The art of cryptography, summer 2016

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Monday, 2 May 2016, 11:59

Exercise 3.1 (RSA Hardcore Bit). (8+6 points)

In this exercise we will examine the question whether an algorithm that gives you partial information on the plaintext (given the public key and the ciphertext) already gives you the complete plaintext.

(i) First assume that you are given an algorithm BitZero that on input (N, e, y) outputs the least significant bit of the plaintext x (so it says whether x is even or odd). Construct given BitZero an algorithm $\mathcal{A}$ on input (N, e, y) produces the whole plaintext x. [Hint: If $\mathcal{A}(N, e, y) = 0$ then $x = 2x'$. Otherwise note that N is odd!] 8

(ii) Often one has probabilistic algorithms which will not always give the correct answer, but work with a certain error probability. You are now going to explore how such an algorithm would behave in our setting. So assume now that the algorithm BitZero has a small error probability of 2^{-n} where n is the number of bits in N. Compute the probability that your algorithm $\mathcal{A}$ returns the correct plaintext. [Hint: The Bernoulli inequality states that $(1 + x)^r \geq 1 + rx$ for $x > -1$ and $r \geq 0$.] +3

(iii) Finally assume that the attacking algorithm has a huge error probability of 40%. Can you still compute the entire plaintext efficiently? +3

Exercise 3.2 (CBC not IND-CCA). (6 points)

CBC with any block cipher can never be IND-CCA secure. Prove this!

(i) Write down an exact definition of CBC. You need encryption and decryption, in particular, it is important to specify the ciphertext exactly. 2

(ii) Prove that CBC is not IND-CCA secure. 4