Assignment 0x03

Frank Kaiser – 1742945, Jan Martin – 1796943

December 9, 2017

Contents

1 A Ciphertext Only Attack on the Vigenre Cipher

First we used the Kaisiki-Test do determine the Key length:

letters	distance	prime factors
KC:	41	41
CM:	17	17
SY:	66	2 * 3 * 11
XOC:	140	2 * 2 * 5 * 7
OC:	20	2 * 2 * 5
GK:	12	2 * 2 * 3
JO:	12	2 * 2 * 3
JO:	42	2 * 3 * 7
JO:	16	2 * 2 * 2 * 2
JO:	74	2 * 37
JO:	136	2*2*2*17
LZKMP	520	2*2*2*5*13
LZKMP	178	2 * 89
LZKMP	366	2*3*61
LKZMP	1448	2*2*2*181

Because of the overwhelming amount of twos we decided to try 4 as key length. Then we did a frequency analysis on the partitions created by `https://cryptotools.psi.h4q.it/vigenere.html`. The most frequent letters for each partition were:

1) P, E, L, Z, S
2) S, H, B, C, O
3) G, V, Q, C, J, K
4) O, D, K, Y, C

After trying a little bit around, we discovered that the word L O C K is readable when taking one character from every partition. We tried it out and had success. The key for the text is LOCK and Alice finds a golden key!

2 Loss of Confidentiality in Counter Mode with Repeated Nonce

Key: c9 3e 1e ba b7 3f c3 3c 05 a6 75 35 41 bd 34 5a e4 57 d1 a3 74 16 43 4e 02 3a 0b 0e d2 2b 9e 2c 32 c5 2a bb 75 5c 0b bf 54 29 2f 8e 63 53 b7 f3 45 b3 a5 c4 ee dd 4c 9a 03 da 4e 2b 2e 15 6b 80 7b ca 28 4c 9b 16 24 21 9b 1e 94 8f 51 59 d6 fb 5f 31 cb 06 f8 cc