Esecurity: secure internet & e-cash, summer 2012

MICHAEL NÜSKEN, RAOUL BLANKERTZ

2. Exercise sheet
Hand in solutions until Sunday, 15 April 2012, 23:59

Exercise 2.1 (Hybrid crypto). (14+2 points)

Consider 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 $c = \mathrm{enc}_{(N,e)}(k)$ 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]

Exercise 2.2 (GnuPG). (6 points)

(i) Which cryptographic algorithms are implemented in GnuPG? How is the idea of a hybrid crypto system implemented in GnuPG? [3]

(ii) Read PHONG Q. NGUYEN, *Can We Trust Cryptographic Software? Cryptographic Flaws in GNU Privacy Guard v1.2.3*. How does the used implementation for RSA differ from the textbook version? What are the consequences? [3]