Security on the Internet, winter 2008

MICHAEL NÜSKEN, DANIEL LOEBENBERGER

11. Exercise sheet
Hand in solutions until
Monday, 26 January 2009, 11^{59}am (deadline!).

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

Exercise 11.1 (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). $\boxed{2}$

(ii) Answer the following questions concerning error propagation for each of the aforementioned modes. $\boxed{3}$

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

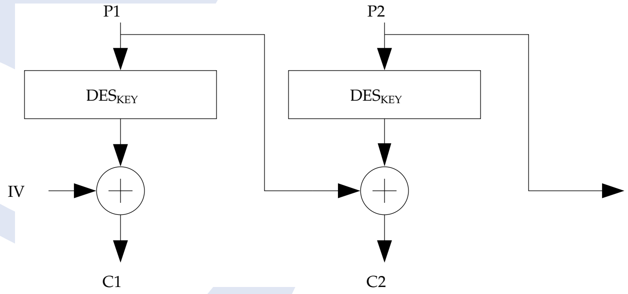
(b) How many text blocks are false if one of the transmitted blocks is dropped unnoticed?

(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. $\boxed{2}$

(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. $\boxed{1}$



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

Exercise 11.2 (MACs are necessary!). (4 points)

4 Consider the following ASCII table

Binary	Decimal	Hexadecimal	Glyph
0100 0001	65	41	A
0100 0010	66	42	B
0100 0011	67	43	C
0100 0100	68	44	D
0100 0101	69	45	E
0100 0110	70	46	F
0100 0111	71	47	G
0100 1000	72	48	H
0100 1001	73	49	I
0100 1010	74	4A	J
0100 1011	75	4B	K
0100 1100	76	4C	L
0100 1101	77	4D	M
0100 1110	78	4E	N
0100 1111	79	4F	O
0101 0000	80	50	P
0101 0001	81	51	Q
0101 0010	82	52	R
0101 0011	83	53	S
0101 0100	84	54	T
0101 0101	85	55	U
0101 0110	86	56	V
0101 0111	87	57	W
0101 1000	88	58	X
0101 1001	89	59	Y
0101 1010	90	5A	Z

Assume you intercepted a message (m, IV), $m \in \{0,1\}^*, \mathrm{IV} \in \{0,1\}^{64}$ where the plaintext was encoded according to the above ASCII table and encrypted with the CBC mode of a block cipher with block length 64 bit and initialization vector IV=`0xAAAAAAAAAAAAAAAA` yielding m. Assume further you know that the plaintext of the message starts with the phrase `DEAR SIR`. Find an initialization vector IV′ such that the decrypted message will start with `DEAR MAM`.

Exercise 11.3 (To boldly go where few men have gone before). (0+13 points)

In 2000 Bellare and others discussed in their paper "The Security of the Cipher Block Chaining Message Authentication Code" the CBC-MAC in great detail. The goal of this exercise is to find out what exactly they proved. Here it is *not* important to get every detail of their (kind of technical and long) proof, but to understand in in principle what they showed.

(i) Read the paper and find out which model they used and what they have proved. $\boxed{+8}$

(ii) In connection with the HMAC construction we discussed a kind of *keyed collision resistance*. Do the results of this paper also imply such a property for the CBC-MAC construction? $\boxed{+5}$