Exercise 11
Friday, July 7, 2017

Problem 1. (Shamir no-key protocol) Alice and Bob are using Shamir’s no-key protocol to exchange a secret message. They agree to use the prime \( p = 31337 \) for their communication. Alice chooses the random number \( a = 9999 \) while Bob chooses \( b = 1011 \). Alice’s message is \( m = 3567 \).

a) Calculate all exchanged values \( c_1 \), \( c_2 \), and \( c_3 \) following the protocol.
   Hint: You may use \( 6399^{1011} \equiv 29872 \) (mod 31337).

Problem 2. (Proof of 8.3) Let \( n = p \cdot q \), \( p \neq q \) be prime and \( x \) a non-trivial solution of \( x^2 \equiv 1 \) (mod \( n \)), i.e., \( x \neq \pm 1 \) (mod \( n \)).

Then
\[
gcd (x + 1, n) \in \{p, q\}
\]

Problem 3. (RSA encryption) A uniformly distributed message \( m \in \{1, \ldots, n - 1\} \) with \( n = pq \) with two primes \( p \neq q \) is encrypted using the RSA-algorithm with public key \( (n, e) \).

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 of (b) roughly, if \( n \) has 1024 bits and the primes \( p \) and \( q \) are approximately of same size \( (p, q \approx \sqrt{n}) \).