Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

12. Exercise sheet
Hand in solutions until
Monday, 02 February 2009, 11^{59}am (deadline!).

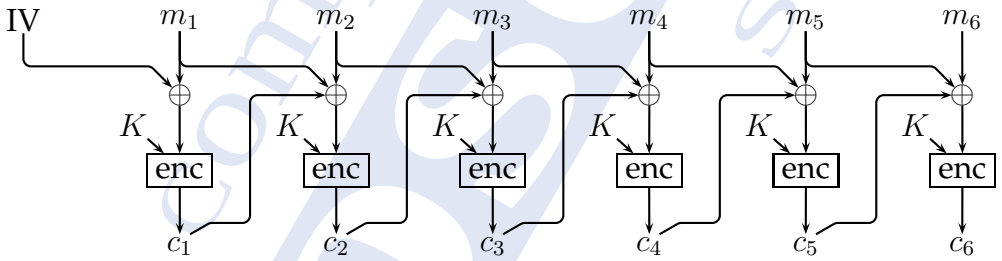
As usual: Any claim needs a proof or an argument.

Exercise 12.1 (What to ask.). (0+4 points)

Think about what you have learned during the semester and find at least one appropriate exam exercise. +4

Exercise 12.2 (Plaintext ciphertext block chaining, PCBC). (8+2 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.

(i) Describe the decryption. 2

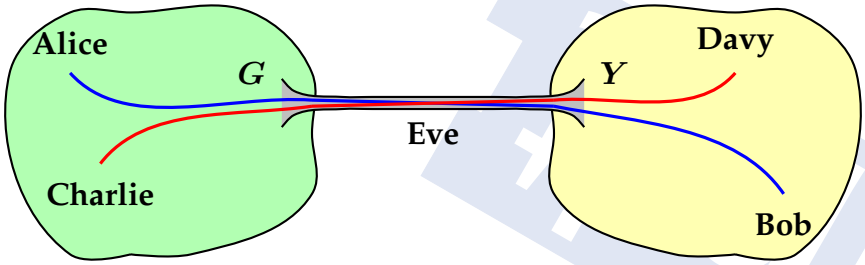
(ii) Which blocks are affected if an attacker or an error changes c_3? Explain. 2

(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? 2

(v) Go beyond! +2

Exercise 12.3 (Splicing Attack). (6+2 points)



Suppose that the gateways G and Y link the green and the yellow LAN by an encrypted but not authenticated IPsec tunnel using a fixed SA. Assume that the encryption is done by some symmetric cipher in CBC mode. We want to show that Eve and her boss Davy can read all the traffic between Alice and Bob.

2 (i) How does the beginning of a packet from Charlie to Davy look like?

2 (ii) Replace the beginning of a packet from Alice to Bob or from Bob to Alice with the start of an eavesdropped packet from Charlie to Davy. What happens?

+2 (iii) How can Davy find out the part just after the replaced beginning? [Consider retransmitting...]

2 (iv) Draw conclusions. [Formulate a proposal, explain, argue.]

(v) Go beyond.