Homework 12 in Cryptography I

Prof. Dr. Rudolf Mathar, Wolfgang Meyer zu Bergsten, Michael Reyer

03.02.2009

Exercise 36. Assume an RSA module $n := pq$ with two primes $p \neq q$ and a public key $e = d^{-1}$. The message $m \in \{1, \ldots, n-1\}$ is encrypted using the RSA-algorithm with e.

(a) Show that it is possible to compute the secret key d if m and n are not coprime, i.e. if $p \mid m$ or $q \mid m$.

(b) Calculate the probability for m and n having common divisors.

(c) How large is the probability if n has 1024 bits? The primes p and q are approximately of same size ($p, q \approx \sqrt{n}$).

Exercise 37. Assume a single message m is encrypted with RSA twice: once with the public key (n, e) and once with the public key (n, f). The numbers e and f are relatively prime. Is it possible to decode the message with knowledge of the public parameters and the cryptograms?

Exercise 38. Alice encrypts a message m for Bob with RSA. Bobs public key is $(899, 11)$. Alice sends the encrypted message 468 to Bob.

What is the message m?