Heidi's Cryptographic Commerce
Heidi et son Commerce Cryptographique
Heidis kryptographisches Gewerbe

Robert R. Enderlein

Medium Task

Heidi lost her private key! She looked everywhere on her board computer, but apparently she hid her key so well that she can't find it anymore. Fortunately the computers of her friends are not as quick as hers, and so far she never used prime numbers that are larger than 2^{34}, and so she thinks you can help her read her messages despite the fact that she lost her key.

Can you write a decryption function that given just the ciphertext (E,F) and her public key (p,g,y) recovers the messages that were sent to her?

Note: there will be around hundred testcases in this sub-problem, and the primes p will vary between 3 and 2^{34}. Doing an exhaustive search of all possible values of x is going to be too slow.

Tâche Moyenne

Heidi a perdu sa clef privée! Elle a regardé partout sur son ordinateur de bord, mais apparemment elle a caché sa clef si bien qu'elle-même ne peut plus la trouver. Heureusement les ordinateurs de ses amis ne sont pas aussi puissants que le sien, et jusque là elle n'a jamais eu à utiliser des nombres premiers plus grands que 2^{34}. Ainsi, elle espère que vous pourrez l'aider à lire des messages même si sa clef a été perdue.

Pouvez-vous écrire une fonction de décryptage qui, étant donné uniquement le texte chiffré (E,F) et la clef publique (p,g,y), puisse retrouver le message envoyé à Heidi?

Remarquez: il y aura environ une centaine de cas de tests pour ce sous-problème, et les nombres premiers p varieront entre 3 et 2^{34}. Faire une recherche exhaustive pour toutes les valeurs possible de x sera trop lent.

Mittlere Aufgabe

Heidi hat ihren privaten Schlüssel vertan! Sie hat ihren gesamten Bordrechner durchforstet, aber scheinbar hat sie den Schlüssel so gut versteckt, dass auch sie selbst ihn nicht mehr wiederfindet. Zum Glück besitzen ihre Freunde weniger schnelle Rechner als Heidi, darum hat sie bisher keine Primzahlen über 2^{34} verwendet. Demnach ist Heidi zuversichtlich dass ihr die Nachrichten immer noch entziffern könnt.

Seid ihr tatsächlich in der Lage, eine Entschlüsselungsfunktion zu schreiben, welche ausschliesslich auf Basis des verschlüsselten Textes (E,F) und des öffentlichen Schlüssels die erhaltenen Nachrichten entziffert?

Bemerkung: Diese Aufgabe enthält etwa einhundert Testfälle, und die Primzahlen p varieren zwischen 3 und 2^{34}. Es ist zu langsam, einfach alle möglichen Werte für x auszuprobieren.