MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Modulo Arithmetic with n – Appendix 2

Authors: Tanja Lange, Andreas Gruener, Bernhard Esslinger

August 2011

Hints for the solution of the challenge

If you need any hints, you can find here four spoilers that help to solve the challenge:

Hint 1:
Plaintext can be derived from ciphertext through converting the encryption equation to x and replacing numbers with appropriate letters after the calculation of x.

A	B	$\cdots$	Y	Z
0	1	$\cdots$	24	25

Hints for the solution of the challenge

Hint 2:
During the conversion of the encryption equation ($y = a \cdot x + b \mod 26$), a division appears. The result of a division with a number equals a multiplication with the appropriate inverse element of this number.

Hints for the solution of the challenge

Hint 3:
A multiplicative inverse of an element, within a finite field, is computable with the extended Euclidean algorithm.

Hints for the solution of the challenge

Hint 4:

The following steps are necessary to convert the encryption equation:

1. $y = 17 \cdot x + 7 \bmod 26$
2. $17 \cdot x = y - 7 \bmod 26$
3. $x = (y - 7)/17 \bmod 26$
4. $x = y/17 - 7/17 \bmod 26$
   ($23 = 17^{-1} \bmod 26$, because $23 \cdot 17 = 1 \bmod 26$)
5. $x = 23 \cdot y - 7 \cdot 23 \bmod 26$
6. $x = 23 \cdot y + 21 \bmod 26$

The extended Euclidean algorithm has to be executed to accomplish the transition from step 4 to step 5.

P.S.: If there is only a small alphabet it is possible to generate the complete mapping table with $y = a \cdot x + b \bmod 26$ and to create a correlation comparable to a cipher disc.

This is a part of the mapping table for $a = 17$ and $b = 7$:

X	A	$\cdots$	D	$\cdots$	Z
	0	$\cdots$	3	$\cdots$	25
Y	7	$\cdots$	6	$\cdots$	$\cdots$
	H	$\cdots$	G	$\cdots$	$\cdots$

Cipher Disc [1]

References

[1] Mills, Austin: Cipher Disc. URL: http://www.flickr.com/photos/austinmills/13430514/sizes/m/in/photostream/