Zahlentheorie und Kryptologie, SS2014
M. Hortmann

Blatt 2

Aufgabe 1

Benutzen Sie die Pari-Funktionen random und nextprime, um folgende Frage zu beantworten:

Wie groß ist im Durchschnitt die Differenz zwischen einer 1024-Bit Zufallszahl und der nächsten Primzahl? (Machen Sie mindestens 1000 Versuche.)

Dieselbe Frage fur 2048 Bit.

Aufgabe 2

Im RSA-System hat jeder Teilnehmer zwei zufällige hinreichend große Primzahlen p, q so erzeugt, daß $e = 2^{16}+1$ teilerfremd zu $m=(p-1)(q-1)$ ist.

Man zeige, daß sich p,q aus dem Produkt $n=pq$ und m rekonstruieren lassen, und tue dies (mit Hilfe von Pari) für

n = 17962435528650376228925114174356054392430433237595618820413076826800906805485153422968667554747198029051225799342225373169838308361170491627978562510823249519344836936480459778809310375905798855926486678078896817818985279032839537194797591233312434100675572838723192873111630228963667180533229577492843926606596003841331383903550682085548379131262311483849069494618018925579939879652309176143960169092329647172928166650216984171957164742569919314678007829366917353577485610260279234855886050678712459674432083026516781016735106040395527062457378028532360277611920279945078914899527316677507909174510876733218883677 87

und

m = 17962435528650376228925114174356054392430433237595618820413076826800906805485153422968667554747198029051225799342225373169838308361170491627978562510823249519344836936480459778809310375905798855926486678078896817818985279032839537194797591233312434100675572838723192873111630228963667180533229577492843926605748334565830026229762117313805111029558635790112985187525291579385990855442787909912099610280364240156997189978768539387079028867303899717319010265496078736118455950091759112851219679121948774115034079079993970882681586685745250453929154909568798990141534341532626581008006728437785392136101426171437084834 56

Aufgabe 3

Finden Sie eine zufällige 4096-Bit-Primzahl r, so daß $q=2r+1$ und $p=2q+1$ Primzahlen sind. Benutzen Sie dabei nicht die Pari-Funktion isprime, sondern die Funktion ispseudoprime. Sie sollten Ihr Ergebnis dann aber mittels isprime überprüfen. Dokumentieren Sie den zugehörigen Pari-Code.