MODERN CRYPTOGRAPHY
Bachelor Computer Science, University of Amsterdam, 2017/18
TEACHER: Christian Schaffner, TA: Jan Czajkowski, Chris Majenz

Problem set 1

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

Your homework problems are very similar to Problems 4 and 5. Your homework must be handed in within one week **electronically via Canvas before Monday, 11 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 these problems as well as the homework. However, after this discussion phase, you have to write down and submit your own individual solutions.

The problems marked with $*$ are more challenging bonus problems, often referring to extra material covered only in the [KL] book (or elsewhere), but possibly not in the videos. These bonus problems are optional and will not be part of the material you have to master for the final exam.

Problem 1: Formal definitions

In the Katz-Lindell [KL] book, the *shift cipher* is informally described as follows: "Algorithm Gen outpus a uniform key $k \in \{0, 1, \ldots, 25\}$; algorithm Enc takes a key k and a plaintext and shifts each letter of the plaintext forward k positions (wrapping around at the end of the alphabet); and algorithm Dec takes a key k and a ciphertext and shifs every letter of the ciphertext backward k positions."

In a more formal mathematical language, we can define the shift cipher as follows: Let us identify numbers and English letters in the natural way ($a = 0, b = 1, c = 2$ etc.). Then, the message space $\mathcal{M}$ is any finite sequence $m = m_1 m_2 \cdots m_\ell$ where $m_i \in \{0, 1, \ldots, 25\}$.

$$\begin{aligned} \text{Gen} &: k \leftarrow \{0, 1, \ldots, 25\}\,, \\ \text{Enc}_k(m_1 m_2 \ldots m_\ell) &= c_1 c_2 \ldots c_\ell \text{ where } c_i = [(m_i + k) \mod 26]\,, \\ \text{Dec}_k(c_1 c_2 \ldots c_\ell) &= m_1 m_2 \ldots m_\ell \text{ where } m_i = [(c_i - k) \mod 26]\,. \end{aligned}$$

Provide formal definitions for Gen, Enc, Dec for

(a) the mono-alphabetic substition cipher,

(b) the Vigenère cipher.

Problem 2: Chosen-plaintext attacks

Let us consider the scenario of *chosen-plaintext attacks*. In this scenario, an attacker has the ability to obtain plaintext/ciphertext pairs (under the same unknown key) for plaintexts of its choice. For example, for the case of a shift cipher, the attacker might ask for encryptions of messages `foo` and `bar` and obtains (plaintext,ciphertext) pairs `(foo,oxx)` and `(bar,kja)`.

Show that shift, mono-alphabetic substition and Vigenère ciphers are all trivial to break using a chosen-plaintext attack. How much chosen plaintext is required to recover the key for each of the ciphers?

Problem 3: Birthday paradox

This exercise deals with some basic probability as described in Appendix A.3 of the book [KL]. Compute the probability that any two students in the room have the same birthday (ignoring the birth year).

Problem 4: Asymptotic growth rate

Let ε and c be arbitrary constants such that $0 < \varepsilon < 1 < c$. Order the following terms in increasing order of their asymptotic growth rates.

$$n^n \quad \exp(\sqrt{n}) \quad 1 \quad \log\log n \quad c^{c^n} \quad n^c \quad n^\varepsilon \quad n^{\log n} \quad \log n \quad c^n$$

Hint: In some cases, it might help to express two terms you want to compare in the form $e^{\cdots}$ and then compare their exponents.

Problem 5: Logical Contrapositives

In logic, contraposition is an inference that says that a conditional statement $A \Rightarrow B$ is logically equivalent to its contrapositive $\neg B \Rightarrow \neg A$. For instance, the proposition "If the weather is good, then I'm biking

to work." can be restated as "If I'm not biking to work, then the weather is bad."

State the contrapositive of the following statements:

(a) If it rains, the trees get wet.

(b) If the car drives, its fuel tank is not empty.

(c) If p is a prime, then p = 2 or p is odd.

(d) If assumption X holds, protocol Y is secure.

(e) The RSA protocol is insecure, if you can factorize efficiently.

Problem 6: ∗ Breaking the Vigenère cipher

See Canvas for the bonus material.