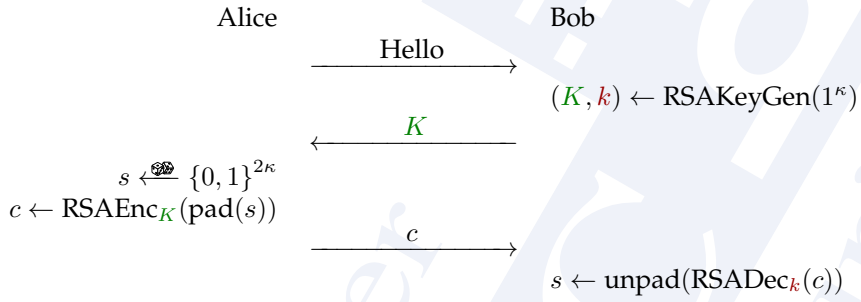
The art of cryptography, summer 2017

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Friday, 19 May 2017, 11:59

Exercise 3.1 (RSA key exchange). (8+2 points)

Consider the RSA key exchange:



(i) It is used in TLS. Under which name? [1]

(ii) What is known about its security? Find related security proofs, cite the papers and briefly explain their results and assumptions. [7]

In particular: Is it passively ROR-POA secure? Is it more?

(iii) In which respect is it worse than the Diffie-Hellman key exchange? [+2]

Exercise 3.2 (Hybrid crypto). (14+2 points)

Consider the situation in the exercises 1.2 and 1.3 from the last sheet. Eve has eavesdropped the conversation between Alice and Bob. She has recorded the RSA-cypher text $c = \text{enc}_{(N,e)}(k)$ of the AES key k. She tries the following attack to recover k from c. We consider an attack as successful if it takes less than 2^{100} bit operations.

(i) How could Eve recover k if she tries all possible values? Is this a successful attack? [2]

(ii) Eve computes $cx^{-e} \bmod N$ and y^e for all $1 \leq x, y \leq 2^{64}$ and stores these values in two lists. How can Eve recover k from these lists? Is this a successful attack? [4]

(iii) The attack in (ii) may fail in some situations. In which does it fail? What is the probability of failing? [2+2]

(iv) Eve finds that $e = 3$. Can she successfully recover k even if the attack in (ii) fails? [3]

(v) How can one fix the vulnerability in the way RSA and AES is employed by Alice and Bob? [3]