Cryptography (SS2006) Prof. Michael Backes

Exercise Sheet 8

Out: June 20, 2006 Saarland University

Problem 1: Wiener's Attack

Let $N = 99221$ and $e = 39437$ be an RSA public key, and suppose that for efficiency reasons the secret RSA exponent d was chosen small, i.e., you know that $d \leq \frac{1}{3}N^{0.25}$. Apply Wiener's attack to find the secret exponent d and factor N.

Problem 2: Breaking ElGamal Signatures

(a) For creating an ElGamal signature one chooses a value r and keeps it secret. Suppose this r is leaked somehow to the public. Show how to compute the secret key x from a signature (s, t) for a message m knowing the value r used for creating this signature.

(b) The random value r needs to be chosen freshly for each new signature. Suppose that in order to save time, a value r was used to compute two signatures. Show how to compute the secret key x given two signatures (s_1, t_1) for m_1 and (s_2, t_2) for m_2 where the same value r was used.

(**Hint:** From part (a) it follows that it is sufficient to find the value r which was used to compute the signature.)

Problem 3: Breaking DSA Signatures

The specification of DSA requires that if either $s = 0$ or $t = 0$ for a DSA signature (s, t), then one needs to recompute the signature using another r. Show how to compute the secret key x given a "DSA signature" $(s, 0)$ for m.