

Bob realized a cipher machine for encoding integers from 0 to n-1 by 128-bit strings using the secret function Enc. He set n = 1060105447831. The cipher machine works as follows: it takes as input a pair of non-negative decimal integers x and d and returns

 $\operatorname{Enc}(x^d \mod n).$ 

Bob chose a secret number k from 0 to n-1 and asked Alice to guess it. Alice said that she can find k if Bob provides her with the cipher machine with an additional property. Namely, x can be also of the form "k", and then the cipher machine will return  $\operatorname{Enc}(k^d \mod n)$ . In particular, for the query "k, 1", the cipher machine returns

Enc(k) = 41b66519cf4356cbbb4e88a4336024da

(the result is in hexadecimal notation). Here it is the cipher machine!

Prove Alice is right and find k with as few requests to the cipher machine as possible!





nsucrypto.nsu.ru

Page 4 from 13

nsucrypto@nsu.ru