Cryptology I (spring 2014)	Prof. Dr. Dominique Unruh
Exercise Sheet 1	
Out: Feb 18, 2014	Due: March 3, 2014

You will need 50% of all homework points to qualify for the exam. (That is, if you get at least 50%, your final grade will be the exam grade. And if you do not get 50%, you do not pass the course.)

You may hand in your solutions in person or by email. If you submit by email, either scan a handwritten solution or typeset your solution readably. I do not consider ASCII formulas readable.

When submitting, indicate your name and your matriculation number. On your first submission, please also indicate a password, this password will be needed for accessing the solutions and your points online.

Problem 1: Enigma

The Enigma machine is a symmetric electromechanical encryption device which was used by the German army during World War II. The secret key consists of the initial position of three rotors (each rotor has 26 different positions), and an electric connection which represents a permutation on $\{a, b, c, \dots, z\}$ with 14 fixed points and 6 non-overlapping exchanges of two characters. For example,

$$[b \leftrightarrow t, e \leftrightarrow q, g \leftrightarrow z, h \leftrightarrow i, k \leftrightarrow p, m \leftrightarrow s]$$

lets $a, c, d, f, j, \ell, n, o, r, u, v, w, x, y$ unchanged, maps b to t and t to b, e to q and q to e, etc. A toy Enigma machine (limited to 6 letters) is represented in Figure 1.

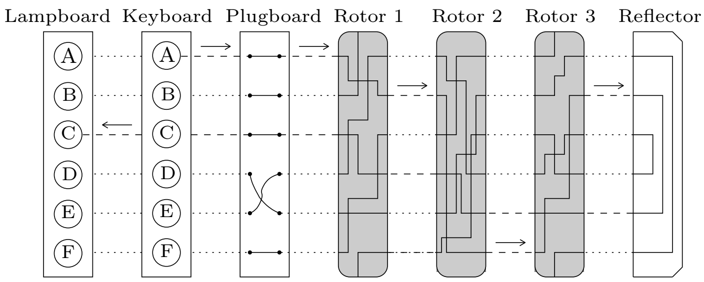

Figure 1: An Enigma machine limited to 6 letters

1. How many different keys does the Enigma machine have?

2. A terrorist attack is being prepared against Estonia. The potential targets are Narva, Parnu, Saaremaa, Tallinn, Tartu and Viljandi (in alphabetical order). The police managed to intercept a ciphertext of the chosen location for the attack: "FAVXCHFATZ". From a trusted source we know that the plaintext consists of the name of the target, filled up with trailing X's to a length of ten characters. Where will the attack be perpetrated? Justify your answer.

Problem 2: One-time-pad

(a) In a brute force attack, one tries every possible key k and tries to decrypt the ciphertext c using k. When decrypting c using k yields a valid plaintext (e.g., an English sentence), one has found the key.

Given enough time, one can also enumerate all possible keys for the one-time pad. Thus, given unlimited computational power, one can apply the brute-force attack to the one-time pad. One the other hand, we have proven that the one-time pad has perfect secrecy. Thus is should not be possible to break the one-time pad.

Explain why a brute-force attack fails on the one-time pad (even if one has unlimited time).

(b) Write a program that achieves the following: It takes as input two ciphertexts c_1 and c_2 of the same length. Both are expected to be the encryption of a single word m_1, m_2 using the one-time-pad. To produce the ciphertexts, the *same* key has been used. The program then finds m_1 and m_2.

Consider the following ciphertexts: c_1 = `4ADD55BA941FE954`, c_2 = `5AC643BE8504E35E` (eight bytes each, presented in hex). Figure out the plaintexts using your program.

Note: On many Linux systems, you find a wordlist in /usr/share/dict/words. Please submit a printout of your source code and the plaintexts.

(c) **[Bonus problem.]** Write a program that does the same as in (b), except that m_1, m_2 are now English sentences.

This is much more difficult (I have not done it myself), but if you enjoy the challenge, you can do it.

No solution will be provided for this problem unless a student writes one.

Problem 3: Perfect secrecy

Show that there is no encryption scheme that has perfect secrecy and allows us to reuse the key. More precisely, show that there is no encryption scheme E that satisfies the following definition (and that can be decrypted):

Definition 1 (Perfect secrecy with key reuse) *Let K be the set of keys, let M be the set of messages, and let E be the encryption algorithm (possibly randomized) of an encryption scheme. We say the encryption scheme has* perfect secrecy with key reuse *iff for all n, and all $m_0^{(1)}, \dots, m_0^{(n)}, m_1^{(1)}, \dots, m_1^{(n)} \in M$ and for all $c_1, \dots, c_n$, we have that*

$$\begin{aligned} &\Pr[(c_1, \dots, c_n) = (c'_1, \dots, c'_n) : k \xleftarrow{\$} K, c'_1 \leftarrow E(k, m_0^{(1)}), \dots, c'_n \leftarrow E(k, m_0^{(n)})] \\ =&\Pr[(c_1, \dots, c_n) = (c'_1, \dots, c'_n) : k \xleftarrow{\$} K, c'_1 \leftarrow E(k, m_1^{(1)}), \dots, c'_n \leftarrow E(k, m_1^{(n)})] \end{aligned}$$

Hint: If you have an encryption scheme E with perfect secrecy with key reuse, first construct from it a scheme E' with perfect secrecy that has messages longer than keys. (Show that it indeed has perfect secrecy.) Then use Theorem 1 in the lecture notes.