Cryptographic passports & biometrics, summer 2009

MICHAEL NÜSKEN, KONSTANTIN ZIEGLER

8. Exercise sheet
Hand in solutions until Monday, 22 June 2009.

Any claim needs a proof or argument.

Exercise 8.1 (Modes of operation). (8 points)

(i) Discuss advantages and disadvantages of each of the modes of operation presented in class: ECB (Electronic Codebook) and CBC (Cipher Block Chaining). [2]

(ii) Answer the following questions concerning error propagation for each of the aforementioned modes. [3]

(a) How many text blocks are false if one of the transmitted blocks is corrupted?

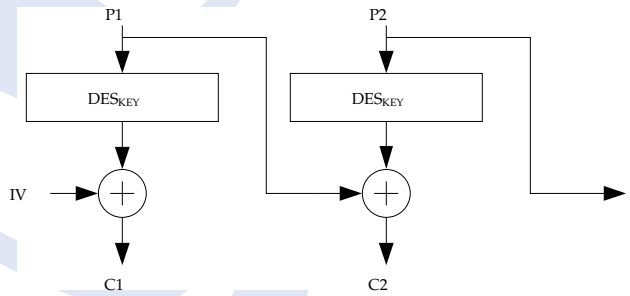
(b) How many text blocks are false if one of the transmitted blocks is dropped unnoticed?

(c) How many text blocks are false if one of the block cipher boxes outputs a wrong result?

Try to draw conclusions from your observations.

(iii) Look up the definitions for the modes CFB (Cipher Feedback), OFB (Output Feedback) and discuss one of them. [2]

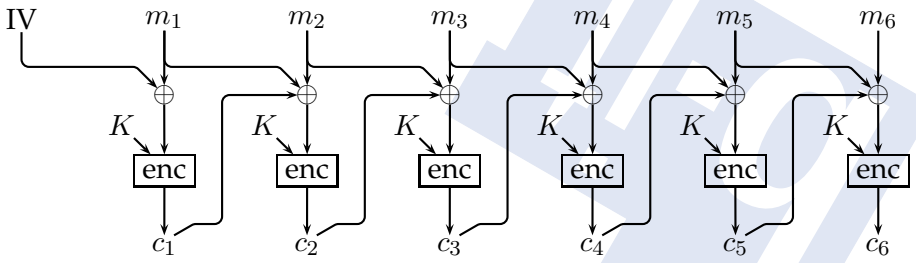
(iv) We define a further mode PBC (Plain Block Chaining) that adds the message P_i to the encrypted message C_i as depicted in the following picture. [1]



Answer the questions under (ii) also for this mode.

Exercise 8.2 (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.

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?

+2 (v) Go beyond!

Exercise 8.3 (entropy of the MRZ). (4 points)

4 Give a first rough upper bound on entropy of the MRZ by simply considering the types of entries for all involved places. Next reduce this bound using reasonable assumptions on the information. What else can you do using publicly available information of a given person?

Exercise 8.4 (primary biometric identifier). (4 points)

4 In the lecture you discussed "'Why ICAO selected the face as primary biometric identifier specified to epassports"'. Consider the voice of a person as biometric identifier and comment whether the arguments for the ICAO's decision still hold or not.