Program Design & Data Structures (Course 1DL201)
Uppsala University Autumn 2013/Spring 2014
Homework Assignment 3: Cryptography: **Clarifications**

Prepared by Dave Clarke

January 28, 2014

Example

There are two small typos in the examples in section **Some Test Cases**. They should read

```
CLEPK HHNIY CFPWH CDFEH
GOINB NYXEW BLKCB ZNGIH
```

You'll see why when you have your solution.

Variant for `keygen`

On first inspection, the variant for the function `keygen` appears to be straightforward. But due to the fact that jokers need to be ignored, it turns out to by much much more complicated. For the purposes of this assignment, ignore this complication and give the obvious variant.

If you understand the reason I'm alluding to, you may include an explanation in your documentation.

Complexity Analysis

The assignment description states that you need to consider the number of cards as not being fixed when performing the complexity analysis of the various functions. A consequence of this is that the complexity of some functions will be defined in terms of two variables, the size of the input and the number of cards. This goes beyond what you have learned in class.

Here is how the complexity should be addressed.

- if the function deals exclusively with cards, then consider its complexity in terms of a variable number of cards.
- if the function deals exclusively with input being encrypted (or something proportional to the size of the input), then consider its complexity in terms of the size of the input.
- if the function deals with both input and cards, consider the number of cards to be fixed.

State clearly in your analysis which of these assumptions is being made.

If you would like an additional challenge, consider both the size of the input and the number of cards to be variable.