The art of cryptography, summer 2016

MICHAEL NÜSKEN

4. Exercise sheet
Hand in solutions until Monday, 9 May 2016, 11:59

Exercise 4.1 (Repetition: Security notions). (8 points)

Recall the security notions for signatures. You can also find more about them in Chapter 12 in Katz & Lindell (2008), Chapter 7 in Stinson (2006) or Chapter 10 in Bellare & Goldwasser (2008).

(i) Consider the ElGamal signature scheme. Namely, the key generator outputs a triple (G, g, q), a easily-revertable function $* \to G\mathbb{Z}_q$, a hash function h and a public key A and private key a with $A = g^a$ in G. The verification tests whether [6]

$$A^{B^*} B^c = g^{h(m)}.$$

Assume that the discrete logarithm problem for G ($\mathrm{DL}_{G,g,q}$) is hard, ie. it is hard to compute a from g^a where g is a generator of G. Decide for each of the nine security notions whether the scheme is

- secure (Under which assumption?),
- not secure, or
- the answer is unknown.

Give for each claim a short hint or quote.

(ii) What can you say if you assume that $\mathrm{DL}_{G,g,q}$ is easy? [2]

Exercise 4.2 (Necessities of security). (4 points)

For a signature scheme, a message is first hashed and then the hash value is signed. Assume that the signature scheme is secure in the EUF-CMA model. Does that imply that the hash function is collision resistant? Prove your answer. [4]

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.