Exercises Classical Cryptography 2b

crypto@os3.nl

Friday, February 17, 2023

(version 22.4, 2023/02/08 10:20:59 UTC)

Problem 1: **"Easy" route transpositions**

(a) Solve the route transpositions from Prac 2.2.1 and 2.2.2.

Hints for 2.2.1:

1. Wkh sodlqwhaw zdv zulwwhq lq urz eb urz.
2. Wkh flskhuwhaw zdv uhdg rxw dorqj gldjrqdov.
3. Gldjrqdov vwduw lq wkh qruwkzhvw.
4. Gldjrqdov dowhuqdwh lq gluhfwlrq.
5. Wkh uhfwdqjoh kdv hljkw urzv dqg qlqh froxpqv.

Hints for 2.2.2:

1. Wkh sodlqwhaw zdv zulwwhq lq urz eb urz.
2. Wkh flskhuwhaw zdv uhdg rxw yhuwlfdoob.
3. Dowhuqdwh jrlqj xs dqg grzq.
4. Xvh d vhyhq eb vhyhq vtxduh.

Problem 2: **Harder route transposition**

(a) Solve the route transposition from Prac 2.2.3.

Hints:

1. Wklv wlph wkh **flskhuwhaw zdv uhdg** iurp d uhfwdqjxodu eorfn, urz eb urz.
2. Zulwh wkh flskhuwhaw lqvlgh d uhfwdqjoh ri 10 urzv dqg 6 froxpqv.
3. Wkh mixfkqbuq zxk yb uhdg rxw dorqj gldjrqdov.
4. Gldjrqdov vwduw lq wkh qruwkhdvw.

Problem 3: **Exchanging rows and columns with Ruby**

This exercise prepares some tools that come in handy for the next exercise.

(a) Write a Ruby script to automate exchanging rows and columns of a block of text.

(b) Write a Ruby script to implement a simple columnar transposition.

Problem 4: **Transpositions with common endings**

(a) Solve the "partly filled" transpositions of Prac 2.1. First read the introduction given in "Practicumboek Cryptografie".

Hints:

1. Wkh nhbzrug lv wkluwhhq fkdudfwhuv orqj.
2. Wkh iluvw whaw kdv rqh orqj froxpq dqg wzhoyh vkruw rqhv.
3. Wkh vhfrqg whaw kdv wkuhh orqj froxpqv dqg whq vkruw rqhv.
4. Wkh sdwwhuq iru wkh iluvw whaw lv vvvvvvvovvvvv.
5. Wkh sdwwhuq iru wkh vhfrqg whaw lv vvovvvvovovvv.