Exercises Classical Cryptography 3b

crypto@os3.nl

Friday, February 24, 2023

(version 22.5, 2023/02/08 11:06:22 UTC)

Problem 1: **ADFGVX decryption**

Decrypt the following ADFGVX encrypted message

AGGAV	AXGDA	DFGGA	FXFFV
VXXFG	XXVGF	VAAXX	ADAXG
FFFFV	D		

The keyword is GANDHI and the 6-by-6 encryption table is

	A	D	F	G	V	X
A	b	5	x	q	j	c
D	6	y	r	k	d	7
F	z	s	l	e	8	1
G	t	m	f	9	2	u
V	n	g	0	3	v	o
X	h	a	4	w	p	i

Problem 2: **Kerckhoffs super(im)position**

Solve the Kerckhoffs superimposition (practicumboek hoofdstuk 7).

Hints:

1. Wkh vhfrqg ohwwhu (zlwk d vfruh ri 5) lv wkh fruuhfw rqh.
2. Wkh iluvw ohwwhu lv rqh ri wkh rswlrqv zlwk d vfruh ri 4: K, Q, R ru V. Wub wkhp doo wr ilqg wkh uhdo rqh.

Problem 3: **Repetitions "out of phase"**

(a) Given a repeating-key Vigenère, can you think of a method to find repetitions in the plaintext, even if they are not aligned/superimposed?

Hints:

1. Orrn zkdw kdsshqv li brx kdyh d uhshwlwlrq wkdw lv wzlfh dv orqj dv wkh nhbzrug ohqjwk, exw rxw ri skdvh, dqg brx vxewudfw wkh fubswrjudp lwvhoi iurp wkh fubswrjudp, vkliwhg eb rqh nhbzrug ohqjwk.
2. HHQYR RUEHH OGYDQ HHQKH UKDOL QJELM YRRUE HHOGY DQGLW
   RSWHO RSWHO RSWHO RSWHO RSWHO RSWHO RSWHO RSWHO RSWHO
   == +
3. FJXLS CVRHB VWJOS IZWSW EYXPX MGKYP VWHKJ RFZPH
   VWJCC FJXLS CVRHB VWJOS IZWSW EYXPX MGKYP VWHKJ
   == -

(b) *This exercise is only for the diehards*

Solve the Midway encicode. Use the method from part (a). For more explanation, see "practicumboek hoofdstuk 5".