Exercises Classical Cryptography 1b

crypto@os3.nl

Friday, February 10, 2023

(version 22.5, 2023/02/08 09:49:37 UTC)

Problem 1: **Caesar cipher**

(a) Encrypt a message using a Caesar (additive) cipher and let a colleague student solve it.

(b) Write a little Ruby script to aid in solving additive ciphers.

Problem 2: **Alphabet creation**

(a) What is the cipher alphabet based on the keyphrase `ALPHABET CREATION`?

(b) Write a little Ruby script to aid in creating alphabets from keywords.

Hint: Frqfdwhqdwh d frpsohwh doskdehw wr wkh nhbzrug dqg xvh wkh phwkrgv `fkduv`, `xqlt` dqg `mrlq`.

Problem 3: **Decimation**

(a) What is the decimation (multiplicative cipher) with key 11?

Differentiate between modern and legacy encoding.

(b) Write a little Ruby script to decimate the alphabet.

Problem 4: **Extended Euclidean algorithm**

(a) Use the extended Euclidean algorithm to find p and q such that $p \cdot 144 + q \cdot 55 = 1$. Bonus question: what is special about 55 and 144?

Hint: Edeb udeelwv

(b) Use Ruby to brute force a solution to this problem.

Hint: Orrn dw pxowlsohv ri 55 lq vxffhvvlrq xqwlo brx ilqg rqh zklfk lv rqh prgxor 144.

Problem 5: **Playfair cipher**

(a) Encrypt a message using a Playfair cipher (without a keyword) and let a colleague student solve it.

Problem 6: **Hill cipher**

This exercise uses the modern encoding.

(a) Encrypt the message `FINALLY READY` using the example Hill cipher in the slides.

(b) Decrypt the message `HHJAAHGF` using the example Hill cipher in the slides.