MysteryTwister C3
THE CRYPTO CHALLENGE CONTEST

Affine Codes / Modulo Arithmetic with n / Extended Euclid

Authors: Tanja Lange, Andreas Gruener, Bernhard Esslinger

August 2011

Janina and Carolin are 14 year old girls, who attend the high school next door. They love to write letters to each other to talk about the important things in life, for example boys and parties to come. Once, Carolin's mom got a letter by accident and read the content. As a result Carolin's parents asked many unpleasant questions. Now the two girls are thinking about a solution to make this awkward situation never happen again. They ask their best friend Tom for a hint as he regularly reads "The Three Investigators" and is very keen on cryptography in his spare time. The affine cipher comes to Tom's mind. It describes a possibility to encrypt single letters to obfuscate the meaning of a text.

Tom's idea in detail:

1. The Latin alphabet consists of 26 letters.
2. Each plaintext letter is mapped by a rule to a ciphertext letter. For that, each letter is represented as a number within {0,1,2,3, ... 23,24,25}. The rule to encrypt a plaintext letter x to a ciphertext letter y is: $y = a \cdot x + b \bmod 26$
3. a, b are the parts of the secret key, which Carolin and Janina should not tell anybody.
4. The key consists of the following numbers: $a = 17$, $b = 7$

Tom makes a final rehearsal before he presents his proposal to Carolin and Janina. He encrypts a text and gets:

GNXB NBS XNUX FXWXNDX UHPWKNPWS

The plaintext letter D is represented by the value $x = 3$. Therefore y is calculated by $y = 17 \cdot 3 + 7 \bmod 26 = 58 \bmod 26 = 6$, representing G.

Now Tom realized, that he has not thought yet about the decryption of the message. He is short on time and overdue with his suggestion.

Support Tom by finding a way to decrypt the ciphertext. Reveal the meaning of the shown example and hand it in as solution. Please use only capital letters.

There is an additional ZIP file for this challenge with two appendices. Appendix 1 introduces in an easy-to-understand way to modulo arithmetic.

Appendix 2 contains four hints for solving the challenge.