MysteryTwister C3

THE CRYPTO CHALLENGE CONTEST

Factorization Cipher – Part 1

Author: Viktor Veselovsky

October 2011

The fundamental theorem of arithmetic (or the unique-prime-factorization theorem) states that any integer n, $n > 1$, can be written as a unique product of prime numbers.

In this challenge an unknown symmetric cipher based on this theorem has been used. This cipher is essentially a playful riddle instead of a serious cipher.

It is your task to find out how to perform the encryption and decryption of this cipher.

Examples

To find out how this method works, you got 7 pairs of plaintext-ciphertext (p_i - c_i) encrypted with this method:

p_1: CAR
c_1: 168919260200

p_2: A CAR
c_2: 402271083010688000

p_3: CAB
c_3: 48600

p_4: ART
c_4: 1638103129277324

p_5: I AM
c_5: 490303442632

p_6: ABBA
c_6: 235092492288

p_7: BEEF
c_7: 2359045149946171711556103

Plaintexts can only contain capital letters of the normal alphabet (26 letters, A-Z).

All spaces between words are removed before encryption.

Decrypted ciphertexts contain no spaces, hence after the decryption you have to add spaces at the appropriate positions in order to separate the words.

Assignment

To solve this challenge you only need a pen and paper but using a hand calculator or a computer algebra program may be helpful.

Find the English plaintext of the following ciphertext:

c: 32535610350861218929402373343432584856134615644613646196

When you enter the solution, please use capital letters and separate the words by spaces.

Hint

The cipher uses the uniqueness of factorization of integers to produce unique plaintext-ciphertext pairs. Please start by factoring the given number c (using e.g. SAGE, WolframAlpha or CrypTool).

The smallest prime numbers are always included as exponents.

If you intend to solve this challenge without the help of a computer, prepare for a "relatively long" long division. ;-)