Esecurity: secure internet & e-cash, summer 2015

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Monday, 27 April 2015, 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 (Repetition: Security notions). (12 points)

Recall the following notions from your Cryptography lecture or read Chapter 12 in Katz & Lindell (2008), Chapter 7 in Stinson (2006) or Chapter 10 in Bellare & Goldwasser (2008): There are several levels of security

- Unbreakability (UBK or UB),
- Universal Unforgeability (UUF; also called *selective* unforgeability),
- Existential Unforgeability (EUF);

along with different means for an attacker:

- Key-Only Attack (KOA),
- Known Signature Attack (KSA),
- [Adaptively] Chosen Message Attack (CMA).

Pairing an adversarial goal with an attack model defines a security notion, e.g. EUF-CMA.

4 (i) Give a short description of each security level and each attack. Does security in one notion imply security in some other notions? Picture the implications in a suitable way.

6 (ii) Consider the ElGamal signature scheme with a cyclic group G. Assume that the discrete logarithm problem for G (DL_G) is hard, ie. it is hard to compute a from g^a where g is a generator of G. Decide for each of the 9 security notions whether the scheme is

- secure,
- not secure, or
- the answer is unknown.

Give for each claim a short hint or quote.

2 (iii) What can you say, if you assume that DL_G is easy?

References

MIHIR BELLARE & SHAFI GOLDWASSER (2008). Lecture Notes on Cryptography. URL `http://cseweb.ucsd.edu/~mihir/papers/gb.html`.

JONATHAN KATZ & YEHUDA LINDELL (2008). *Introduction to Modern Cryptography*. Cryptography and Network Security. Chapman & Hall/CRC. ISBN 1-58488-551-3. 534 pages.

DOUGLAS R. STINSON (2006). *Cryptography - Theory and Practice*. Discrete Mathematics and its Applications. Chapman & Hall / CRC Press, Boca Raton FL, third edition. ISBN 1584885084, 593pp.