Exercises Classical Cryptography 1a

crypto@os3.nl

Tuesday, February 7, 2023

(version 22.3, 2023/02/01 10:16:27 UTC)

Hints are given in Caesar encryption to prevent accidental reading.

Problem 1: **Slitherlink**

(a) Solve a few easy "Slitherlink" puzzles.
A nice site for this is `https://brainbashers.com/`.
In particular `https://brainbashers.com/slitherlink.asp`.

(b) What are some patterns that you find when solving those puzzles?
Hint 1: Orrn dw d chur qhaw wr d wkuhh.
Hint 2: Orrn iru d chur gldjrqdoob dgmdfhqw wr d wkuhh.
Hint 3: Orrn dw d wkuhh qhaw wr d wkuhh.
Hint 4: Orrn iru d wkuhh gldjrqdoob dgmdfhqw wr d wkuhh.

(c) Try some more Japanese puzzles.

Problem 2: **Ruby as a calculator**

(a) Install Ruby (or Python or a scripting language of your own choice) and check that it works.

(b) Check that the interactive interpreter `irb` works.

(c) Calculate some big numbers like 2^{100000} using `irb`.

Problem 3: **Simple Ruby string and character handling**

(a) What is the difference between `puts` and `print`?
Hint 1: Orrn dw wkh hqg ri olqh ehkdylrxu.
Hint 2: Zkdw kdsshqv li wkhuh lv douhdgb dq HRO lq wkh dujxphqw?

(b) Find out what the method `ord` does on characters, strings and numbers.

(c) Find out what the method `chr` does on numbers, characters and strings.

(d) Can you also use the methods `ord` and `chr` for unicode codepoints?
Hint: Pdnh vxuh brx xvh wkh fruuhfw hqfrglqj iru wkh xqlfrgh vwulqj dw kdqg.

Problem 4: **Simple Ruby alphabet generation by loop and conditional**

(a) Find out how to print the alphabet, alternating between upper and lower case.
Hint: Xvh wkh "hdfk" phwkrg dv orrs dqg wkh "li wkhq hovh hqg" wr dowhuqdwh.

Problem 5: **Basic concepts**

(a) Why does encryption have to be injective (one-to-one)?
Hint: Wklqn derxw wkh qhfhvvlwb ri d srvvleoh ghfubswlrq.

(b) Does encryption have to be surjective (onto the domain of ciphertexts)?
Hint: Pdnh wkh vhw ri flskhuwhawv eljjhu wkdq wkh vhw ri sodlqwhawv ru xvh dq lqilqlwh vhw.

(c) What simple "encryption" can you think of that is injective but not surjective?
Hint: Wkh hqfubswlrq qhhgv qrw eh vhfxuh.