Esecurity: secure internet & e-passports, summer 2011

MICHAEL NÜSKEN, RAOUL BLANKERTZ

9. Exercise sheet
Hand in solutions until Sunday, 5 June 2011, 23:59

Exercise 9.1 (CBC-MAC). (9+4 points)

Consider a block cipher in CBC mode and a CBC-MAC with the same underlying block cipher.

(i) What happens if we use for both schemes the same key? Which blocks can be changed while keeping the MAC tag valid? [3]

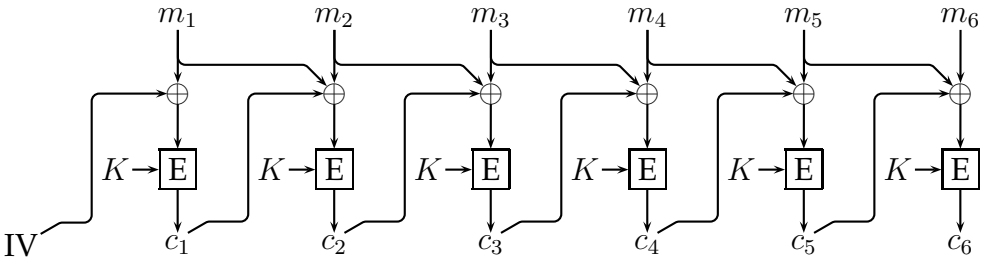
(ii) Assume we choose the initial vector for the MAC randomly and send it along with the message and the MAC tag. How can an attacker change the message? [3]

(iii) Given two pairs of message and MAC tag (m, t) and (m^*, t^*), can an attacker somehow concatenate them to achieve a longer message with valid MAC tag? [3]

(iv) Construct a modified version of CBC-MAC that prevent such a "concatenating attack". [+4]

Exercise 9.2 (Plaintext ciphertext block chaining, PCBC). (8 points)

The Kerberos designers unsuccessfully tried to do encryption and authentication in one go as follows:



At the end of the message they put a special recognizable piece of text. If and only if it decrypts properly the recipient decides that the message is ok.

2 (i) Describe the decryption.

2 (ii) Which blocks are affected if an attacker or an error changes c_3? Explain.

2 (iii) What happens if an attacker exchanges c_2 and c_3?

2 (iv) What happens if an attacker exchanges c_2 and c_4?

Exercise 9.3 (Authenticated encryption). (4+4 points)

(i) Read P. ROGAWAY & D. WAGNER (2003). A Critique of CCM.

1 (ii) What is authenticated encryption?

3 (iii) Briefly describe the CCM mode.

+4 (iv) Summarize the criticism made in the paper.