Esecurity: secure internet & evoting, summer 2010

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

8. Exercise sheet
Hand in solutions until Sunday, 20 June 2010, 23.59 h

Exercise 8.1 (AES-XCBC-MAC-96). (8 points)

Read RFC 3566.

(i) Describe the insecurities for "[t]he classic CBC-MAC algorithm [...] for messages of varying lengths". 2

(ii) Describe the extensions used to construct AES-XCBC-MAC-96. 4

(iii) How are performance and security affected? 2

Exercise 8.2 (Zero-Knowledge). (10 points)

Read

JEAN-JACQUES QUISQUATER, MYRIAM QUISQUATER, MURIEL QUISQUATER, MICHAËL QUISQUATER, LOUIS GUILLOU, MARIE ANNICK GUILLOU, GAÏD GUILLOU, ANNA GUILLOU, GWENDOLÉ GUILLOU, SOAZIG GUILLOU & TOM BERSON (1989). How to Explain Zero-Knowlegde Protocols to Your Children. Number 435, 628–631. ISSN 0302-9743

to one of your children. Alternatively take one of your fellow students.

(i) Write down the protocol in a form appropriate for computer science students rather than for children. 4

(ii) Prove for this protocol the three properties mentioned in Exercise 7.2 (iii). 6

Exercise 8.3 (Voting). (11 points)

Two fundamental steps in voting are

election process getting the voters' opinion (assuming they have one),

tallying process transforming the voters' opinion into a final result.

The party pooper for the second point is ARROW's theorem. In this lecture we deal with the first point. The bad news here is reality. The US Presidential Election in 2000 had several problem's with the first step.

3 (i) List three of these problems as precisely as possible (give your sources).

4 (ii) Has something similar happened in Germany or in your home country (take your state, if you are German)?

4 (iii) Derive general principles for the election process.