Symmetric primitives, winter 2014/15

MICHAEL NÜSKEN

3. Exercise sheet
Hand in solutions until Monday, 10 November 2014, 13:59

Exercise 3.1 (CBC not IND-CCA). (6 points)

CBC with any block cipher can never be IND-CCA secure. Prove this!

(i) Write down an exact definition of CBC. You need encryption and decryption, in particular, it is important to specify the ciphertext exactly. [2]

(ii) Prove that CBC is not IND-CCA secure. [4]

Exercise 3.2 (FOS vs. IND). (6+6 points)

Consider the notion FOS-CPA[1]: in IND-CPA the attacker gets an encryption oracle and a challenge oracle. Here, the attacker just gets one oracle accepting two plaintexts and returning one encryption namely either

- FIRST which returns the encryption of the first plaintext, or
- SECOND which returns the encryption of the second plaintext.

Prove or disprove:

(i) If an encryption scheme is FOS-CPA secure then it is IND-CPA secure. [4]

(ii) If an encryption scheme is IND-CPA secure then it is FOS-CPA secure. [2+4]

(iii) Which model do you consider more realistic? Reason. [+2]

[1] Name changed.