc}$.

(f) Let Π be the monoalphabetic substitution cipher. Give an adversary $\mathcal{A}$ that manages to win the $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$ experiment all the time, i.e. such that $\Pr[\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi} = 1] = 1$.

Problem 3: Negligible functions

Recall Definition 3.4: A function $f : \mathbb{Z}^+ \to \mathbb{R}^+$ is called *negligible* if for every positive polynomial $p(n)$ there exists $N \in \mathbb{Z}^+$ such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.

(a) Example 3.5 states that $f(n) = 2^{-\sqrt{n}}$ is negligible. For the polynomial $p(n) = 16n^4$, give a possible N as in the definition above, i.e. such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.

(b) Example 3.5 states that $f(n) = n^{-\log n}$ is negligible. For the polynomial $p(n) = 16n^4$, give a possible N as in the definition above, i.e. such that for all integers $n > N$, it holds that $f(n) < \frac{1}{p(n)}$.

★ Let negl_1 and negl_2 be negligible functions. Prove that the function negl_3 defined by $\mathsf{negl}_3(n) = \mathsf{negl}_1(n) + \mathsf{negl}_2(n)$ is negligible.

★ For any positive polynomial p, the function negl_4 defined by $\mathsf{negl}_4(n) = p(n) \cdot \mathsf{negl}_1(n)$ is negligible.

Problem 4: Exercise 3.2 from [KL]

Prove that Definition 3.8 cannot be satisfied if Π can encrypt arbitrary-length messages and the adversary is not restricted to output equal-length messages in experiment $\mathsf{PrivK}^{\mathsf{eav}}_{\mathcal{A},\Pi}$. **Hint:** Let $q(n)$ be a polynomial upper-bound on the length of the cipher-text when Π is used to encrypt a single bit. Then consider an adversary who outputs $m_0 \in \{0,1\}$ and a uniform $m_1 \in \{0,1\}^{q(n)+2}$.

Problem 5: Exercise 3.4 from [KL]

Prove the equivalence of Definition 3.8 and Definition 3.9 from the book [KL].